Internet in China:

Big Mama is Watching You

Internet Control and the Chinese Government

MA Thesis
Supervisor: Dr. S.R. Landsberger
Chinese Languages & Cultures
University of Leiden
July 2001

Lokman Tsui 9639454
Marshallsingel 30
1187 LG Amstelveen
020-4560283
lokmant@euronet.nl
mail@lokman.nu

Acknowledgements

This thesis would not have been possible without the patience and support of Waiyu and my parents. I am also grateful to my supervisor Dr. Landsberger, Drs. Keijser, Dr. Schneider and my friend Raymond van Erkel for reading and helping me to revise this thesis.

Abstract

Initially, the internet was an open medium with certain characteristics that made it hard to control. According to Western journalists and politicians, the efforts of the Chinese government to control the internet are doomed to fail. This study attempts to counter this view and discusses to what degree the Chinese government can control the internet in China and, more than that, to what degree the internet can be used as a means for control. Methodologically, the four modalities of control (the law, architecture, social norms and the market), set forth by Lessig will be used. As a result, this study will offer a legal, technical, social and economical perspective in discussing the degree of internet control in China. Lessig further argues that the architecture of the internet is undergoing changes that continue to enable control. A prime example of using architecture as a means of control is the concept of the Panopticon prison, invented by Bentham and mediated by Foucault. The concept of the Panopticon will be used to show how the internet can be used as a means for control. The conclusions are that the Chinese government are quite capable of controlling the internet in China and that China has the perfect ingredients for deploying a digital Panopticon. This digital Panopticon will continue to improve and develop, driven by the market. These conclusions show that the internet, to contrary belief, can be controlled and even be used as a means for control.

Problem

To what degree can the Chinese government control the internet in China and to what degree can the internet be used as a means for control?

Keywords

internet regulation, internet control, social control, political control, censorship, privacy, surveillance, panopticon, Lessig, internet in China, Chinese Internet, media.

Index of Contents

1. 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."[1] (former President of the United States Bill Clinton, 8 March 2000)

This quote from Clinton shows what appears to be the general consensus in the West and in particular the United States: the development of the internet will bring immense changes to authoritarian regimes such as China. These regimes are trying to stop an irresistible force in their efforts to control the internet.[2] One cannot but agree with Clinton when one keeps hearing from journalists and politicians that the internet is the harbinger of freedom without boundaries. Information previously unavailable to the ordinary Chinese citizen is now accessible on the World Wide Web (WWW). Although the Chinese government attempts to block websites deemed undesirable, the information can still travel in China due to the "inherent characteristics" of the internet by re-routing the information around the filters. "The state is [just] too big, too slow, too geographically and technically limited to regulate a global citizenry's fleeting interactions over a mercurial medium."[3]

Or is it? Why is the Chinese government promoting the use of internet if by doing so, they will shoot in their own feet? What are the inherent characteristics of the internet that make it impossible to control? What means does the Chinese government currently employ to control

All online articles were last visited on 4 June 2001.

[1] Bill Clinton in a speech at Paul H. Nitze School for Advanced International Studies at Johns Hopkins University on 8 March 2000, quoted after Shanthi Kalathil, William J. Drake, Taylor C. Boas, "Dictatorships in the Digital Age: Some Considerations on the Internet in China and Cuba," *Information Impacts* (October 2000), http://www.cisp.org/imp/october_2000/10_00drake.htm

[2] More outspoken authors include two from The New York Times. See Friedman, Thomas,"Censors Beware," *The New York Times* Jul. 25, 2000 and Wright, Robert, "Gaining Freedom by Modem," *The New York Times* Jan. 28, 2000. A couple of other examples include Barbara Crossette, "The World: Out of Control; The Internet Changes Dictatorship's Rules," *New York Times* Week In Review, 1 August 1999, p.1. Bay Fang, "Chinese 'Hacktivists' Spin a Web of Trouble: The Regime is Unable to Control the Internet," *U.S. News and World Report* September 1998, p.47. Dan Gillmor, "Internet will find Way around China Censorship," *Mercury News*, http://www0.mercurycenter.com/svtech/news/indepth/docs/dg112200.htm. The latest example would be Walter Isaacson, "Going Online when the Emperor's Away", *Time* (4 June 2001), http://www.time.com/time/world/printout/0,8816,109632,00.html

[3] Boyle, James, "Foucault in Cyberspace," (1997) http://www.law.duke.edu/boylesite/fouc1.html

the internet? This thesis wants to provide a broader framework to the question to what degree control of the internet by the Chinese government is possible.

Internet and internet control are issues that are closely linked to matters of state power, privacy and in China's case – democracy. However, the scope of this thesis is not to research whether the internet will facilitate democracy in China.[4] The ethical question of the desirability of internet control will not be discussed either. This thesis will solely focus on the question whether the Chinese government is capable of controlling the internet, which should be a moot question, according to libertarians. However, in the past two to three years, studies that are more critical of the possibilities of internet regulation started to appear in Western literature. The notion that the internet is impossible to control is already giving way to more sceptical sounds.[5] Non-authoritarian and authoritarian regimes alike are looking for ways to control and regulate the internet.

1.1 Literature Review: Internet in China

Existing literature that discusses the impact of the internet has consistently been written from a Western point of view. It is needless to say that the theories used in these books cannot be readily applied on a 1-to-1 basis to China, a country that through sheer size, history and culture has its distinctive differences that warrants its own research. Literature that deals with the internet in China in specific is sparse.[6] This section will review sources that deal with the internet in China. The following two sources show some typical shortcomings this thesis tries to address:

Taubman in "A Not-So World Wide Web" examines whether the internet will facilitate democracy in China.[7] He argues that the internet eventually will pose an insurmountable threat to the Chinese government. The biggest deficiency in his arguments however, is that he takes "the built-in incompatibility of the internet with authoritarian regimes" for granted.[8]

Hill and Hughes in *Cyberpolitics: Citizen Activism in the Age of Internet* mounted a laudable project trying to quantify political activities on the internet.[9] They base their method on measuring messages posted in the newsgroups (Usenet). Usenet in China, however, is almost non-existent, virtually none of the postings in the newsgroup originated from China.[10] The biggest flaw of the study is thus the lack of knowledge about the situation of the internet in China.

[4] For a comprehensive study that discusses the question of democracy and the internet in China, see Qiu, Jack Linchuan, *Mediating the Political Impact of the Internet: The Case of China*. MA. Thesis, University of South California., 1999.

[5] According to the Economist, governments do have a certain amount of control and are very capable of regulating the internet. See The Economist, "Stop Signs on the Web," *The Economist* (11 January 2001), http://www.economist.com/printedition/PrinterFriendly.cfm?Story_ID=471742

[6] Lynch even argues that "on the question of telecommunications, the silence of the transitions literature is deafening." See Lynch, Daniel, *After the Propaganda State: Media, Politics and "Thought Work" in Reformed China*. Stanford, CA: Stanford University Press, 1999. p.227.

[7] Taubman, Geoffry, "A Not-So World Wide Web: The Internet, China, and the Challenge to Nondemocratic Rule," *Political Communication* 15 (1998), pp.255-272.

[8] Idem, p.256.

[9] Hill, K.A. & Hughes, J.E., *Cyberpolitics: Citizen Activism in the age of the Internet.* Lanham, MD: Rowman & Littlefield, 1998.

[10] What they ***did*** measure, were mostly the opinions of Chinese people located overseas. Usenet is sparsely available in China, a handful of known Usenet servers exists, and one can also reach the newsgroups by way of the web, groups.google.com.

1.2 Literature Review: Control of Internet in China

Literature that deals with internet control in China can broadly be divided in two categories: sources that deal with technical issues and sources that deal with censorship issues. Below, representative examples will be reviewed.

Professor Tan from Syracuse University has published numerous articles on the control of the internet in China. His useful articles are written from a primarily technical point of view, but become dated quickly because of the rapid developments in the infrastructure of China.[11]

Huang Yu, Hao Xiaoming and Zhang Kewen published an article "Challenges to Government Control of Information in China" in the journal *Media Development*.[12] This article discusses the loss of control of the Chinese government over state media due to the introduction of satellite television and the internet; unfortunately the article is quite dated. (1996)

An article that deals with online censorship is "Censorship and Protest: The Regulation of BBS in China People Daily" from Wenzhao Tao that examines how censorship is enacted in the popular Qiangguo BBS managed by the *People's Daily*.[13]

Jack Linchuan Qiu discusses virtual censorship in his article "Virtual Censorship in China: Keeping the Gate Between the Cyberspaces" in *International Journal of Communications Law and Policy*. He examines how the internet in China functions as a means for political communication.[14]

Katherine Hartford, professor of Political Science at the University of Massachusetts, describes the situation of internet in China in *Current History*, partly discussing control, and argues that the government very much has the power to control the internet .[15]

Currently the most comprehensive study on the internet in China comes from the report of William Foster and Seymour E. Goodman titled *The Diffusion of the Internet in China* dated November 2000.[16] Internet control is discussed amongst other topics. The report offers a wealth of information but is mostly descriptive in nature without drawing too much conclusions.

1.3 Choice of Theoretical Framework

In order to discuss government control of the internet, we will need to look at various aspects concerning internet in China. Lessig is considered to be the foremost scholars on internet law.[17] He has a distinctive view on the regulation of the internet and argues that regulation of

[11] Articles include Tan & Yurcik, "The Great (Fire)Wall of China: Internet Security and Information Policy Issues in the People's Republic of China," http://www.tprc.org/abstracts/tan.txt and also Tan, Mueller, Foster, "China's New Internet Regulations: Two Steps Forward One Step Back," http://som.csudh.edu/cis/lpress/devnat/nations/china/chinah.html also published in *Communications of the ACM*, Vol. 40, No. 12, December 1997, pp. 11-16.

[12] Huang Yu, Hao Xiaoming, Zhang Kewen, "Challenges to Government Control of Information in China," *Media Development* (February 1997), http://www.oneworld.org/wacc/media/china.html

[13] Tao, Wenzhao, "Censorship and Protest: The Regulation of BBS in China People Daily," *First Monday* (January 2001), http://www.firstmonday.dk/issues/issue6_1/tao/

[14] Qiu, Jack Linchuan, "Virtual Censorship in China: Keeping the Gate between the Cyberspaces," *International Journal of Communication Law and Policy*, Vol. 4, Winter 1999/Spring 2000, pp.1-25.

[15] Hartford, Katherine, "Cyberspace with Chinese Characteristics," University of Massachusetts, Boston, September 2000. http://www.pollcyber.com/ch/pubs/home.htm

[16] Foster and Goodman, *The Diffusion of Internet in China*, Center for International Security and Cooperation, Stanford University, November 2000.

[17] Lessig has been consulted in the anti-trust case of the U.S. versus Microsoft and in the Napster case, both landmark lawsuits. He was previously Law professor at the University of Chicago, then went to Harvard and recently moved to Stanford University.

the internet is very much possible. This thesis will explore to what degree Lessig's view can be applied to the situation in China. Internet as a means of surveillance to control behaviour is another issue that will be addressed. The concept of the Panopticon, invented by Jeremy Bentham and mediated by the French philosopher Michel Foucault, will be used to explore the issue of how the internet can be used as a means for surveillance.

This thesis will use Lessig's framework to examine how the government controls the internet and use the concept of the Panopticon to expand upon the previous question and examine how the internet can be used as a means for control.

1.4 Set-up

Chapter 2 will set forth the main problem and examine the problems that the internet poses to those who attempt to regulate or control it. The original characteristics of the internet will be described and explained why they make life difficult for those who seek to control it. Having defined the problem, the theoretical framework that is used to canvass this thesis will be explored.

In chapter 3, we will provide some basic information on the internet in China, laying the foundation for further discussion. First, we will try to explain why the Chinese government insisted in introducing and developing the internet, since it is supposed to be so troublesome to control. Then, the function of the media in China will be explained, as it is crucial to understand how the Chinese government view the media and their function in society. The role of the media underwent some drastic changes in the last two decades and these changes will be described in the remainder of chapter 3. A concept that needs to be explored is the 'Chinese government', which underwent changes due to the internet. The different government bodies and their specific functions related to the internet, and the complex power struggle between them are described. Lastly, the development of the internet in China will be examined, giving a brief overview of the history of the development from the beginning up until 2001.

In chapter 4, we will examine how control is enacted in China and which developments can strengthen this control. The way the law, architecture, social norms and the market can regulate behaviour and for what reasons they do this well, or fail to do so, are discussed.

The thesis will conclude with a model that describes how the Chinese government is implementing a control structure with regard to the internet in China. The conclusion will also offer the limitations of this thesis and provide grounds for further research.

The appendix will hold a list of technical definitions regarding the internet although this thesis is written in such a way that a less technical person should also be able to read it. Along with this technical list, a table with the key government bodies and their functions, a list of the key regulations, a list of the functions of the Ministry of Information Industry (MII), the main body responsible for the internet in China, a list of specific internet crimes and an example of censorship is given.

All transcriptions are in *pinyin*, the official transcription system for Mandarin Chinese.

2. Control of the Internet

This chapter will introduce the theoretical framework that is used to canvass the thesis. First, the question why the original characteristics of the internet made it hard to control will be discussed. Then, the view of Lessig will be used to explain by which means the internet can be controlled. We will also explain the concept of the Panopticon prison as a means to use the internet for the purpose of control.

2.1 Characteristics of the Internet

> "The linking of the world's people to a vast exchange of information and ideas is a dream that technology is set to deliver. It will bring economic progress, strong democracies ... and a greater sense of shared stewardship of our small planet."[18] (former Vice President Al Gore)

According to libertarians, authoritarian regimes such as China that rely on information control will be defenceless against the internet. Some authors even go as far as to imply that eventually the internet will facilitate a civil society that in turn will bring democracy. States are unable to regulate the internet because of 'the technology of the medium, the geographical distribution of its users, and the nature of its content'; what Boyle calls the "Internet Holy Trinity".[19]

The Technology of the Medium

> "The Net interprets censorship as damage and routes around it."[20] (John Gilmore)

From a technical point of view, the internet is a packet-switched network, meaning it is designed so that data are 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. People with sufficient technical knowledge always will find a way to reach the blocked information. However, as the internet population grows, the majority consists of users that do not have the required technical knowledge. Filters are being placed by libraries, employers and states and investment in filter software continues to grow.

[18] Taubman, "A Not-So World Wide Web," p.255

[19] Boyle, "Foucault in Cyberspace," http://www.law.duke.edu/boylesite/fouc1.html

[20] Though the quote is attributed to Gilmore, he himself acknowledges he does not know when and where he used it. For a more detailed explanation of the origin of this quote, see Reagle, Joshep, "Internet Quotation Appendix," (26 March 1999), http://cyber.law.harvard.edu/people/reagle/inet-quotations-19990709.html

"On the internet, nobody knows you're a dog" [21] (cartoon from *the New Yorker*)

The high degree of anonymity and pseudonymity is another characteristic of the internet that makes it hard to control.[22] One can anonymously browse the web or use a pseudonym to chat with other users. It is common to adopt a nickname on the internet. However, companies and governments are spending a lot of money to invest in technology that raises the degree of identification and accountability. Greenleaf even argues that the default condition of communication IRL (In Real Life) is anonymity, as compared to the internet where the default condition of communication is some form of identification.[23]

The Geographical Distribution of Internet Users

A result of the routing ability of the internet is what Froomkin calls 'regulatory arbitrage': if one does not like the regulation of one country, one can easily move to a server elsewhere because the internet knows no boundaries.[24] Post and Johnson repeated the same principles. In their article "Law and Borders", they discuss that any attempt by an existing government to assert authority and control over the internet would be futile due to the ease of escaping jurisdiction on the internet that knows no boundaries.[25] However, artificial borders are starting to appear on the internet, spurred by commercial incentives from advertising companies and legislative developments as the Yahoo vs. France case.[26] In this case, France demanded Yahoo to make Nazi memorabilia, physically located at Yahoo servers in the United States,

[21] Cartoon reproduced from *The New Yorker* 5 July 1993, p61.
http://www.nytimes.com/2000/12/14/technology/14DOGG.html?pagewanted=all
[22] Froomkin, "Internet as a Source of Regulatory Arbitrage," University of Miami, 1996.
http://www.law.miami.edu/~froomkin/articles/arbitr.htm Also published in Brian Kahin, Charles Nesson (eds.), *Borders in Cyberspace*. MIT Press, 1997, p. 29.
[23] Greenleaf, Graham, "An Endnote On Regulating Cyberspace: Architecture VS Law?," (1998)
http://www.austlii.edu.au/au/other/unswlj/thematic/1998/vol21no2/ greenleaf.html
Also published as *University of New South Wales Law Journal* Volume 21,
Number 2, 'Electronic Commerce: Legal Issues For The Information Age', November 1998.
[24] Froomkin, "Internet as a Source of Regulatory Arbitrage," University of Miami, 1996.
http://www.law.miami.edu/~froomkin/articles/arbitr.htm
[25] Post and Johnson, "Law And Borders – The Rise of Law in Cyberspace," 48 *Stanford Law Review* 1367 (1996). Online version at http://www.firstmonday.dk/issues/issue1/law/
[26] For a legal study of the Yahoo case, see Salis, Richard, *A Look at how U.S. based Yahoo! Was Condemned by French Law*, University of Montreal (November 2000),
http://www.law.asu.edu/karjala/cyberlaw/Yahoo(France)Analysis.html#4 and also see Jim Hu and Evan Hansen, "Yahoo Auction Case May Reveal Borders in Cyberspace," *CNET* (11 August 2000),
http://news.cnet.com/news//0-1005-200-2495751.html

inaccessible for French citizens. This sets a legal precedence. Imagine China demanding organisations to remove content that is deemed undesirable in China, from servers not physically located in China.

The Nature of Content

"Information wants to be free"[27] (Stewart Brand)

It is hard or even impossible to block any form of content from the internet because it can be transferred using any other protocol and copied at almost no cost. Webpages can be sent by e-mail, transferred by FTP, retrieved from newsgroups or sent as a message over ICQ. If there is only one person or host who can access the content, that content can be shared over the whole network. However, commerce continues to battle copyright infringement.[28] Products are released that digitally protect intellectual property.[29]

2.2 The Four Modalities of Control

"Code is Law"[30] (Lessig)

Lessig provides a theoretical framework in *Code and Other Laws of Cyberspace* that uses a more comprehensive view to tackle the question how government can regulate the internet.[31] He disagrees with the view that the internet is impossible to regulate. He argues that the government can regulate behaviour by way of the law, architecture, social norms and the market. The law regulates by threat of state sanctions, social norms regulate by the threat of sanctions of a community. Markets regulate through price. According to Lessig:

> "Architecture, law, norms and markets together regulate behaviour. Together, they set the terms on which one is free to act or not; together, they set the constraints that affect what is and is not possible. They are four modalities of regulation; they together determine how individuals and states within their scope are regulated."[32]

Lessig then goes on to discuss how these four modalities compare with regard to the internet. Architecture that is precedented by code is the foremost regulator on the internet. In his own words:

> "Cyberspace is an architecture first. It is a platform that gets designed. It is constituted by a set of code – by software and hardware that make cyberspace as it is. This code imbeds certain values; it enables certain practices; it sets the terms on which life in cyberspace is lived, as crucially as the laws of nature set the terms on which life in real space is lived."[33]

[27] This is a quote so often used that its origin is unclear. The quote is often attributed to Stewart Brand. For a detailed description of the origin of this quote, see Clarke, Roger, "Roger Clarke's Information Wants To Be Free," (24 February 2000), http://www.anu.edu.au/people/Roger.Clarke/II/IWtbF.html

[28] The most famous example is the Napster case. See King, Brad, "Napster Loss is Copyright Gain," *Wired* (3 March 2001), http://www.wired.com/news/culture/0,1284,42167,00.html The article has links to other related articles.

[29] There are plans to implement copy protection in hard drives: Content Protection Recordable Media (CPRM). See Orlowski, Andrew, "Stealth Plan puts Copy Protection in Every Hard Drive," *The Register* (20 December 2000), http://www.theregister.co.uk/content/2/15620.html
For a good general explanation on CPRM see Orlowski, Andrew, "Everything you ever wanted to know about CPRM, but ZDNet would not tell you...," *The Register* (29 December 2000), http://www.theregister.co.uk/content/2/15718.html

[30] Lessig, Lawrence, *Code and Other laws of Cyberspace*. New York: Basic Books, 1999 p.3

[31] For a whole collection of Lessig's publications, see http://cyberlaw.stanford.edu/lessig

[32] Lessig, Lawrence, "Architecting for Control," (2000) http://cyber.law.harvard.edu/works/lessig/camkey.pdf. p.4

[33] idem, pp.4-5

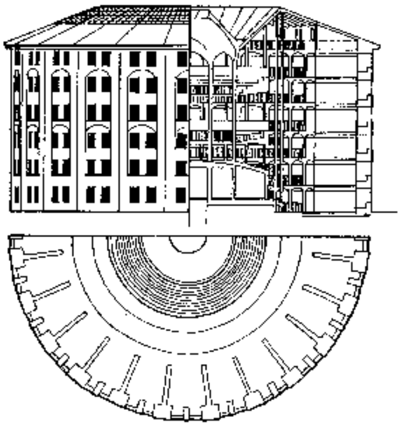
Developments in the architecture of the internet are spurring changes that make the internet easier to control. In real life, the laws of nature set constraints on what is possible. For example, gravity makes it impossible for a person to jump over a building. On the internet, the code of the architecture is the equivalent of the laws of nature in real life. Because code is malleable, characteristics 'inherent' to the internet, such as the Internet Holy Trinity from Boyle, do not exist and can be changed. Lessig continues that current changes in the code that erode the original libertarian concept of the internet are driven by commerce.

Although Lessig's theories have been attacked they still form a useful framework for the study of the internet and internet control in the People's Republic of China. Critics of Lessig do not find fault with the concept of the four modalities regulating behaviour. They also do not find fault with the theory that the code of the internet is undergoing changes, and that these changes will erode one's privacy. Critics find fault in the normative calls Lessig proposes to guard against the changes of the code that will erode one's privacy.[34] However, this thesis will not touch upon the measures as proposed by Lessig.

2.3 Panopticon

> "Morals reformed – health preserved – industry invigorated – instruction diffused – public burthens lightened – Economy seated, as it were, upon a rock – the Gordian knot of the Poor Laws not cut, but untied – all by a simple idea in Architecture!"[35] (Jeremy Bentham, 1791)

A great example of how architecture can regulate behaviour is the prison Jeremy Bentham describes as the Panopticon, a Greek-based neologism for 'all-seeing place'. Bentham invented the concept of the Panopticon in 1791 as a model prison designed as a means for social discipline. The design of the Panopticon is crafted so that all cells can be viewed from one central position and that prisoners cannot tell whether they are being watched, and thus a fear of constant surveillance is induced. The constant fear of being watched regulated the prisoners and induced "proper" behaviour.



[34] Catlett and Post represents the group that disagrees with Lessig on his proposals for reactive measures. See Catlett, Jason, "Privacy, Property and P3P: A Critique of Lessig's Property Regime Proposal," http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/somak/somak00/catlett.htm and see Post, David, "What Larry doesn't get," http://www.temple.edu/lawschool/dpost/Code.html or PDF at www.temple.edu/lawschool/dpost/Code.pdf p.1448 Rotenberg disagrees with Lessig on his explanation of the concept of privacy. In Lessig's defense: privacy is hardly a concept that is easy to define. Discussions about the precise concept of privacy are numerous. For the critique, see Rotenberg, Marc, "What Larry doesn't get," http://stlr.stanford.edu/STLR/Working_Papers/00_rotenberg_1/index.htm

[35] Lyon, David, "From Big Brother to Electronic Panopticon," http://www.rochester.edu/College/FS/Publications/Lyon.html
It is the text of chapter four of Lyon, David, *The Electronic Eye: The Rise of Surveillance Society* (Minneapolis: University of Minnesota Press, 1994): 57-80.

The concept of the Panopticon in modern society only gained recognition and widespread interest after being mediated by Michel Foucault. In *Discipline and Punish,* he describes how the Panopticon provides new insight into how surveillance in modern society takes form. Foucault recognises a few characteristics of the Panopticon prison that are essential for its functioning. The major function recognised by Foucault is:

> 'to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power. So to arrange things that the surveillance is permanent in its effects even if it is discontinuous in its action; that the perfection of power should tend to render its actual exercise unnecessary; that this architectural apparatus should be a machine for creating and sustaining a power relation independent of the person who exercises it; in short, that the inmates should be caught up in a power situation of which they themselves are the bearers.'[36]

Although Foucault never mentioned the Panopticon with regard to the internet, Lyon recognises several traits of the Panopticon that are reinforced by electronic surveillance, notably the invisibility of the inspection and its automatic character.[37] The Panopticon derives its power from the accumulation of information and the direct supervision of subordinates. As a result, a 'normalizing discipline' from the prisoners is derived. Prisoners exhibit 'anticipatory conformity', showing the behaviour that is deemed appropriate.[38]

With regard to internet regulation, Boyle proposes a model of 'privatised Panopticons' in his article 'Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors'.[39] The model seeks to decentralise multiple instances of the Panopticon. It is based on the notion of implementing the regime into the architecture to avoid the need for policing after the fact.[40] The privatised Panopticons are responsible for what happens on their part of the network, resulting in a high degree of self-regulation.

This chapter has shown why attempting to control the internet could pose a problem to the Chinese government. Before we continue to discuss how the government can control the internet, the following chapter will first provide some basic information about the internet in China. Subsequently, this thesis will describe how the four modalities of Lessig are put into practice for the case of China and how they help control the internet. This thesis will also show how and which characteristics of the concept of the Panopticon are implemented in the structure of the internet in China, as a means for control.

[36] Foucault, Michel, *Discipline and Punish: the Birth of the Prison.* Harmondsworth: Penguin Books, 1977. p.201.
[37] Lyon, "From Big Brother to Electronic Panopticon," http://www.rochester.edu/College/FS/Publications/Lyon.html
[38] ibidem
[39] Boyle, "Foucault in Cyberspace," http://www.law.duke.edu/boylesite/fouc1.html
[40] ibidem

3. The Internet in China

This chapter will provide information about the origin and history of the internet in China. First, we will take a look at the incentives for the Chinese government to develop the internet, even if the internet is supposedly hard to control.[41] Most literature only mention the economic benefits the internet can offer.[42] This one-sided perspective overlooks other advantages the internet can offer to China and its government.

Secondly, we will give an introduction to the role of the media under Chinese communism and show how this role has changed since the Open Door Policy in 1977. With the introduction of the internet, a lot of changes were made in the structure of the Chinese government, and therefore the different ministries and government bodies with regard to the internet and their responsibilities are discussed. Lastly, we will provide some information about the development of the internet in China. A short overview of the history of the internet infrastructure in China will be given. Furthermore, the demographic characteristics of the current internet users will be explored and the use of the Chinese language on the internet
.

3.1 How the Internet can Benefit China

> "The new technological revolution or information revolution ... may help China skip over some of the stages which have been experienced by other developing countries"[43] (former premier Zhao Ziyang, 1983)
>
> "We should … recognise the tremendous power of information technology and vigorously promote its development. The melding of the traditional economy and information technology will provide the engine for the development of the economy and society in the 21st century."[44] (Jiang Zemin, August 2000)
>
> "None of the four modernizations would be possible without informatization."[45] (Jiang Zemin)

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. China's interest in the Information Revolution has been stated by a wide array of government and party officials starting in the 1980s. It gained strong support because both conservatives and reformers agreed that this 'class neutral technology' was needed to close the gap with both its Asian neighbours and the Western world.[46]

[41] The Chinese government could have spared itself a lot of problems by forbidding access to the internet, a measure the Taliban in Afghanistan for example has taken. See "Afghanistan's Taliban Bans Internet" *Yahoo* (13 July 2001), http://dailynews.yahoo.com/h/nm/20010713/wr/tech_afghan_internet_dc_1.html

[42] Articles that only mention the economic advantages of internet see Earnshaw, Graham, "China Online," *Brill's Content*, February 2001, http://www.brillscontent.com/2001feb/columns/next.shtml or
Pfaffenberger, Bryan, "The Internet in China," 22 november 2000, http://noframes.linuxjournal.com/articles/currents/0024.html

[43] Zhao Ziyang in Hamrin, Carol Lee*, China and the Challenge of the Future*. San Francisco: Westview Press, 1990. p.213. Quoted after Taubman, "A Not-So World Wide Web," p. 262

[44] Jiang Zemin in a speech at the World Computer Congress 2000 in Beijing, quoted after Lin Neumann, A., "The Great Firewall," *Committee to Protect Journalists* (January 2001), http://www.cpj.org/Briefings/2001/China_jan01/China_jan01.html

[45] Jiang Zemin's slogan can be found on the preface of a book series on informatization. See *Xinxihua Congshu* (Book Series on Informatisation), Beijing: Jinghua Chubanshe, 1998. Quoted after Yuezhi Zhao and Dan Schiller, "Dances With Wolves? China's Integration into Digital Capitalism," *Info,* Vol.3, No. 2., April 2001. p.5.

[46] Taubman, "A Not-So World Wide Web," p. 262

E-government

县官不如现官 “The County Magistrate is not as powerful as the official on the spot.”

The impact of the internet on the organisation of the government itself is usually overlooked with all the attention on the democratic effect and the economic impact of the internet. The Chinese government recognised early on the potential of e-government for streamlining its organisation.[47] 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.’[48]

Policies in China are enforced with more strength at the centre than at the periphery. This is based on geographical distances and inherent in the political structure of the Chinese government, which has both a horizontal and vertical hierarchical structure.[49] The internet is a continuation of a long-standing tradition of using telecommunications to strengthen central control over the local authorities.[50] In 1993, the first of the so-called Golden Projects were launched. These Golden Projects are the name for the initiatives of the government with regard to the internet. The objectives are threefold:

1. to build a national infrastructure as a way to national modernization and economic development
2. to stimulate the development of information technology in China
3. to tighten the administrative structure, both horizontally (across ministerial lines) and vertically (from the centre to the periphery)

Originally starting out with three Golden Projects, the number has grown steadily over the years as more plans were initiated. Although the Golden Projects look good in theory, in practice they did not always work the way the central government intended. In the case of the Golden Customs project, which had the objective of linking and centralising all the customs in China, the very same target group hampered developments.[51] The local officials had no incentive to change or surrender (part of) their autonomy. It is exactly from the lack of centralised control and of standardised processes that the local officials derive their power.[52] Regionalisation can be detrimental in implementing projects that aim to strengthen central authority, because of conflicting interests.

The central government is experimenting with the internet to become more transparent, needed to attract foreign investment and a requirement for entry to the World Trade Organisation (WTO). It wants to use the internet to battle corruption, considered a big problem that weakens transparency and undermines the central authority. An example is how the State Council and MII are considering using online auctions for procurement to raise efficiency and transparency.[53] To appreciate the changes in transparency, one only has to look at Chinese regulations that used to be confidential. Regulations were generally unpublished

[47] For a comprehensive discussion of China’s E-Government initiative, see Zhang Junhua, “China’s “Government Online” and Attempts to Gain Technical Legitimacy,” *Asien* (Juli 2001) 80.

[48] Deloitte & Touch, *At the Dawn of E-government: the Citizen as Customer*, http://www.us.deloitte.com/PUB/egovt/egovt.htm p1.

[49] For an excellent description of the political system in China, see Lieberthal, Kenneth, *Governing China: From Revolution Through Reform*. New York: W.W. Norton, 1995. pp.155-240.

[50] Westland, Christopher, “China’s Golden Projects,” *Global Electronic Commerce*, The MIT Press, 2000, http://www.itheadline.com/feat_art/FA8/china_golden.htm

[51] Kevan Bradshaw and Ken DeWoskin, “The Internet in China,” PriceWaterhouseCoopers, http://www.pwcglobal.com/extweb%5Cnewcolth.nsf/docid/2B48471E81BEB97B85256959006A8E34?OpenDocument

[52] ibidem

[53] Hsieh, “A Cure for Corruption?,” *Asiaweek* (30 June 2000), http://asiaweek.com/asiaweek/technology/2000/0630/tech.b2b.html

and not available to the public. They are now published on the internet and available to anyone interested.[54]

Propaganda

The internet, in its function as media, is seen as an important playing ground for propaganda. The Internet Propaganda Administrative Bureau, responsible amongst others for guiding and coordinating the Chinese content web sites, was formed in April 2000. The strategy is to produce own content (*Xinhua News Agency, People's Daily*) and limit other news sources.[55] Chinese websites do not have an option but to copy most of the news articles from the official sources. For example, portals, such as *Sina* and *Sohu*, have partnerships with Western media companies Dow Jones and Reuters, but both stopped publishing non-financial news after a warning from the central government. The three big portals (*Sina, Sohu, Netease*) all stopped carrying news sources that were not officially state-sanctioned, fearing to lose their license. An example of an active propaganda policy is the Chinese website for Human Rights that sets out the government's human rights policy.[56] Another example is the state-run website that criticises the Falun Gong.[57] Sometimes it even seems that the Western media is an extension of Chinese propaganda. The Western media blatantly copy news from the official state-sanctioned news websites, such as *Xinhua* and *People's Daily*, because it is so easy to pick it up from their websites.[58]

3.2 The Changing Role of the Media in China

The function of media under Chinese communism is different from the function of media in Western democracies. Media under communism and especially under Chinese communism are regarded as an essential political instrument. The media should function under the Party's apparatus and are responsible for educating the masses and disseminating ideology. Ideology as defined by Schurmann is a "systematic set of ideas with action consequences serving the purpose of creating and using organisation."[59] The function of media is thus to ensure the loyalty and unity of the organisation's members, to induce not only correct thinking but also correct behaving. The Party is the owner, the manager and the practitioner of the media. However, since the introduction of the Open Door Policy in 1977, China has gradually opened up to the West. The role of the media has changed and according to Lynch, three factors (administrative fragmentation, property-rights reforms and technological advance) are responsible for the changes in thought work.[60]

First, administrative fragmentation granted cadres in the provinces and lower levels of administration more freedom in decision making in thought work activities during the 1980s. The reason was that the local authorities had better access to higher quality information from

[54] For example, all regulations concerning telecommunications and internet are available at the website of the MII, see http://www.mii.gov.cn/mii/zcfg.html (in chinese)
[55]"江泽民强调互联网要成为思想政治工作新阵地,"(Jiang Zemin Stresses that the Internet Must Become a New Playing Ground for Propaganda Work) *Sina* (11 January 2001), http://tech.sina.com.cn/i/c/49699.shtml
[56] see http://www.humanrights-china.org/
[57] see http://ppflg.china.com.cn/indexE.html
[58] Crampton, Thomas "Beijing Uses Cyberspace to Widen Control," *International Herald Tribune* (24 March 2001),
http://www.iht.com/cgi-bin/generic.cgi?template=articleprint.tmplh&ArticleId=14484
A good example is the Dutch ANP Nieuws, that copies news from the official state media in China. These ANP news items then are copied by the newspapers again.
[59] Schurmann, Franz, *Ideology and Organisation in Communist China*. Berkeley: University of California Press, 1966. p.18.
[60] Lynch, Daniel, *After the Propaganda State: Media, Politics and "Thought Work" in Reformed China*. Stanford, CA: Stanford University Press, 1999.

the local public and a better flow of information was needed to develop the economy.[61] The central government anticipated at that time that a division could be made between commercial information and propaganda, which the central authorities still wanted to retain control over. This is similar to the way the central government is attempting to separate political and non-political information on the internet.

Secondly, the property-rights reforms started in the 1990s. They had a profound effect on most state-owned enterprises, including the media industry. This did not and still does not mean that a full-blown privatisation of the media and telecommunications firms occurred. The media and telecommunications firms still officially belong to the party-state. For example, *Xinhua News Agency* still belongs to the State Council, and China Telecom to MII. However, the reforms granted firms the rights to income and the managers the rights of control.[62]

The third and last determining factor to spur the changes in the role of the media was technological advance, mediated by the administrative fragmentation and the property-rights reforms. One of the reasons the Chinese government failed in adapting the new role of the media was that they lacked the information and expertise to manage the new technologies effectively.[63] Satellite television is a well-known example of a technology the government did not quite know how to deal with. Privately owned satellite dishes were initially banned but the government ended up allowing them because the central government found it impossible to enforce the ban. Rupert Murdoch saw opportunities in this market and boldly proclaimed in 1993 that satellite television was 'an unambiguous threat to totalitarian regimes everywhere', remarkably similar to libertarian claims that are made for the internet.[64] He bought a majority stake in StarTV in July 1993 and started offering the BBC World Service Television next to entertainment, sports and music channels. However, in 1994 the BBC was taken off StarTV in an effort to appease the Chinese government and not until January 2001, after years of strained relations, was BBC World allowed again.[65] Even more striking is the change of attitude of Hong Kong TV stations. Over the years, they stopped broadcasting anything that might offend the government in Beijing after they realised they could reach the massive and commercially attractive Chinese market.[66] Self-censorship out of commercial interest is, as we will see, quite common for companies in Hong Kong and China.

Increasing commercialisation forced the media organisations to learn to become financially self-sufficient. Thus, a shift to more audience-oriented content was inevitable as the media organisations turned to advertising as their major source of income. Since the government only was able to churn out boring content, the media increasingly turned to foreign imported content to please the audiences, exposing them to new – foreign – images and ideas. This globalisation of thought work was further spurred by the advent of new distribution channels enabled by new technology such as satellite dishes, fax machines, mobile phones and the internet. Distribution channels of media proliferated and as a result, the Chinese people are no longer solely dependent on the official government media channels. The organisations responsible for media content became increasingly more independent and were able to offer a wide array of content next to the official government channels.[67] What concerns the central

[61] idem, p. 30

[62] idem, p. 41-42

[63] idem, p.9

[64] Earnshaw, Graham, "China Online," *Brill's Content* (February 2001), http://www.brillscontent.com/2001feb/columns/next.shtml

[65] Gittings, John, "Deal Clinched as BBC and China Make Up," *Guardian Unlimited* (10 January 2001), http://www.guardian.co.uk/china/story/0,7369,472355,00.html

[66] See the 1998 Human Rights Report of Hong Kong for more details, available at http://www.state.gov/www/global/human_rights/1998_hrp_report/hongkong.html

[67] A side note to keep in mind: the internet seems to be on its way to transform traditional media. The internet is converging the traditional media with telecommunications and this development could make it possible for the government to retain control over media as it is easier to control just one instead of multiple distribution channels.

government most is that because of the pluralisation, the signal-to-noise ratio has gotten worse. It becomes much harder for the central government to get their message across in the midst of all the so-called noise.

3.3 The Regulatory Regime with Regard to the Internet

> "The power struggle among government agencies over who will supervise what on the Net has been brutal"[68] (Time, February 2000)

For a number of years, since the emergence of the internet, it remained unclear which ministry would be responsible for the internet. A power struggle erupted between the former Ministry of Posts and Telecommunications (MPT) and the former Ministry of Electronics Industry (MEI) over control of the lucrative internet. In order to control the struggle, the Ministry of Information Industry (MII) was constructed as a super ministry. Tan recognises three different stadiums of the regulatory regime in China, what he calls "the past, the transitional and the future."[69] The past regime, from before 1994, was characterised by its fragmented structure. The transitional regime, between 1994 and 1998, was represented by the State Council's Steering Committee of NII (National Information Infrastructure), a single regulatory coordinator that held no true power due to its lack of legislative power, financial means and political backing.[70] The future regime is characterised by the MII.

The past regime had trouble formulating a coherent set of regulations for the internet since all parties involved held different interests. This stifled the development of the internet. Because rival bodies were not capable of working together, the State Council created the National Joint Conference on State Economic Informatisation in 1994, later re-organised into the Steering Committee of NII in 1996.[71] The Steering Committee was seriously handicapped in its decision-making power, as it did not hold final responsibility. It was forced to negotiate with all the parties, as implementation would still lie with the government bodies involved. The Steering Committee did manage to formulate regulations, notably the Internet Provision Regulations and the Domain Name Registration.[72] The new regime was initiated in March 1998, when an ambitious reform was started and China's 9th National People's Congress accepted the formation of the MII. The MII is primarily responsible for the 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 informatisation.[73] Wu Jichuan, former head of the MPT, was elected as the head of the MII in March 1998.[74]

Various other ministries and government bodies have an influence with regard to the Chinese internet policy as well, some of the more important ones are mentioned here.[75] The Ministry of Public Security (MPS) is responsible for network security. It looks after abuse of the network, i.e. the leak of state secrets, political subversion or the spread of pornography or hatred. It has the legal rights to monitor network traffic. The Ministry of State Security (MSS)

Imagine IP telephone, television, newspapers, fax, unified instant messaging, your tax form, all by way of the internet.

[68] "China's Net Commandments," *Time Asia* Vol. 155 No. 8, http://www.time.com/time/asia/magazine/2000/0228/cover.regulation.html

[69] Tan, "Regulating China's internet," *Telecommunications Policy* 23 (1999) p. 265

[70] ibidem

[71] idem, p.266

[72] For the original Chinese texts of these regulations, a complete overview of all regulations is available at the website of the MII, see http://www.mii.gov.cn/mii/zcfg.html

[73] see appendix for a complete overview of the responsibilities of the MII

[74] Five vice-ministers were chosen from the MPT and MEI. The former MPT faction slowly gained the upper hand, reflected in the fact that in the MII about 230 former MPT staff members reside, as compared to 80 from the former MEI. See Foster and Goodman, *The Diffusion of the Internet in China,* p 136.

[75] For a complete table of key government bodies with regard to the internet and their functions, see appendix 2.

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 unauthorised people.[76] Furthermore, the China Internet Network Information Center (CNNIC) is responsible for the registration of domain names and the distribution of IP addresses. [77] Other important bodies are the Sate Council Information Office and the Propaganda Department that work closely together and oversee much of the internet content policy.

The converging characteristics of the internet caused some confusion in the beginning. The lack of clarity which department would be responsible for the internet was the cause for a power struggle. The main struggle between the MPT and MEI was solved by forming the MII as part of a converging regime for the internet. However, other government bodies besides the MII also have a say in certain parts of the internet policy. This can be detrimental in striving for a coherent and clear regime for the internet.

3.4 The Development of the Internet in China

> 越过长城，走向世界 “Crossing the Great Wall to join the world”[78] (the subject of the first email sent in China by Qian Tianbai , 1987)

The development of the internet infrastructure in China commenced in academic and scientific circles, as in most other countries. The first computer network was the China Academic Network (CANET). It was set up in 1987 to provide support for academic and scientific research in computer science; the staff had access to email facilities. Other academic networks soon sprung up, amongst others the network of the Institute of High Energy Physics (IHEP) and the China Education and Research Network (CERNET). These earlier networks all shared the same inconvenience: they had no direct connection to the internet. The US government still regulated the internet and forbade any socialist country access.[79] This changed in April 1994, when the appeal for direct linking to the internet was accepted during the Sino-American Federation of Scientific and Technological Cooperation meeting in Washington DC. The first network directly connected to the internet became active when the National Computing Facilities of China (NCFC) project opened up a dedicated circuit to the internet through Sprint Corporation on 20 April 1994.

The year 1995 proved to be a turning point.[80] The development of the infrastructure really took off after commerce on the internet was introduced. In May 1995, the MPT and China Telecom set up the first commercial network, ChinaNet. In 1997 and 1998, discussions started on whether to allow competition on the national infrastructure. One of the issues was how efficient it would be to have the government finance all the infrastructure on a national scale. China Telecom argued that it would be very hard to ensure national security if more companies entered the market. Those who supported competition pointed to the example of the China Golden Bridge Network (ChinaGBN) whom many believed forced China Telecom to invest, deploy and offer new services by threatening to lock in new customers.[81] The issue was resolved by allowing competition but requiring these new companies to connect with China Telecom for traffic outside China. The State Council approved Unicom as an Interconnecting Network early 1998. Unicom is under the control of the MII and is seen as a

[76] Definition of encryption, see http://whatis.techtarget.com/definition/0,289893,sid9_gci212062,00.html

[77] The origin of the acronym is unknown to me, as it does not reflect the first letters of the long title. However, everybody knows what you are talking about when you mention the CNNIC.

[78] The title of the first e-mail sent within China. The email was sent by Qian Tianbai on 20 September 1987 and marked the beginning of the use of internet in China.

[79] Evolution of internet in China, http://www.edu.cn/english/cernet/net/introduction/intro_05.php

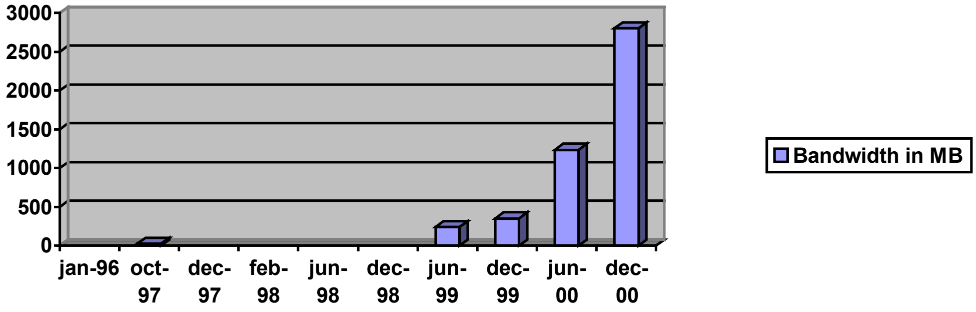
[80] For a good description of the state of the internet in China before 1995, see Cindy Zheng, “Opening the Digital Door,” *Telecommunications Policy* 18 (1994), pp.236-242. One of the obstacles she describes is the US export restrictions on technology.

[81] Foster and Goodman, *The Diffusion of the Internet in China*, p. 19

counterweight to the former monopoly of China Telecom. Netcom gained approval to function as an Interconnecting Network a year later, bringing the total of IN in China up to six. China Netcom's board of directors include Jiang Mianheng, son of president Jiang Zemin, ensuring political support.[82] As of 2001, nine networks received approval from the State Council to offer Internet services.[83]

Bandwidth

> "You can never have too much bandwidth in your country."[84] (Thomas Friedman)
> "Enlightenment can flow through the taps like water."[85] (Edward Tian, CEO of Netcom, on the effect of superfluous bandwidth)



(source: CNNIC reports, available at http://www.cnnic.com.cn)

Bandwidth is the amount of data traffic per second the network can process. Enough bandwidth is essential for a network to be able to work fluently. It should be pointed out that the Chinese government could exert larger control over the internet by limiting bandwidth, an option some authoritarian governments have chosen.[86] This is not the case with the Chinese government that instead chooses to stimulate the use of the internet.[87] In the latest CNNIC report, the total internet bandwidth is listed at 2.8 Gbps, which is almost twenty times more

[82] idem, p. 20
[83] Hartford, "Cyberspace with Chinese Characteristics," http://www.pollcyber.com/ch/pubs/home.htm pp.13-14.

- CERNET – China Education and Research Network, overseen by the Ministry of Education, for schools and research institutes
- CSTNET – China Science and Technology Network, overseen by Chinese Academy of Sciences, for scientific research institutes, some government enterprises and state enterprises
- ChinaNET – operated by China Telecom under MII (former MPT), for general public
- ChinaGBN – China Golden Bridge Network operated by Jitong Co. under MII (former MEI), for general public
- UNINet – operated by China Unicom, aimed at SME (Small Medium Enterprises).
- CNCNet – operated by China Netcom, heavily involved in broadband services.
- CMNet – operated by China Mobile (spin-off from China Telecom)
- CGWNet – planned by China Great Wall Communications.
- CIETNet – China International Economics and Trade Net, no other information yet available.

[84] Friedman, *The Lexus and the Olive Tree*, p.199.
[85] Sheff, David, "Betting on Bandwidth," *Wired* 9.02 (February 2001), http://www.wired.com/wired/archive/9.02/tian.html
[86] Myanmar and Cuba are governments that limit bandwidth in order to control the internet. See Mai Jiesi (迈杰斯)，"各国政府能否控制互联网," (Whether Each Country Can Regulate the Internet), http://bbs.huanet.com/fanfubai/91.shtml
[87] A big problem was that traffic within China was often routed to the United States and back because of congestion (limited bandwidth) in the Chinese network. This was not resolved until October 1998 when China got its first Internet Exchange that linked the four INs together. See The Global Information Technology Assessment Group, *The Global Diffusion of the Internet Project: Asian Giants On-Line*, Chapter 4. P126. http://mosaic.unomaha.edu/Asian_Giants_China.pdf

than in 1999.[88] Future plans are even more ambitious. According to CNNIC director Qian Hualin at the Chinatech Conference (January 2001), the ChinaNet network of China Telecom is about to be upgraded to 3.3 Gbps in 2001.[89] This alone caps the whole current bandwidth of China of 2.8 Gbps.

Duncan Clark states that the concern is not a shortage of bandwidth, but that it might have too much bandwidth.[90] Although that is an overstatement, it shows that the government is concerned about bandwidth limitation curbing internet development.[91] The Chinese still complain about the speed though: 46,41% of the internet users in the latest CNNIC report of January 2001. However, compared to the 88,9% of the internet users in the CNNIC report of July 1998, it is a vast improvement. The Chinese government is doing a credible job in maintaining the growth of bandwidth with the growth of the internet users, although there is still a lot that can be improved.

Internet Users

"Connectivity is now productivity"[92] (Thomas Friedman)
"Power to the People"[93] (slogan of a NetEase advertising campaign)

The internet population amounts to roughly 20 million according to the CNNIC report of January 2001.[94] These statistics are unfortunately notoriously inaccurate and several other companies that specialises in market research, notably IAMAsia and NetValue, contest these statistics, both counting a few million users less. Nonetheless, the enormous growth is

[88] The current network of 2.8 Gbps is built with over 820 thousand kilometers of fibre-optic cable. For an extensive overview of the development of bandwidth in China, see Foster and Goodman, *The Diffusion of the Internet in China*, p.57

[89] Presentation of Qian Hualin, "Internet Development in China," http://www.chinatech.org/Library/QianHualin.ppt

[90] Clark, Duncan, "BDA: Bandwidth Growth Turns Spotlight on Censorship Threat," (30 January 2001) http://www.bdaconnect.com/news/bb_2001_01_31/

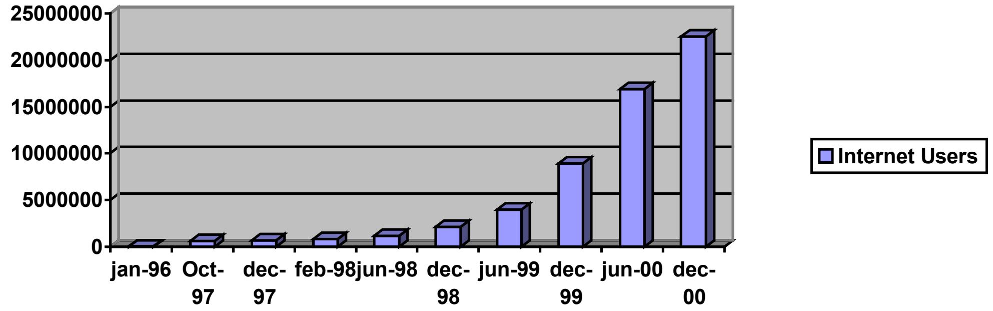
[91] The development of bandwidth in China was even outgrowing the growth of internet users in the second half of 2000, meaning the average bandwidth per internet user is increasing. See Qiu, Jack Linchuan, "Internet Censorship in China (1999-2000)," *Communications Law in Transition Newsletter*, http://pcmlp.socleg.ox.ac.uk/transition/issue2_3/qiu.htm

[92] Friedman, Thomas, *Lexus and the Olive Tree*. London: Harper Collins, p199.

[93] Yang, Dali L., "The Great Net of China," *International Harvard Review* winter 2001, also available at http://www.mfcinsight.com/article/010209/oped4.html

[94] The CNNIC reports are available at http://www.cnnic.com.cn/develst/e-index.shtml

undeniable.[95] In January 2000, the CNNIC report counted 8.9 million internet users and in July 2000 16.9 million internet users.



(source: CNNIC reports, available at http://www.cnnic.com.cn)

To put things in perspective, 20 million internet users still only account for about 1.5% of the whole Chinese population. Not all 1,3 billion people will go online anytime soon, but in the short term, further growth is very likely. PC penetration per urban household in China is about 5% and while this is relatively low, it provides sufficient room for further growth of the internet in China.[96] The Chinese government is also stimulating further growth by slashing its internet fees in order to stimulate competition between the providers.[97]

Internet users are not representative for China on the whole. Users aged 18 to 35 account for almost 70% of all the internet users, and most of these hold a bachelor degree. The internet is mainly diffused over the three big cities, Beijing, Shanghai and Guangzhou. By the end of 2000, only 0.76% of the internet users came from rural areas that happen to hold 80% of China's population. Male users make up 69,56%, an improvement over July 1998 when male users accounted for 92,8%. The image of the typical internet user (male, highly educated, high income, living in the big city and of middle age) is gradually reversing, meaning the internet is starting to become popular.[98]

[95] One of the reasons that make counting difficult is that an internet account is usually shared by more than one person. See Narayan, Anita, "IAMAsia's Net Survey Contest Official Figures," *ChinaOnline* (11 January 2001), http://www.chinaonline.com/topstories/010111/1/C01011151.asp and "Statistics on Net use are Suspect," *ChinaOnline* (17 April 2001), http://www.chinaonline.com/issues/econ_news/NewsArchive/secure/2001/April/C01041852.asp

[96] Report of Legend on PC industry in China available at http://www.legend-holdings.com/eng/research/archive/prc092500c or see Hartford, Katherine, "Building China's Information Technology Industry," http://www.pollycyber.com/pubs/hapr/infochina.htm

[97] "China Cuts Internet Access Fees to Spur Online Growth," *ChinaOnline* (26 October 1999), http://www.chinaonline.com/industry/infotech/NewsArchive/Secure/1999/october/C9102207.asp and "If You'd Like to Make a Call, China Announces Massive Cuts in Telecom, Net Fees," *ChinaOnline* (26 December 2000), http://www.chinaonline.com/topstories/001226/1/C00122206.asp

[98] Celebrities who offer to teach net lessons further show the popularity and there is even a miss Internet contest. "China Celebs Offer Net Lessons," *Wired* (26 September 2000), http://www.wired.lycos.com/news/culture/0,1284,39023-2,00.html and for Miss Internet contest see http://www.ctc.org.cn/ctc2/contest/miss/album/index.htm

The Chinese Language on the Internet

> "Think Global, Interact Local"[99] (slogan of a marketing campaign for Tridion, a company for content management software)

We will discuss how language makes control easier by raising barriers to access of information. First, problems with Chinese characters on the internet are described. Secondly, we will explore how the English language works as a deterrent to access of information.

The internet was designed with the ASCII set in mind. However, the ASCII set is insufficient for Chinese characters because the ASCII set can only contain 128 possible characters.[100] The Unicode standard addresses this problem and allows for 34.168 possible characters. Unicode is supposed to be a system for "the interchange, processing, and display of the written texts of the diverse languages of the modern world."[101] Unfortunately, most software are not always compatible with Unicode. Development of Chinese language communication over the internet did not really start until the mid 1990s. Due to political reasons, cooperation between Taiwan and China was limited and development hindered. Various different sets of character encoding were developed and used throughout the years, but as of now the GB encoding set for simplified characters (China) and the Big5 encoding set for the traditional characters (Hong Kong, Taiwan) are fairly standard.

The different encoding standards set a barrier for communication. People accustomed to reading simplified characters will not have the same convenience and fluency reading traditional characters. This will not cause a problem where only passive knowledge is required, because the context usually provides ample room for interpretation. The different encoding standards do explain what Buruma thinks is a 'puzzling' development: two Chinese internet users resorting to the use of English to communicate.[102] Besides the different character sets, each region also has its own translations and lingo.[103] Acronyms differ and form a language barrier.[104] Another development that makes the Chinese language on the internet hard to comprehend is the words that are created out of typing errors.[105]

The English language is a barrier for active *and* passive access to non-Chinese information. An IDC research pointed out that Asian web surfers prefer content in their own language, as opposed to content in English, the lingua franca on the internet.[106] This is easily explained as

[99] See http://www.tridion.com/news/pressreleases/file_263620010410125624.asp

[100] There are (obviously) more than 128 Chinese characters. For a definition of ASCII, see http://whatis.techtarget.com/definition/0,289893,sid9_gci211600,00.html

[101] Definition of Unicode, see http://whatis.techtarget.com/definitionsSearchResults/1,289878,sid9,00.html?query=unicode

[102] Buruma, Ian, "China in Cyberspace," (4 November 1999), http://www.nybooks.com/nyrev/WWWfeatdisplay.cgi?19991104009F#top

[103] For example, the word for e-mail can be translated either as electronic mail in Chinese (dianzi youjian 电子邮件) or phonetic as yi-mei-r（伊妹儿）However, the phonetic version of e-mail is only used on the Mainland, and not in Taiwan and Hong Kong. In Hong Kong the characters for the phonetic version of e-mail would come out totally different as the de facto language is Cantonese, which has a different pronunciation of characters.

[104] Examples of acronyms solely used on the Mainland are MM (meimei 妹妹) and GG (gege 哥哥). Another form of acronym used only on the Mainland is the use of ciphers as opposed to letters, for example 886 (ba-ba-liu) means bye-bye 拜拜 and 7456 (qi-si-wu-liu) stands for 'qi si wo le'气死我了 – "it's driving me crazy."
For a list of popular words used in BBS, see "BBS 行话," (BBS Jargon), http://member.netease.com/~hisen/cyberhumor/culture/bbsjargon.htm
and "网络魔鬼辞典," (The Devil's Dictionary of the Internet), http://culture.163.com/edit/000802/000802_40082.htm

[105] The most common example on the BBS is the word for 'moderator', which is in Chinese 版主, but often 斑竹 is used because that is the first combination that appears when you type in the pinyin 'banzhu'.

[106] Bonisteel, Steven, "Asian Surfers Prefer Native," (6 November 1999) http://www.computeruser.com/newstoday/99/11/06/news6.html

English literacy is not widespread. Although the current Chinese internet population is relatively highly educated, the language barrier still prevents them from widely accessing foreign news sources and interacting with foreign internet users. Users need to be fluent in written English to be accepted in foreign communities.[107] Content in English is a natural barrier already, and the government only magnifies this effect by blocking websites deemed undesirable. The government also actively provides Chinese content as part of its propaganda policy. More users are getting satisfied with the amount of Chinese content available.[108] A lot can also be attributed to the arrival of two new portals in 1999, *Sina* (March 1999), and to a lesser degree *China.com* (May 1999). *Sina* has been the most popular portal since its debut in 1999 and also happens to be the only popular portal that offers its content in simplified characters, traditional characters and English.

The Chinese language on the internet has different standards that make it difficult for Chinese users across the Strait to interact. While most of the websites on the internet are still written in English, English literacy among Chinese internet users is low. There is a high demand for local content in Chinese. The Chinese government uses this to its own advantage and is responsible for providing most of the content of the portals.

[107] For an excellent study on the culture of the internet and Usenet, see North, Tim, *The Internet and Usenet Global Computer Networks: An Investigation of Their Culture and Its Effect on New Users*. MA Thesis. http://www.vianet.net.au/~timn/thesis/chap5.html

[108] According to the CNNIC surveys, the percentage of users discontented with the amount of Chinese content available in 1998 and 1999 was over 45%, but this decreased to 9% in 1997 and in the last survey conducted in January 2001, this percentage was reduced to 6,41%.

4. Control of the Internet in China

In this chapter, we will examine how the four modalities of control, as set forth by Lessig, function with regard to the internet in China. We will examine how the law, architecture, social norms and the market are used to control the internet, and how the concept of the Panopticon is employed to use the internet as a means for control.

4.1 The Law

"You make a problem for us, and we'll make a law for you."[109] (unnamed Comrade X)

Differences in definitions between Western and Chinese regulations can cause confusion. Western literature discussing internet regulation usually recognises a few roles with regard to their function in the network. Distinction is made between an Internet Access Provider (IAP), Internet Service Provider (ISP) and Internet Content Provider (ICP). However, the Chinese regulations use other legal definitions. The 1997 implementation of regulations makes a distinction between Interconnecting Networks 互连网络 (IN) and Access Networks 接入网络 (AN). An IN can be compared to a backbone provider, while an AN is comparable with an Internet Access Provider. An AN needs to connect to an IN to access the internet. These differences in terms can cause some confusion when Western concepts are used to translate the Chinese legal terms while they do not necessarily have the same meaning.

The internet in China has been unregulated during its first years. The government waited until the mid 90s with drafting laws to regulate the internet. Regulations concerning internet control can be divided in roughly three different categories, those that:

- govern the network infrastructure and international network connections
- handle illegal activities related to the internet
- deal with monitoring organisations 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). This regulation was formally announced on 1 February 1996 and verified on 20 May 1997. Article 6 of the Temporary Regulation provides that "all direct international networking traffic must use international incoming and outgoing channels provided by the national public network of the MPT."[110] This means that every bit of traffic that comes from foreign servers must pass through the network of the former MPT (now MII), making it easier to monitor the traffic.

[109] Geremie R. Barmé and Sang Ye, "The Great Firewall of China," *Wired* 5.06 (1997), http://www.wired.com/wired/5.06/china_pr.html

[110] Cullen and Choy, "The Internet in China," 13 *Columbia Journal of Asian Law*, p.120

The Temporary Regulation also specifies the illegal activities related to the internet. This includes publishing information that incites hatred, viruses and subversive acts to overthrow the state. It is important to note that these regulations itself are not unreasonable. For example, state subversion and endangering national unity are illegal in every other country. The difference lies in the interpretation of the law that can be quite arbitrary in China. The most noteworthy rule is the leak of 'state secrets', a term so vague that it can be interpreted in multiple ways. Because of its arbitrary character, the leaking of state secrets has been often used as a pretext for detaining people.[111] Ambiguity in law thus is very useful in terms of control.[112]

The MPS, responsible for network security, issued regulations that require users to register with the MPS (January 1996) within 30 days of connection. The second regulation the MPS issued was to strengthen security of computer information networks in December 1997. The regulation furthermore specifies that IN, AN, legal enterprises and institutional internet users are responsible for managing network security, protection and management. Note that there is considerable debate in the West whether ISP should be held responsible for the content transmitted over their network. ISP like to compare themselves to the post office that has no knowledge of what it transports, so therefore they can not be held liable. However, for practical reasons it is much easier to hold the ISP liable, stimulating a high level of self-regulation. This is exactly what Boyle calls the concept of the privatised Panopticons.

The Measures for Managing Internet Information Services (November 2000) specify what kind of information of internet usage needs to be recorded. According to article 14, an AN needs to record the content of the information, the time of release and the name of the website. An AN also needs to record the time the user logged on, the user's account number, the visited websites and the telephone number s/he uses. Records must be kept for a period of 60 days and should be handed over to state authorities upon demand.[113] However, records are not always strictly kept. This is a common problem with internet cafés, and one problem that deeply concerns the authorities. Most internet cafés are generally a bit slack in keeping a strict policy, where you just pay some cash to buy a card and log on. From time to time, the government conducts a crackdown and cafés are closed when information considered harmful is found. The government doesn't hesitate when it does: in the latest crackdown, 6071 internet cafés have been temporarily cut off the internet and 1943 have been shut down.[114]

> "Nobody wants to irritate the government if business is the primary objective"[115] (Tony Zhang, CEO of Chinanow.com)

The basic principle behind the concept of internet regulation in China is "one is responsible for what one publishes." As a result, internet-related companies in China practice a high degree of self-censorship. Self-censorship is necessary in order to gain the trust and cooperation of the government. If not, the government can close the website for a few days as happened to *Sohu* in early 1999, when a pornographic link was found 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'.[116] News portals such as *Sina, NetEase, Sohu* and *Yahoo* therefore try to stay clear from politics in general and focus

[111] Amnesty International, "State Secrets – a pretext for repression, " http://www.web.amnesty.org/ai.nsf/index/ASA170421996

[112] Hartford, "Cyberspace with Chinese Characteristics," http://www.pollcyber.com/pubs/ch/home.htm

[113] As a nice comparison: the Council of the European Union is discussing a **seven years** period of retaining telecommunications data, including e-mail and internet usage. See McAuliffe, Wendy, "Europe: Police Want to Monitor all Net Traffic," *Zdnet* (17 May 2001), http://www.zdnet.com/zdnn/stories/news/0,4586,2761777,00.html

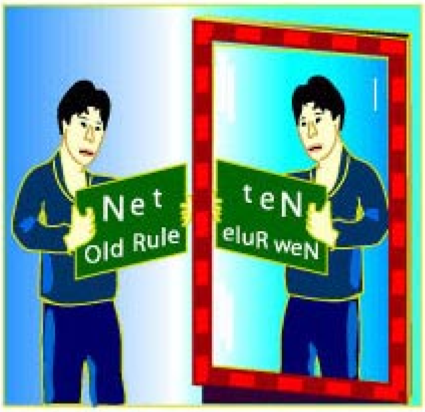
[114] Crampton, Thomas, "China Closes Internet Cafés," *International Herald Tribune* (15 June 2001), http://www.iht.com/cgi-bin/generic.cgi?template=articleprint.tmplh&ArticleId=22928

[115] Earnshaw, "China Online," *Brill's Content* February 2001, http://www.brillscontent.com/feb2001/columns/next.shtml

[116] Hartford, "Cyberspace with Chinese Characteristics," http://www.pollcyber.com/pubs/ch/home.htm

on entertainment and sport instead. Formally, the State Secrets Provisions state that it is forbidden to post any news without proper approval if this news does not come from official state media. It comes down to the fact that the Provisions allow for punishment for those companies that fail to self-censor themselves, a practical development as a result of the decentralised structure of the privatised Panopticons.

4.1.1 Chinese Characteristics of the Law



Graphic by S. Mita

> "Not too many years ago, you needed a license to own a fax machine or a modem in China. I bet those laws are still on the books."[117] (Howard Chao Shang, U.S. law firm O'Melveny & Meyers)
>
> "China does not need to apply any laws – they're already here."[118] (Joe Sweeney)

The enforcement of law in China takes the form of a sine wave. Laws are strictly enforced at first, then after a while the situation relaxes, up till the point where the government feels it needs to issue a warning and the regulations are tightly enforced again.[119] These enforcement swings are best illustrated in the internet café sweeps that occur from time to time to make sure that they adhere to the regulations. These sweeps and other actions are then widely broadcast in state media to maximise exposure. In the context of the Panopticon: these actions are necessary to remind the prisoners that they are being monitored.

To know the law is not sufficient as the law cannot be relied upon as a stable factor. It is more important to have good relationships with the government in order to be able to assess the situation correctly. For example, the Sina office has a direct hotline to relevant officials who help clarify when the policy is unclear and warn in advance on sensitive topics.[120] Thus, companies exhibit anticipatory conformity, showing the behaviour deemed appropriate by the government. A new law therefore does not result in big changes, because companies were already adhering to the government policy. Law codifies what is already common practice.

[117] Lin Neumann, A., "The Great Firewall," *Committee to Protect Journalists* (January 2001), http://www.cpj.org/Briefings/2001/China_jan01/China_jan01.html

[118] Geremie R. Barmé and Sang Ye, "The Great Firewall of China," *Wired* 5.06 (1997), http://www.wired.com/wired/5.06/china_pr.html

[119] Cowhig, "New Net Rules not a Nuisance?, " *ChinaOnline* (December 2000), http://www.chinaonline.com/commentary_analysis/internet/NewsArchive/secure/2000/December/c00120160.asp

[120] Heim, "China keeps firm hand on Net use," *Mercury News* (19 September 2000), http://www0.mercurycenter.com/svtech/news/indepth/docs/china091900.htm.

> "If the regulation does not make sense, they'll change it later"[121] (Steven Xi, CEO of ClubCiti China)

While most laws come as no surprise, the exception to the rule is the Encryption Law of January 2000. When the State Secrecy Bureau initially promulgated the Encryption Law it caused quite some uncertainty. The Encryption Law required individuals and companies using encryption technology to hand in the decryption key to the MPS, so that in case of illegal activities the encrypted message could be decrypted and read. This Encryption Law was received with much scepticism and many found it impossible to comply with the deadline of one month. For example, every browser uses some kind of encryption technology for securing e-commerce transactions. The deadline passed and no one was sure what consequences would follow. The MII re-issued an explanation in March 2000, in which they severely weakened the original intent, restricting it to only a handful of products.[122] Most companies were relieved that the government did not continue its severe stance towards encryption technology. The Chinese Encryption Law was a typical product of the power struggle between government bodies, which explains the resulting confusion.[123]

Intimidation

> 杀鸡给猴子看 "killing the chicken to scare the monkeys" (Chinese proverb)
>
> "The government here [in China] is very good at intimidation"[124] (American newspaper correspondent in Beijing)

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 the Chinese government is very good at. Its goal is to set a 'standard' 标准, so everyone knows which boundaries they should not cross. The government has not hesitated to set examples in order to intimidate the public.

[121] Pappas, "China's internet Syndrome," *The Standard* (21 February 2000), http://www.thestandard.com/article/0,1902,9687,00.html

[122] Marlow, "China Softens Encryption Rules," *ChinaOnline* (14 March 2000), http://www.chinaonline.com/industry/infotech/NewsArchive/Secure/2000/march/C00031430.asp

[123] Pappas, "China's internet Syndrome," *The Standard* (21 February 2000), http://www.thestandard.com/article/0,1902,9687,00.html

[124] Lin Neumann, A., "The Great Firewall," *Committee to Protect Journalists* (January 2001), http://www.cpj.org/Briefings/2001/China_jan01/China_jan01.html

"Lin Hai just wanted to make a buck."[125] (James Ryan)

A good example of intimidation at work has been the case of Lin Hai 林海, an entrepreneur from Shanghai who got arrested and sentenced to two years in prison for submitting 30.000 e-mail addresses to *VIP Reference*, a U.S. based underground pro-democracy newsletter.[126] People were unsure whether Lin Hai was caught because his phone was tapped or because the Chinese government could monitor his e-mail. Lin's case thus alerted Chinese internet users to the fact that the Chinese government is actively monitoring e-mail and that it will not hesitate to take action if they suspect someone is abusing the internet.[127] The uncertainty of being monitored is an important characteristic of the Panopticon.

Lin Hai is considered the first 'internet dissident' in China and gained the attention of the world media.[128] Lin, often portrayed as a political martyr by the Western media, was just hoping to make a few bucks by selling the e-mail addresses. It is ironical that Lin Hai did not act out of political motives but out of commercial interest. The *Digital Freedom Network* website lists nine more known cases of individuals detained for political or religious activities.[129] Among them is Huang Qi, for operating the *Tian Wang* website. Originally a website meant to search for missing persons, the website started to criticise the role of the government in the student massacre, June 4th 1989. Huang was arrested on 3 June 2000, the eve of the 11th anniversary of the repression of the student movement on Tiananmen Square. These examples are intended to intimidate the general public.

4.1.2 Conclusion: Law makes the Panopticon Legal

Several characteristics of the Panopticon can be recognised in the law. First, the law states that all foreign network traffic is required to pass through the gateway of China Telecom. This makes it easier to monitor the traffic. The law furthermore decentralises the responsibility. As a result, content is not double- but triple-checked: at the gateway of China Telecom, at the network responsible for delivering the content, and the receiver itself. Drastic examples, such as Lin Hai and the internet café crackdowns, are set from time to time to remind the people of the fact that they are being monitored.

[125] Ryan, James, "China's Internet: Boon to Reform or Just a Quick Buck?," *Online Journalism Review* (11 February 1999), http://ojr.usc.edu/content/story.cfm?request=159

[126] His two-year sentence is actually fairly lenient considering the fact he has been charged with state subversion, a crime that could result in a sentence of 10 years in prison or even the death penalty. Lin Hai has been released in March 2000, six months shy of his two-year sentence, strengthening the belief that he was indeed used as an example to scare everybody.

[127] Ryan, James, "China's Internet: Boon to Reform or Just a Quick Buck?," *Online Journalism Review* (11 February 1999), http://ojr.usc.edu/content/story.cfm?request=159

[128] Erickson, Jim, "Blocking and Tackling: Is China Cracking Down on internet Activists?," *Asiaweek* (14 August 1998), http://www.asiaweek.com/asiaweek/98/0814/feat1.html

[129] Digital Freedom Network, "Attacks on the Internet in China," *Digital Freedom Network* (24 May 2001), http://www.dfn.org/focus/china/netattack.htm

4.2 Architecture

While the law is based on penalty after the act, the government is also actively trying to implement the regulations into the architecture to prevent the act from happening in the first place. A parallel can be drawn to the concept of the Panopticon that also seeks to prevent the act from happening. This paragraph will seek to examine, clarify and illustrate how the architecture plays a role in controlling the internet in China, and discusses how current countermeasures against control are not effective.

Architecture plays a crucial role in regulating the internet. The code that makes up the internet, both hardware and software, is setting the constraints on what is possible and impossible. The market is a driving force behind the development for the code of the internet. Lessig argues that the market is pushing for code that increasingly erodes the original characteristics of the internet. It becomes easier to know who one is, where one is and what content one uses on the internet.

4.2.1 Control of the Network Infrastructure

There is negative and positive filtering. Negative filtering filters content that is deemed undesirable, for example the CNN website. Positive filtering is the opposite: only the content deemed appropriate is filtered through and accessible, while everything else is inaccessible. Negative filtering takes place through the filters installed at the networks, while positive filtering is what happens in a nationwide intranet.

Negative Filtering

> "Freedom of the press should be subordinate to the interests of the nation. How can you allow such freedom to damage the national interests?"[130] (Jiang Zemin, September 2000)

An important government measure to realise internet control is the control of the main infrastructure: all IN need to connect to ChinaNet from China Telecom if they want to access parts of the internet that are not within China. In other words, ChinaNet controls all network traffic that travels outside China.

It works like this: while you connect to the internet, you cannot access certain sites, for example the CNN website, because the network filters at the packet level.[131] Since traffic has to pass through the gateway of China Telecom and because CNN is blocked at the gateway in an Access Control List (ACL), you will not be able to access the CNN website. It is unknown what the exact list of specified websites is, nor is it known who decides what websites are put on the list. The list is furthermore not centrally controlled; each network seems to implement its own list.[132] This makes it possible that one website is available on one network in China and blocked on another. However, no one can access a website that is blocked at the gateway of China Telecom because it is at the top of the hierarchy of the network structure. Among the websites that are generally blocked are the CNN website, the Voice of America website and the Falun Gong websites. Geocities and Tripod are two examples of very popular services that

[130] Jiang Zemin in an interview with Mike Wallace of CBS in Beidaihe, China on 15 August 2000, quoted after Lin Neumann, A., "The Great Firewall," *Committee to Protect Journalists* (January 2001), http://www.cpj.org/Briefings/2001/China_jan01/China_jan01.html

[131] There are two levels to filter: at the packet level and the application level. See for a detailed technical explanation: Philip McCrea, Bob Smart and Mark Andrews, *Blocking Content on the Internet: a Technical Perspective*. http://www.cmis.csiro.au/projects+sectors/blocking.pdf June 1998.

[132] Internet Censorship Project, "The People's Republic of China," (1998) http://www.soros.org/censorship/eastasia/china.html

provide free opportunity to have an anonymous homepage.[133] Because the website of underground newsletters, such as *Tunnel* and *VIP Reference*, reside on Geocities, the whole range of websites on Geocities is blocked.[134]

Positive Filtering

The internet can also be controlled by positive filtering through a nationwide intranet. A nationwide intranet provides a safe environment with only government-sanctioned content. In 1996, the China Internet Company (CIC) was the first to announce such a controlled intranet, the China Wide Web (CWW). The CWW turned out to be more hype than substance, but the concept of a Chinese Internet was born. Following the CWW came InfoHighway, also known as the Yinghaiwei 瀛海威 network from Zhang Shuxin: a network offering Chinese content protected by sophisticated firewalls.[135] Yinghaiwei did not fare too well either, it was facing bankruptcy in 1999. Next was the Public Multimedia Network, better known as the 169 network.[136] Contrary to its predecessors, the 169 network is relatively successful in offering a cheap alternative to full-blown internet access, which is five times more expensive.[137] The Data Communications Bureau (DCB) of China Telecom is responsible for operating the 169 network. The 169 network is often mentioned alongside ChinaNet, the 163 network, that offers internet access. The latest alternative is C-Net, "an internetworking project of Chinese people" from a company called Sichuan Zhongcheng Network Development Company Ltd. that has been 8 years in the planning. The government has tried to make these intranets appealing by lowering the cost of access. For the 163 and 169 network there are no administrative hassles in registering, as opposed to the internet where one has to go through numerous administrative procedures. In January 2001, plans were made to merge the 163 and 169 networks.[138]

The idea of a nationwide intranet appealed to the government. Several implementations of this idea have surfaced so far and most of them failed miserably in capturing the public's interest. The relatively successful 169 network is planned to merge with the 163 network. As a result we can conclude that the viability of a nationwide intranet has not worked in China so far.

4.2.2 Countermeasures

In order for countermeasures to be practical, they need to have a high degree of accessibility, user-friendliness and continuity. Goldsmith argues that internet regulation can be effective even if it is not 100% airtight.[139] The purpose of internet control is to raise barriers to access of information. Therefore, countermeasures need to be accessible and user-friendly in order to be useful for the average internet user. Continuity is needed in order to be able to rely on the

[133] However, Geocities doesn't seem to hesitate to compromise anonymity for commercial interest. In 1998, it sold personal information gathered during the registration process to outside marketers, despite explicit assurances that it would not do so. See Lyon, David, *Surveillance* Society: Monitoring Everyday Life. Buckingham, Philadelphia: Open University Press, 2001. p.102.

[134] Blocking a whole range causes a whole lot of other homepages to be blocked as well, amongst others my personal homepage about Hong Kong director Wong Kar Wai, partly hosted on Geocities. Since May 2001, my website is not hosted on Geocities anymore. However, I received numerous mails from Chinese users why they were not able to reach my website in the past when it was still hosted on Geocities.

[135] The Yinghaiwei website can be found at http://www.i.com.cn

[136] 169 refers to the dialup number to access the network

[137] Wong, Bobson, "Improving Internet Access in China," *Digital Freedom Network*, http://www.dfn.org/focus/china/chinanet.htm

[138] People's Daily, "China Telecom To Merge and Enlarge 163/169 Network," *People's Daily* (5 January 2001), http://english.peopledaily.com.cn/200101/05/eng20010105_59697.html

[139] Goldsmith, Jack, "Against Cyberanarchy," *Occasional Papers from The Law School The University of Chicago* Number 40, http://www.law.uchicago.edu/Publications/Occasional/40.html

countermeasure. We will examine how these countermeasures work and to what degree they are successful.

Proxy Servers

> "We need to be selective. We hope to restrict as much as possible information not conducive to China's development."[140] (Jiang Zemin in an interview with Mike Wallace, 2000)

One of the practical uses of the routing abilities of the internet is the usage of proxy servers by Chinese internet users to circumvent the blockades.[141] A proxy server can function as an intermediate, enabling blocked sites to be viewed by the audience.[142] The use of proxy servers to circumvent existing filters is the most often mentioned counter measure to content control.[143] Requests for websites are forwarded to the proxy server, which in turn requests the website you requested. Since the proxy server is not hampered by the restrictions, it retrieves e.g. the CNN website 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. Not surprisingly, top search key words in China are 'proxy' or 'free proxy'.[144]

However, there are some complications to this story, often neglected in articles that mention the use of proxy servers as the saviour of 'Free Speech'. For a proxy server to be efficient, it needs to be accessible, and the speed the proxy server connects to a website should not be much slower than when one directly connects. 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, meaning that 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 load is not too high, in other words, as long as there are not too many users using the proxy. Imagine what happens when the Chinese massively start to use a certain proxy: it would simply overload. So, as long as the proxy is running it is not really interesting because the number of users using it is not alarming, and when the number of users starts to rise, performance will suffer, rendering the proxy server useless.[145] There is also no commercial incentive in running a proxy server; therefore continuity of the service is not guaranteed. Another big problem is that the proxy server itself can be blocked. However, it is relatively easy for the internet user to switch servers to avoid the blockades. The search for proxy servers can be simplified by using programs that specialise in searching for proxy servers. Proxy Hunter is such a program, which is available in China.[146] The problem is that if it is easy for the internet user to locate a new server, it will be easy for the government as well to locate it. Zhang Weiguo estimated that it takes two months for the Chinese government to track down proxy servers and block access to them.[147] Rumours even started to go around that the Chinese government was

[140] Jiang Zemin in an interview with Mike Wallace of CBS in Beidaihe, China on 15 August 2000, quoted after U.S. Embassy Beijing, "Kids, Cadres and 'Cultists' All Love it: Growing Influence of the Internet in China," http://www.usembassy-china.org.cn/english/sandt/netoverview.html

[141] The primary function of a proxy server in this context is its caching function. However, a proxy server has several distinct functions not to be confused with each other.

[142] The definition of proxy server spans multiple explanations. In this context, a proxy server is mentioned as a server with primarily a relay function.

[143] For example, see Lin Neumann "The Great Firewall" and Forster and Goodman, *The Diffusion of the Internet in China*.

[144] Zhang Weiguo, "Evading State Censorship: From the Bible to New Century Net," *China Rights Forum* (Fall 1998), http://www.hrichina.org/crf/english/98fall/e7a.html

[145] It is technically possible to prevent the proxy from overloading. One solution is to share the load between multiple proxy servers. For technical details of the Microsoft Proxy server see Posey, Brien, "Balancing the Workload Between Multiple Proxy Servers," (15 December 1999) http://www.microsoft.com/technet/winnt/proxload.asp

[146] Zhang Feng's Proxy Hunter is available for download at http://www.cl.spb.ru/sparta/scanner.htm

[147] Zhang Weiguo, "Evading State Censorship: From the Bible to New Century Net," *China Rights Forum* (Fall 1998), http://www.hrichina.org/crf/english/98fall/e7a.html

deploying fake proxies, using them as a honey pot.[148] A honey pot acts like a real proxy, but monitors the activity and gathers data for prosecution.[149] Once word of these fake proxies goes around, paranoia will set in, causing the user to look at any proxy with suspicion and to be hesitant about using the proxy. Unsure whether they are monitored or not, they show the proper behaviour: a trait of the Panopticon.

Anonymous Networks

> "You have zero privacy, get over it"[150] (Scott Nealy, CEO of Sun Microsystems)

Networks that protect your privacy and let you surf anonymously are sometimes mentioned as a counter measure to the all-seeing eye of the government. Instead of your computer being monitored, the privacy network is monitored. However, this solution has the problem that this network, like proxy servers, can be blocked. Anonymous network services are either free like Anonimyzer, but flawed or painfully slow to operate or, ironically, demand payment, like a service called Freedom.[151] These options make it difficult for Chinese internet users to access because electronic payment currently is almost non-existent. Anonymity here becomes a product you have to be able to afford.

Cybersleuthing

> "The power to extinguish a rumor as soon as it's born."[152] (a feature attributed to the web monitoring software)

BBS are notoriously hard to regulate because of their spontaneous nature. However, cybersleuthing companies are developing software for the industry that makes it possible to spot a rumour posted online within 15 minutes.[153] The software forms a great first line of defence for the moderator who is responsible for spotting undesirable content, countering the argument that the sheer amount of postings is overwhelming for a human by automating a large part of the process.

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. However, a few problems exist that prevent encryption from gaining widespread acceptance. First of all, not a lot of people care about privacy on the net.[154] Security awareness is not very high among the general public and therefore not a lot of people install encryption software.[155] Another factor

[148] Chen, Judy M., "IT Multinationals: Willing Partners to Repression in China?," *Human Rights China* (10 November 2000), http://www.hrichina.org/Beijing%20IT%20Trade%20Show%20--%20Judy%20Chen.html

[149] Schneier, Bruce, *Secrets & Lies: Digital Security in a Networked World*. New York: John Wiley and Sons Ltd., pp.197,198.

[150] Cohen, Nick, "Our Zero Privacy," *Guardian Unlimited* (18 June 2000), http://www.guardian.co.uk/netprivacy/article/0,2763,333529,00.html

[151] Anonimyzer is accessible at http://www.anonymizer.com
An article that discusses the flaws in anonymous web surfing is Oakes, Chris, "Anonymous Web Surfing? Uh-uh," *Wired* (13 April 1999), http://www.wired.com/news/technology/1,1282,19091,00.html
Freenet is available at http://www.zeroknowledge.com

[152] Kumar, "Concern About New Web Monitors," *Wired*, (24 February 2001), http://www.wired.com/news/privacy/0,1848,41931,00.html

[153] ibidem

[154] McCullagh, Declan, "Public: Take Our Privacy, Please," *Wired* (9 May 2001), http://www.wired.com/news/print/0,1294,43657,00.html
There is one exception where the public does care about security and that is when credit cards are concerned.

[155] ibidem

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.[156] Additionally, both the sender and receiver need to have PGP installed in order for it to work. The fewer PGP users you know, the less useful it is.[157] 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 do not have anything to hide?

It is noteworthy to keep in mind that China is not the only country grappling with the issue of encryption. Every country has at one time had to deal, or is still dealing with this problem. Encryption is needed on the one hand for safe transactions over the internet, and on the other hand encryption also allows criminal acts to go undetected.

E-mail Spamming

Underground newsletters are often mentioned as examples why internet would be impossible to control. The following three newsletters are the most representative and oft mentioned.

VIP Reference 大参考 is a newsletter that provides news from most magazines from Hong Kong, Taiwan and China. Its name is borrowed from a Communist term for 'uncensored' internal information only available to high Party officials. Started in 1998, the newsletter hopes to provide the Chinese people access to all information available. The newsletter is compiled in China, anonymously sent by e-mail to the U.S., where the newsletter is sent to thousands of Chinese mailboxes, using a different e-mail account each time to make it difficult for the Chinese government to block it. *VIP Reference* also has a homepage and is posted on a regular basis in Usenet newsgroups, such as *soc.culture.china*. However, the homepage is hosted by *Geocities*, which is blocked, and Usenet newsgroups are sparsely available in China. The website and postings in Usenet newsgroups therefore do not reach their intended target, the people in Mainland China.

Tunnel 隧道, another frequently mentioned newsletter that published dissident writings, has been discontinued since September 1998. The publishers of *Tunnel* were arrested in August 1998.[158]

CND is the first online magazine and it currently still is available. It is set up in 1989 and based in the U.S. Its content is largely in English and its website is blocked in China.

4.2.3 Conclusion: The Internet Is Not Impossible to Control

The 'free' character of the internet made the price of anonymity very low. Free services offered by volunteers were originally one of the characteristics of the internet. Free services, such as proxy servers, provided a very easy and cost effective way to accept and maintain an anonymous identity. However, these services came under severe pressure and became hard to maintain as the internet became more popular and commercialised the last few years.

It is still possible to circumvent control. However, there are barriers such as money and technical knowledge. For example, circumvention is possible by dialling into a foreign ISP but this is an expensive solution. Technical knowledge is needed to use encryption, a proxy

[156] "E-Mail Privacy Remains Elusive," *Wired* (11 March 2001), http://www.wired.com/news/technology/0,1282,442359,00.html

[157] This holds true for any network (e-mail, telephone). The law of Metcalfe states that "the value of a network grows by the square of the size of the network."

[158] Reuters, "China Beefs Up Net Crackdown," *Wired* (29 July 1998), http://www.wired.com/news/politics/0,1283,14099,00.html

server, or any other method to evade control. The current measures are quite effective in preventing users from accessing prohibited content and the government is certainly not powerless in its effort to control the internet.

4.3 Social Norms

Social norms control behaviour and derive their power from the community. Social norms differ depending on the community and culture they operate in. A universal example of social norms regulating behaviour is watching porn in a public place, for example an internet café, an act that is generally frowned upon. This paragraph will examine how social norms in China set constraints on offline and online behaviour.

4.3.1 How the Chinese view Foreign Technology

> "Enemy forces at home and abroad are sparing no effort to use this battlefront to infiltrate us,"[159] (editorial in People's Daily, January 2001)
>
> "China is going to develop the internet, but we do not know whether it will be with the kind of unfettered press freedom that Western experts want. Maybe we do not want that kind of freedom."[160] (Ke Guo, associate professor of journalism at Shanghai International Studies University)

Since the 16th century and the introduction of foreign technology in China, there have been discussions about how to implement new technology while preserving Chinese values. The concept of *tiyong* was introduced in the middle of the 19th century and stands short for "中学为体，西学为用" Chinese learning for substance, Western learning for practical use.[161] The concept of *tiyong* implies a view of social and cultural superiority and a reluctance to accept foreign ideas and technology integrally, especially those from the West. The *tiyong* concept is crucial in understanding how the Chinese approach foreign technological development and its influence on social norms. It shapes the view of Chinese leaders and its citizens and provides them with a sense of being 'Chinese'. Since the 19th century, the introduction of new technology has been critically measured against the ideal of the *tiyong* concept, the obvious example here being the internet.

The government is positioning and justifying its internet control policy as the safeguard of moral values by using the growing concerns for internet phenomena, such as internet cafés, computer games, instant messaging systems. All have, at one point, been compared with electronic opium, directly pointing to the disruptive influence of opium that was introduced by the Western colonialists back in the 19th century leading to the Opium Wars.[162] There

[159] Lin Neumann, A., "The Great Firewall," *Committee to Protect Journalists* (January 2001), http://www.cpj.org/Briefings/2001/China_jan01/China_jan01.html

[160] ibidem

[161] Ssu-Yu Teng and John K. Fairbank (eds), *China's Response to the West: A Documentary Survey 1839-1923.* New York: Atheneum, 1963 [1954], pp. 50-51, 164-166.

[162] "Dependence on foreign hardware, software, Net content concerns China, report says," *ChinaOnline* (8 August 2000), http://www.chinaonline.com/topstories/000808/1/C00080701.asp
For Chinese Sources see:
"OICQ: 现代'网络鸦片'" (OICQ: Contemporary 'Cyber Opium'), *Eastday* (21 February 2001), http://cn.tom.com/tech/Archive/2001/2/21-49655.html
"网络等于鸦片吗？," (Is the Internet the same as Opium?), http://geren.y365.com/my/yapian.htm
Yang Guang (杨光)，"评论：清除电子游戏违规经营还需深入持久," (Opinion: The Removal of Businesses that Violate the Video Games Regulations Still Need to be Enforced and Deepened) *Sina* (15 December 2000), http://dailynews.sina.com.cn/s/158698.html
For a whole collection of articles on the bad influence of the internet (cyber opium) see:
网聊：Q人类的网络鸦片 (Online Chat: The Youth's Cyber Opium), http://cn.tom.com/feature/Archive/2001/5/23-79739.html

have been discussions about the corrupting influence of electronic opium, which draws the attention away from the political aspects of its internet control policy. Another point is the fear of China's IT industry being 'built on sand', pointing towards the fact that the computer chips, which are made from silicium (sand), are all made outside China.[163] It shows the growing concerns of government and citizens alike over the corrupting influence and the increasing dependency on Western technology.[164]

4.3.2 How the Chinese view Privacy and the Internet

> "Why worry about networked databases? They already know everything they want to about me!"[165] (entrepreneur in Beijing's Zhongguancun)

Definitions of privacy vary widely and are also dependent on the social environment. There is a lot of Western literature about the relationship between advanced technology and privacy.[166] However, the lack of Chinese literature discussing the impact of internet on privacy is glaring.[167] In the West, the issue of the internet endangering privacy is becoming relevant, but it seems that privacy is not an issue the Chinese greatly worry about.[168]

The Chinese government can easily implement measures that would raise privacy concerns elsewhere. There are no laws in China to determine exactly what records are too private for release.[169] Things that in the West would be impossible are met with little protest, such as a personnel database that functions as a black list for bad employees.[170] This is an issue that becomes paramount with the increasing capacities of databases. The possibility of linking databases will certainly appeal to the central government, and this is exactly what they are trying to achieve with some of the Golden Projects. The first completed Golden Project is Golden Sea, which "links all government leaders and the databases from all offices and institutions under the jurisdiction of the Party."[171] Furthermore, as has been mentioned in chapter 4.1, regulations require all ICP to keep records for 60 days of all information posted on the website and bulletin boards. AN need to keep a record for 60 days of all customers, tracking how long they were online, from where they logged in and what websites they

[163] O'Neill, Mark, "Net Warning by Beijing Brass," *ZDNet Asia* (12 March 2001), http://www.zdnetasia.com/news/dailynews/story/0,2000010021,20188266-1,00.htm

[164] "No national borders on the internet? No Way! (China PRC)," *China Youth Daily*, http://www.sinopolis.com/Archives/TOPSTORY/ts_990918.htm

[165] Hartford, "Cyberspace with Chinese Characteristics," http://www.pollcyber.com/pubs/ch/home.htm

[166] The classic work that springs to mind is George Orwell's *1984*. More academic discourses are from Garfinkel Simon, *Database Nation: The Death of Privacy in the 21st Century*. Sebastopol: O'Reilly, 2000 and two books from David Lyon, see Lyon, David, *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press, 1994 and Lyon, David, *Surveillance Society: Monitoring Everyday Life*. Buckingham, Philadelphia: Open University Press, 2001

[167] A little search among the Chinese top portals (Sina, Sohu, Netease) for 隐私 "yinsi" and 私隐 "siyin" resulted in very few hits. If there were any hits at all, most of them were not China related, but instead talked about privacy in America or the West. The exception is the IT website Yesky at http://www.yesky.com where a couple of articles discuss the impact of the internet on privacy.

[168] There is, for example, no non-governmental organisation that strives to protect the privacy of Chinese citizens. Also see Luo Xinzhong (罗新忠)，"专家呼吁加强保护网络隐私," (Experts Call for Strengthening of Protection of Privacy on the Internet), *Sohu* (2 March 2001), http://it.sohu.com/20010302/file/0000,643,100007.html

[169] Zhou, Jamila, "Internet Archive to Snitch on Workers," *South China Morning Post*, http://prodev.learningnetwork.com/HR_Professionals/News/0000-5077-KEYWORD.Missing.htm

[170] The database is run by a Beijing company and a company official claimed that already 10.000 companies applied to make use of this database. For more information, see Zhou, Jamila, "Internet Archive to Snitch on Workers," *South China Morning Post*, http://prodev.learningnetwork.com/HR_Professionals/News/0000-5077-KEYWORD.Missing.htm

[171] Peter Lovelock, "E-China: Putting Business on the Internet," *Virtual China* (29 October 1999), http://www.virtualchina.com/archive/infotech/analysis/e-business-101899-3.html

visited.[172] Black boxes are installed at AN that automate the recording of this kind of information.[173]

[172] Crampton, "Beijing Uses Cyberspace to Widen Control," *International Herald Tribune* (24 March 2001), http://www.iht.com/cgi-bin/generic.cgi?template=articleprint.tmplh&ArticleId=14484

[173] On a similar note, the Dutch government has great trouble installing the same wiretap technology at its ISPs.

4.3.3 Offline Social Norms

> "Nobody really cares or can control what you're doing at home as long as you do not take things [into the] public."[174] (Dr. Yun Tao, vice president of Cenpok Intercom Technology Company, Beijing)

Social norms can be enacted in two different spheres, online and offline. According to the CNNIC survey of January 2001, 60,3% of the internet users access the internet at home, 43,9% at work and 20,9% from an internet café. The trend is growing towards access at home, as more people can afford the luxury of buying a PC. Social control in a public place is stronger than in a private place. Prying and curious eyes can prevent one from accessing material that is deemed offensive. On the other hand, users perceive more freedom while accessing the internet at an internet café. However, this perceived freedom directly relates to whether the café actively registers the users and has been a point of concern for the central government. The latest CNNIC report states that 43,9% of the internet users access the internet from work. Accessing the internet from a public place such as the work unit puts the user in a vulnerable position among colleagues. A common phenomenon is that people would wait until night time when they could surf in private. This got so popular that some work units shut the server down at night or allocated surfing hours.[175]

4.3.4 Online Social Norms

> "We go with our intuition. If something makes us uncomfortable, we nix it."[176] (*Sohu* staff member)
>
> "Being as visible as we are, there's no getting away from the government"[177] (Hurst Lin, co-founder of *Sina*)

Netiquette is a contraction of network and etiquette, meaning the formal and informal rules that govern online interaction between internet users. An example is that you do not SHOUT by typing capitals. The Bulletin Board Systems (BBS) are the closest resemblance of an

[174] Shaw, Joy C., "Internet Censorship in China," *Online Journalism Review* (6 May 1998), http://ojr.usc.edu/content/story.cfm?request=239

[175] Qiu, Jack Linchuan, *Mediating the Political Impact of the Internet: The Case of China*. MA. Thesis, p. 83

[176] Marshall and Kuhn, "China Goes One-on-One With the Net," http://www.latimes.com/business/cutting/lat_chitek010127.htm

[177] Heim, "China Keeps Firm Hand on Net Use," *Mercury News*, http://www0.mercurycenter.com/svtech/news/indepth/docs/china091900.htm

online community in China, and therefore the most interesting to examine with regard to social norms.

The news forums on BBS are often mentioned as the most problematic to regulate because of the massive amount and spontaneous nature of information. In chapter 4.2.2, cybersleuthing software is mentioned that can spot a posted rumour within 15 minutes. Besides filter software, every news forum also has its own moderator.[178] They are responsible for weeding out messages that are either not in line with government policy or news forum policy and those that are off-topic. These moderators are called 'big mamas', pointing to the Orwellian concept of the 'Big Brother' and their parental and guiding function with respect to social norms. Besides the 'big mamas', community members can keep each other in check and correct behaviour when needed. For example, 'hanjian' 汉奸, which translates as 'traitor of the Chinese' and has a strong negative connotation, was often used to label people who were sympathising with the Americans in the spy plane incident of April 2001.[179] The community itself was correcting those people who did not conform. The moderator stepped in when things got out of hand, calling for an 'orderly and rational discussion'.[180] People commit themselves to conform to the moral order to protect the harmony of the community or risk getting flamed and becoming an outcast.[181]

There are generally two ways to post a message on the BBS, anonymously and as a registered user. An anonymously posted message directly goes to the queue, waiting to be approved by the moderator. Postings by registered users are filtered on key words and either placed in the queue if they contain the targeted key words or posted to the BBS. A circumvention of key words is possible by using homophones, characters that have the same pronunciation but have a different meaning. Inside knowledge is required in order to understand what is meant, which raises barriers to access.

If undesirable content is found, there are a few penalties that can be given. First, the moderator can issue a warning to the poster, or simply remove the posting. This is the most common penalty. A heavier penalty is to deny the user the right to post messages temporarily or even to remove and ban the user from the BBS, denying him access to the community. However, it is relatively easy to register a new account with a new username. Penalties can also be given to the company or organisation that operates the website. First, technical personnel can be warned, fined or removed from their position. Secondly, the website or BBS can be suspended for an indefinite time. Third, the license of the website can be revoked so that the website needs to suspend service.[182] The most severe and telling example is Peking University's *Weiming* 未名 BBS. Political discussions were commonplace and discussions were relatively liberal until 1996, when the government decided to close the BBS for an indefinite time.[183] It was not allowed until late 1999 to reopen its service. The shutdown of the *Weiming* BBS shows that the government has no problems with closing a popular service to make a statement. The closing of BBS also occurs prior to sensitive dates. However, this is a pre-emptive measure by the BBS themselves. For example, most BBS close prior to June 4th, the date of the repression of the student movement on Tiananmen Square.

[178] Again, China is not unique in using paid labor to exercise control over discussions in chat rooms and BBS. In the United States, several services, among them America Online (AOL), do the same.
[179] Qiu, Jack Linchuan, "Chinese Opinions Collide Online," *Online Journalism Review*, http://ojr.usc.edu/content/story.cfm?request=561
[180] ibidem
[181] To flame is "to send nasty or insulting messages, usually in response to someone's having broken the rules of Internet etiquette (called netiquette)." See http://www.its.bldrdoc.gov/projects/t1glossary2000/_flame.html
[182] Qiu, Jack Linchuan, "Virtual Censorship in China: Keeping the Gate between the Cyberspaces," *International Journal of Communication Law and Policy*, Vol. 4, Winter 1999/Spring 2000, pp.1-25.
[183] ibidem

> “It’s a low-grade way to allow people to let off steam.”[184] (unnamed foreign journalist in Beijing)

Little by little, BBS are making the central government realise that 100% airtight information control is not possible. A great example is how Zhu Rongji in March 2001 offered an apology about how the school blast incident that killed 38 children was handled, after chat rooms at *Sina* were flooded with messages and the moderators had to take strenuous measures to cover things up, quite unsuccessfully. The BBS gave angry citizens a public place to vent their anger, something that did not exist before. The discussion over the school blast became so heated that *Sina* was forced to shut down its forum. Unofficial news often circulates in BBS long before it is published in the official news media.

4.3.5 Nationalism

> “Maintains the reunification of the motherland, guards the national sovereignty”[185] (slogan of the Honker Union of China)

In China, nationalism is within the accepted range of social norms. It is an important source of government legitimacy, often mentioned in the mass media and heated up during political events. An interesting development occurred in the BBS during the bombing of the Chinese embassy in Belgrade in May 1999 and the spy plane collision of April 2001, the effects of which among the general populace of the Western media did not foresee. Where Clinton hoped that the internet would eventually facilitate a democracy in China, the internet users in China use the internet to amplify their nationalistic sentiments. The spy plane collision caused a lot of heated discussions and nationalistic sentiments ran rampant in the Chinese BBS. Accordingly, the number of hack attacks performed on U.S. servers went up, while American hackers responded by hacking Chinese servers. [186] The heated nature of the BBS brought back memories of the nationalistic sentiments after the NATO bombing of the Chinese embassy in Belgrade. Chinese hackers, also known as “honkers” 红客, were called upon to hack American websites.[187] Whole websites were set up providing information and a place for venting one’s anger.[188]

4.3.6 Conclusion: Wary of Foreign Technology, Not Wary of Privacy

The Chinese have a tradition of approaching foreign technology critically, and the internet in particular. Copying a Western model in China is doomed to fail, according to the Chinese. The central government uses this to legitimise the internet control policy by focusing on the

[184] Earnshaw, Graham, “China Online,” *Brill’s Content*, February 2001, http://www.brillscontent.com/2001feb/columns/next.shtml

[185] see http://www.cnhonker.com/eabout.htm

[186] Costello, Sam, “U.S., Chinese Hackers Continue Web Defacements,” *CNN Sci-Tech* (2 May 2001), http://www.cnn.com/2001/TECH/internet/05/02/china.hacks.idg/

[187] Honker 红客 is derived from the Chinese translation of hacker, in Chinese 黑客 “heike” , literally meaning black guest. Honker is the Chinese equivalent 红客 “hong ke”, meaning red guest. A full explanation can be found on the website of the Honker Union of China at http://www.cnhonker.com

[188] See for example http://killusa.abc.yesite.com

harmful effects of the internet such as instant messaging, games and porn. They compare these effects with electronic opium.

The sense of being watched in a public place can work as a deterrent to accessing socially not accepted material. The trend is however growing towards home-based access to the internet. Netiquette are the equivalent of social norms online. Big Mamas determine what is acceptable in the BBS. The community itself also influences what one can say in the BBS. Noteworthy are the strong nationalistic sentiments in the BBS during international political incidents.

4.4 The Market

We described how the Chinese government uses the market in combination with the law to force businesses to self-censor themselves. Businesses adhere to the policy out of fear of having to close their operations. In this paragraph, we will show how the market allows the Chinese government to procure technology that enables it to strengthen its internet control.

The U.S. has a very relaxed export restriction for advanced technology, as the U.S. 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.[189] As a practical result of this policy, 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.

The Golden Shield project, culminating in the exhibition called Security 2000 held in Beijing, shows what is possible when Western companies meet the Chinese government. The Golden Shield project was started 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."[190] At the Security 2000 exhibition, a whole group of Silicon Valley companies were anxious to do business with the Chinese government.[191] Not only Fortune 500 companies, such as Sun, Hewlett-Packard, Compaq and Cisco are doing business with China, but lesser known companies, such as Websense as well. Websense is a company that specialises in systems that are responsible for blocking 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 (read: the Chinese government, LT) choose to block. It’s up to them.”[192] In other words, Websense does not care about how its product is used. The only company that has a known record with the Chinese government and refused to do business out of ethical motives is InfoGlide. [193] InfoGlide sells a technology that is able to search and detect patterns in huge databases. InfoGlide refused to deliver, but the question is, how many others did?

[189] In the past, the U.S. didn’t even allow China to have internet access. An example of the relaxation of the U.S. export control policy is the case of encryption technology. U.S. companies are allowed to export any encryption technology to individuals, commercial firms or other non-governmental end-users in any country, including China. An exception is the export of the High Performance Computers (HPC), although even in this case, the definition of a HPC continues to relax. For information concerning the U.S. export policy, see the website of the Bureau of Export Administration, http://www.bxa.doc.gov
For more information concerning the HPC export controls, see http://www.bxa.doc.gov/HPCs/Default.htm
For more information concerning encryption export controls, see http://www.bxa.doc.gov/Encryption/Default.htm

[190] Chen, Judy M., “IT Multinationals: Willing Partners to Repression in China?,” *Human Rights China* (10 November 2000), http://www.hrichina.org/Beijing%20IT%20Trade%20Show%20--%20Judy%20Chen.html

[191] Marshall and Kuhn, “China Goes One-on-One With the Net,” http://www.latimes.com/business/cutting/lat_chitek010127.htm

[192] ibidem

[193] Hartford, “Cyberspace with Chinese Characteristics,” http://www.pollcyber.com/ch/pubs/home.htm

4.4.1 The Digital Panopticon

> "We do not provide security or legal advice to our clients. It's a tool."[194] (Patrice Bourgeois, director of marketing of Raytheon)

According to Lessig, the architecture of the internet is changing because commerce is developing code that continues to erode privacy. A prime example of this development is a product from Raytheon called SilentRunner. Raytheon is a defence contractor that did not do too well after the Cold War. It decided to go for the money and started developing surveillance software in 2000, thereby serving as a good example of Lessig's theory how commerce is driving the development of code that continues to erode privacy. So what is SilentRunner capable of? It will ..

> "allow companies to monitor absolutely everything passing over their network, from e-mails to instant messages [..] SilentRunner is completely undetectable to end users [..] On an individual user, we can see what you're e-mailing, where you are surfing, if you send anything to be printed, collaborate with anyone on a Word document, access or change the database -- basically everything you're doing on the network [..]The program analyses text of any language with equal acuity."[195]

SilentRunner is the digital equivalent of the Panopticon. The Chinese are fully aware of the possibilities such code offers. The MPS released a filtering software package in March 2001 called "Internet Police 110". Internet Police 110, referring to the emergency police telephone number, is designed to keep "cults, sex and violence" away from the internet users.[196] It can also monitor packets of data transferred and decide whether to block them if the content is deemed undesirable. The software is available in three versions for households, schools and internet cafés. While Internet Police 110 does not seem as sophisticated as SilentRunner, one wonders about the infinite possibilities this code would give the Chinese government.

Electronic monitoring in the workplace is becoming commonplace. A study published by the American Management Association in April 2001 revealed that the percentage of companies actively monitoring their employees rose from 45% in 1998 to 74% in 1999.[197] IDC estimates that the worldwide corporate market for network monitoring and filtering products will rise from $62 million in 1999 to $561 million in 2004.[198] There is a big demand for monitoring software, ensuring further development of code that facilitates the control of the internet.

[194] Lyman, Jay, "SilentRunner Spyware Out-Snoops FBI's Carnivore," *NewsFactor Network* (2 March 2001), http://newsfactor.com/perl/story/7873.html

[195] Benner, Jeffrey, "Nailing the Company Spies," *Wired* (1 March 2001), http://www.wired.com/news/business/0,1367,41968-2,00.html

[196] Stout, Kristie Lu, "China Police Unleash Net Filterware," *CNN* (1 March 2001), http://asia.cnn.com/2001/WORLD/asiapcf/east/02/28/hk.policefilter/

[197] Benner, Jeffery, "Privacy at Work? Be Serious," *Wired* (1 March 2001), http://www.wired.com/news/privacy/0,1848,42029,00.html

[198] ibidem, for a whole list of other surveillance software see Cambridge, Lennie, "A Spy Free Workplace," (2001) http://student.fortlewis.edu/~lccambridge/CS361%20Final.htm

5. Conclusion

This thesis starts with a quote from Clinton, saying that the internet is impossible to control and would undermine any authoritarian regime that attempts to control it. China has a long-standing tradition of strict control over the media and the internet has not been an exception. The government lost its share of control due to pluralisation, commercialisation and globalisation of thought work. The introduction of the internet caused organisational problems for the government because it was unclear which ministry was responsible. The different ministries all had their own agenda and a struggle erupted. The MII was created to supervise the development of the internet, but other government bodies still have a say regarding internet matters. These internal struggles between government bodies can work detrimental in implementing a coherent policy with regard to the internet. So is the internet impossible to control? Although limiting access by stifling the growth of bandwidth is an option for internet control, the government has strived to improve the bandwidth. A natural deterrent for access to information and communication is language, because English literacy is low and the Chinese language does not work quite well on the internet.

Lessig argues that there are four modalities of control: the law, architecture, social norms and the market. The architecture is the foremost regulator of the internet. A prime example of how architecture regulates behaviour is the concept of the Panopticon, invented by Bentham and mediated by Foucault. The concept of the Panopticon prison depends on the visibility and individualisation of the user and the uncertainty of being monitored.

In China, the law legitimises the Panopticon. It determines what kind of content is prohibited and enforces the monitoring of networks and internet users. The law also makes the organisation of the network responsible for any violations that take place on the network. This creates a decentralised structure of self-censorship: the privatised Panopticons. As a result, businesses self-censor themselves out of commercial interest. A powerful weapon is intimidation. It serves to remind the internet users that the Chinese government is actively monitoring them and not hesitant to take action if needed.

The control of the internet infrastructure in China starts with the architecture. All networks need to connect with the ChinaNet network from the MII for traffic outside China. This simplifies controlling the internet, because there is only one gateway that needs to be monitored, and it makes the Panopticon even easier to maintain. This is not a waterproof concept: a person with enough money or technical knowledge can still access what is filtered. Nonetheless, internet regulation can be quite effective without offering 100% protection. Internet regulation is about raising barriers to the access of prohibited content, and the Chinese government is doing just that.

Social norms influence behaviour when the internet is accessed from a public place. Prying eyes prevent one from wandering too far from the socially accepted standard. More than 40% of the internet users access the internet from a public place. In online communities, such as the BBS, Big Mamas determine what is acceptable or not. The law does little to protect the privacy of an individual. On the contrary, the law requires networks to monitor and keep detailed records.

China has the perfect ingredients ready for a digital Panopticon. There is a decentralised structure of self-censorship. There is little public awareness or legal protection of privacy. There is only one gateway that needs to be monitored. The market is producing code that is the digital equivalent of the Panopticon; code that makes it possible to turn what is private into public and that enables complete monitoring of each individual user. China can readily purchase this code. Big Mama will be watching you.

5.1 Further Research

This thesis probably raises more questions than answers due to limitations of time and the broad scope of the topic. Below, I hope to provide some leads for further research on this topic.

5.1.1 Topic Limitations

The purpose of this thesis is to provide a broad framework to address the issue of internet control by the Chinese government. Inherent to this set-up is that one cannot go into detail with each topic precisely because of the topic's broad nature. Further specialised research of internet control with regard to the diverse topics, such as law, architecture, social norms and the market would shed more light on the matter.

5.1.2 Used Methodology

In this thesis a top-down approach is used for practical reasons. Although a lot of information on the internet in China is available online, much is still unclear as it is a very new topic. Writing this thesis, I was not physically located in China and therefore lack local understanding. For example, it will be interesting to see how the filtering of websites works in practice. Field research will be very beneficial to a better understanding of the internet in China. I also had preliminary plans to conduct a bottom-up research for the Chinese BBS but due to time constraints I was not able to finish it. The results of the research would have added a lot of value to the topic, especially with regard to the amount of control and censorship conducted in the BBS and how social norms are conducted on the internet.

5.1.3 Comparative Studies

All countries regulate the internet in one way or another. A comparative study of internet regulation would enhance our understanding of the internet. A beginning has been made by Shanti Kalathil who is conducting a comparative study of authoritarian regimes and internet control, specifically in China and Cuba.[199]

5.1.4 Limitations of the Sources

Most sources are from Western media. The topic is relatively new and although general literature on internet control is available, these articles generally tackle the issue from a Western point of view. There is little specific literature available that discusses internet in China. Online Chinese documents have been used but suffer from the problem of non-diversity.

[199] Shanthi Kalathil, William J. Drake, Taylor C. Boas, "Dictatorships in the Digital Age: Some Considerations on the Internet in China and Cuba," *Information Impacts* (October 2000), http://www.cisp.org/imp/october_2000/10_00drake.htm

Bibliography

“江泽民强调互联网要成为思想政治工作新阵地,”(Jiang Zemin Stresses that the Internet Must Become a New Playing Ground for Propaganda Work) *Sina* (11 January 2001), http://tech.sina.com.cn/i/c/49699.shtml

“加入 WTO 对中国互联网影响,” (The Influence of the WTO Entry on the internet in China), *Sohu* (11 September 2000), http://business.sohu.com/20000911/file/045,022,100281.html

“BBS 行话,” (BBS Jargon),
http://member.netease.com/~hisen/cyberhumor/culture/bbsjargon.htm

“网络魔鬼辞典,” (The Devil’s Dictionary of the Internet),
http://culture.163.com/edit/000802/000802_40082.htm

“网络等于鸦片吗？,” (Is the Internet the Same as Opium?),
http://geren.y365.com/my/yapian.htm

“中国收紧对互联网的控制,” (China Tightens Control over the Internet),
http://bbs.huanet.com/fanfubai/90.shtml

“中国有关方面将加强对网络新闻的管理,” (China Strengthens Content Regulation on the Internet), http://bobbychen.3322.net/monographic/news/2.htm

“互联网新闻管制，应如何进行?, ”（How to Implement the New Internet Content Regulation), http://www.bobbychen.3322.net/monographic/news/4.htm

“保护网络用户个人隐私是当务之急,” (The Urgency of Protecting the Privacy of Internet Users), http://go5.163.com/~elaw/monographic/privacy/12.htm

“Dependence on Foreign Hardware, Software, Net Content Concerns China, Report Says,” *ChinaOnline* (8 August 2000),
http://www.chinaonline.com/topstories/000808/1/C00080701.asp

“China Cuts Internet Access Fees to Spur Online Growth,” *ChinaOnline* (26 October 1999), http://www.chinaonline.com/industry/infotech/NewsArchive/Secure/1999/october/C9102207.asp

“China Telecom To Merge and Enlarge 163/169 Network*,” People’s Daily* (5 January 2001), http://english.peopledaily.com.cn/200101/05/eng20010105_59697.html

“China’s Net Commandments,“ *Time Asia* Vol. 155 No. 8,
http://www.time.com/time/asia/magazine/2000/0228/cover.regulation.html

“China Celebs Offer Net Lessons,” *Wired* (26 September 2000),
http://www.wired.lycos.com/news/culture/0,1284,39023-2,00.html

“E-Mail Privacy Remains Elusive,” *Wired* (11 March 2001),
http://www.wired.com/news/technology/0,1282,42359,00.html

"If You'd Like to Make a Call, China Announces Massive Cuts in Telecom, Net Fees," *ChinaOnline* (26 December 2000), http://www.chinaonline.com/topstories/001226/1/C00122206.asp

"No national borders on the internet? No Way! (China PRC)," *China Youth Daily*, http://www.sinopolis.com/Archives/TOPSTORY/ts_990918.htm

"OICQ: 现代 '网络鸦片'" (OICQ: Contemporary 'Cyber Opium'), *Eastday* (21 February 2001), http://cn.tom.com/tech/Archive/2001/2/21-49655.html

"Statistics on Net use are Suspect," *ChinaOnline* (17 April 2001), http://www.chinaonline.com/issues/econ_news/NewsArchive/secure/2001/April/C01041852.asp

Xinxihua Congshu (Book Series on Informatisation), Beijing: Jinghua Chubanshe, 1998

Ang, "Censorship and internet: a Singapore Perspective," (4 May 1995), http://www.isoc.org/HMP/PAPER/132/txt/paper.txt

Geremie R. Barmé and Sang Ye, "The Great Firewall of China," *Wired* 5.06 (1997), http://www.wired.com/wired/5.06/china_pr.html

Benner, Jeffrey, "Privacy at Work? Be Serious," *Wired* (1 March 2001), http://www.wired.com/news/privacy/0,1848,42029,00.html

Benner, Jeffrey, "Nailing the Company Spies," *Wired* (1 March 2001), http://www.wired.com/news/business/0,1367,41968-2,00.html

Bonisteel, Steven, "Asian Surfers Prefer Native," (6 November 1999) http://www.computeruser.com/newstoday/99/11/06/news6.html

Boyle, James, "Foucault in Cyberspace," (1997) http://www.law.duke.edu/boylesite/fouc1.html

Kevan Bradshaw and Ken DeWoskin, "The Internet in China," *PriceWaterhouseCoopers*, http://www.pwcglobal.com/extweb%5Cnewcolth.nsf/docid/2B48471E81BEB97B85256959006A8E34?OpenDocument

Buruma, Ian, "China in Cyberspace," (4 November 1999), http://www.nybooks.com/nyrev/WWWfeatdisplay.cgi?19991104009F#top

Castells, Manuel, *The Information Age: Economy, Society and Culture* (three volumes). Oxford: Blackwell, 1996-1998; 2nd edition, 2000

Catlett, Jason, "Privacy, Property and P3P: A Critique of Lessig's Property Regime Proposal," http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/somak/somak00/catlett.htm

Chen, Judy M., "IT Multinationals: Willing Partners to Repression in China?," *Human Rights China* (10 November 2000), http://www.hrichina.org/Beijing%20IT%20Trade%20Show%20--%20Judy%20Chen.html

Clark, Duncan, "BDA: Bandwidth Growth Turns Spotlight on Censorship Threat," (30 January 2001) http://www.bdaconnect.com/news/bb_2001_01_31/

Clarke, Roger, “Roger Clarke’s Information Wants To Be Free,” (24 February 2000), http://www.anu.edu.au/people/Roger.Clarke/II/IWtbF.html

Cohen, Nick, “Our Zero Privacy,” *Guardian Unlimited* (18 June 2000), http://www.guardian.co.uk/netprivacy/article/0,2763,333529,00.html

Costello, Sam, “U.S., Chinese Hackers Continue Web Defacements,” *CNN Sci-Tech* (2 May 2001), http://www.cnn.com/2001/TECH/internet/05/02/china.hacks.idg/

Cowhig, David, “New Net Rules not a Nuisance?, ” *ChinaOnline* (December 2000), http://www.chinaonline.com/commentary_analysis/internet/NewsArchive/secure/2000/December/c00120160.asp

Crampton, Thomas, “Beijing Uses Cyberspace to Widen Control,” *International Herald Tribune* (24 March 2001), http://www.iht.com/cgi-bin/generic.cgi?template=articleprint.tmplh&ArticleId=14484

Crampton, Thomas, “China Closes Internet Cafés,” *International Herald Tribune* (15 June 2001), http://www.iht.com/cgi-bin/generic.cgi?template=articleprint.tmplh&ArticleId=22928

Crossette, Barbara “The World: Out of Control; The Internet Changes Dictatorship’s Rules,” *New York Times* Week In Review, 1 August 1999, p.1.

Richard Cullen and Pinky D.W. Choy, “The Internet in China,” *Columbia Journal of Asian Law* 13, (1999), pp.99-134.

Deloitte & Touch, *At the Dawn of E-government: the Citizen as Customer*, http://www.us.deloitte.com/PUB/egovt/egovt.htm

Digital Freedom Network, “Attacks on the Internet in China,” *Digital Freedom Network* (24 May 2001), http://www.dfn.org/focus/china/netattack.htm

Earnshaw, Graham, “China Online,” *Brill’s Content* (February 2001), http://www.brillscontent.com/2001feb/columns/next.shtml

Erickson, Jim, “Blocking and Tackling: Is China Cracking Down on internet Activists?,” *Asiaweek* (14 August 1998), http://www.asiaweek.com/asiaweek/98/0814/feat1.html

Fang, Bay, “Chinese ‘Hacktivists’ Spin a Web of Trouble: The Regime is Unable to Control the Internet,” *U.S. News and World Report* September 1998, p.47.

Fang Xingdong (方兴东)，“互联网与中国未来,” (The Internet and China’s Future), *Sohu* (7 November 2000), http://it.sohu.com/20001107/file/0000,643,100108.shtml

Foster and Goodman, *The Diffusion of Internet in China*. Center for International Security and Cooperation, Stanford University, November 2000.

Foucault, Michel, *Discipline and Punish: the Birth of the Prison.* Harmondsworth: Penguin Books, 1977.

Friedman, Thomas, “Censors Beware,” *The New York Times* Jul. 25, 2000

Friedman, Thomas, *The Lexus and the Olive Tree*. London: Harper Collins, 2000.

Froomkin, “Internet as a Source of Regulatory Arbitrage,” University of Miami, 1996. http://www.law.miami.edu/~froomkin/articles/arbitr.htm Also published in Brian Kahin, Charles Nesson (eds.), *Borders in Cyberspace*. MIT Press, 1997, p. 29.

Gillmor, Dan, “Internet will find Way around China Censorship,” *Mercury News*, http://www0.mercurycenter.com/svtech/news/indepth/docs/dg112200.htm.

Gittings, John, “Deal Clinched as BBC and China Make Up,” *Guardian Unlimited* (10 January 2001), http://www.guardian.co.uk/china/story/0,7369,472355,00.html

The Global Information Technology Assessment Group, *The Global Diffusion of the Internet Project: Asian Giants On-Line*, Chapter 4. P126. http://mosaic.unomaha.edu/Asian_Giants_China.pdf

Goldsmith, Jack, “Against Cyberanarchy,” *Occasional Papers from The Law School The University of Chicago* Number 40, http://www.law.uchicago.edu/Publications/Occasional/40.html

Greenleaf, Graham, “An Endnote On Regulating Cyberspace: Architecture VS Law?,” (1998) http://www.austlii.edu.au/au/other/unswlj/thematic/1998/vol21no2/ greenleaf.html
Also published as *University of New South Wales Law Journal* Volume 21,
Number 2 'Electronic Commerce: Legal Issues For The Information Age', November 1998

Hachigian, Nina, “China’s Cyber-Strategy,” *Foreign Affairs* (March/April 2001) Volume 80, No. 2.

Hamrin, Carol Lee*, China and the Challenge of the Future*. San Francisco: Westview Press, 1990.

Hartford, Katherine, “Cyberspace with Chinese Characteristics,” University of Massachusetts, Boston, September 2000. http://www.pollcyber.com/ch/pubs/home.htm

Hartford, Katherine, “Building China’s Information Technology Industry,” http://www.pollycyber.com/pubs/hapr/infochina.htm (draft for summer 2000 article of *Harvard Asia-Pacific Review)*

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

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

Hsieh, “A Cure for Corruption?,” *Asiaweek* (30 June 2000), http://asiaweek.com/asiaweek/technology/2000/0630/tech.b2b.html

Jim Hu and Evan Hansen, “Yahoo Auction Case May Reveal Borders in Cyberspace,” *CNET* (11 August 2000), http://news.cnet.com/news//0-1005-200-2495751.html

Hu Jinming (胡金明), “网上隐私权保护为何难,” (Why Protection of Online Privacy is Difficult), *Yesky* (5 October 2001), http://www.yesky.com/37389312/173612_1.shtml

Hu Jinming (胡金明), “网上隐私权侵权研究,” (A Research of Breach of Online Privacy), *Yesky* (5 October 2001), http://www.yesky.com/37393408/173621_2.shtml

Huang Yu, Hao Xiaoming, Zhang Kewen, "Challenges to Government Control of Information in China," *Media Development* (February 1997), http://www.oneworld.org/wacc/media/china.html

Internet Censorship Project, "The People's Republic of China," (1998) http://www.soros.org/censorship/eastasia/china.html

Isaacson, Walter, "Going Online when the Emperor's Away", *Time* (4 June 2001), http://www.time.com/time/world/printout/0,8816,109632,00.html

Shanthi Kalathil, William J. Drake, Taylor C. Boas, "Dictatorships in the Digital Age: Some Considerations on the Internet in China and Cuba," *Information Impacts* (October 2000), http://www.cisp.org/imp/october_2000/10_00drake.htm

King, Brad, "Napster Loss is Copyright Gain," *Wired* (3 March 2001), http://www.wired.com/news/culture/0,1284,42167,00.html

Klaver, Marie José, "Spyware," *NRC* (22 May 2000), http://www.nrc.nl/W2/Lab/At/20000522.html

Kumar, "Concern About New Web Monitors," *Wired* (24 February 2001), http://www.wired.com/news/privacy/0,1848,41931,00.html

Lessig, Lawrence, *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999

Lessig Lawrence, "Architecting for Control," (2000) http://cyber.law.harvard.edu/works/lessig/camkey.pdf

Lin Neumann, A., "The Great Firewall," *Committee to Protect Journalists* (January 2001), http://www.cpj.org/Briefings/2001/China_jan01/China_jan01.html

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

Peter Lovelock, "E-China: Putting Business on the Internet," *Virtual China* (29 October 1999), http://www.virtualchina.com/archive/infotech/analysis/e-business-101899-3.html

Luo Xinzhong (罗新忠)，"专家呼吁加强保护网络隐私," (Experts Call for Strengthening of Protection of Privacy on the Internet), *Sohu* (2 March 2001), http://it.sohu.com/20010302/file/0000,643,100007.html

Lyman, Jay, "SilentRunner Spyware Out-Snoops FBI's Carnivore," *NewsFactor Network* (2 March 2001), http://newsfactor.com/perl/story/7873.html

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

Lyon, David, "From Big Brother to Electronic Panopticon," http://www.rochester.edu/College/FS/Publications/Lyon.html

Lyon, David, *The Electronic Eye: The Rise of Surveillance Society.* Minneapolis: University of Minnesota Press, 1994.

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

Mai Jiesi (迈杰斯)，“各国政府能否控制互联网,” (Whether Each Country Can Regulate the Internet), http://bbs.huanet.com/fanfubai/91.shtml

Marshall and Kuhn, “China Goes One-on-One With the Net,” *L.A. Times* (27 January 2001), http://www.latimes.com/business/cutting/lat_chitek010127.htm

Marlow, “China Softens Encryption Rules,” *ChinaOnline* (14 March 2000), http://www.chinaonline.com/industry/infotech/NewsArchive/Secure/2000/march/C00031430.asp

McAuliffe, Wendy, “Europe: Police Want to Monitor all Net Traffic,” *Zdnet* (17 May 2001), http://www.zdnet.com/zdnn/stories/news/0,4586,2761777,00.html

Philip McCrea, Bob Smart and Mark Andrews, *Blocking Content on the Internet: a Technical Perspective*. (June 1998) http://www.cmis.csiro.au/projects+sectors/blocking.pdf

McCullagh, Declan, “Public: Take Our Privacy, Please,” *Wired* (9 May 2001), http://www.wired.com/news/print/0,1294,43657,00.html

Mueller, Foster, “China’s New Internet Regulations: Two Steps Forward One Step Back,” http://som.csudh.edu/cis/lpress/devnat/nations/china/chinah.html also published in *Communications of the ACM*, Vol. 40, No. 12, December 1997

Narayan, Anita, “IAMAsia’s Net Survey Contest Official Figures,” *ChinaOnline* (11 January 2001), http://www.chinaonline.com/topstories/010111/1/C01011151.asp

Newman, Ron, “The Church of Scientology vs. anon.penet.fi,” http://www.xs4all.nl/~kspaink/cos/rnewman/anon/penet.html

O’Neill, Mark, “Net Warning by Beijing Brass,” *ZDNet Asia* (12 March 2001), http://www.zdnetasia.com/news/dailynews/story/0,2000010021,20188266-1,00.htm

Oakes, Chris, “Anonymous Web Surfing? Uh-uh,” *Wired* (13 April 1999), http://www.wired.com/news/technology/1,1282,19091,00.html

Orlowski, Andrew, “Stealth Plan puts Copy Protection in Every Hard Drive,” *The Register* (20 December 2000), http://www.theregister.co.uk/content/2/15620.html

Orlowski, Andrew, “Everything you ever wanted to know about CPRM, but ZDNet would not tell you...,” *The Register* (29 December 2000), http://www.theregister.co.uk/content/2/15718.html

Pappas, “China’s internet Syndrome,” *The Standard* (21 February 2000), http://www.thestandard.com/article/0,1902,9687,00.html

Pfaffenberger, Bryan, “The Internet in China” (22 November 2000), http://noframes.linuxjournal.com/articles/currents/0024.html

Posey, Brien, “Balancing the Workload Between Multiple Proxy Servers,” (15 December 1999) http://www.microsoft.com/technet/winnt/proxload.asp

Post, David, “What Larry doesn’t get,” http://www.temple.edu/lawschool/dpost/Code.html or PDF at www.temple.edu/lawschool/dpost/Code.pdf

Qian Hualin, “Internet Development in China,” (Powerpoint Presentation) http://www.chinatech.org/Library/QianHualin.ppt

Qiu, Jack Linchuan, “Virtual Censorship in China: Keeping the Gate between the Cyberspaces,” *International Journal of Communication Law and Policy*, Vol. 4, Winter 1999/Spring 2000, pp.1-25.

Qiu, Jack Linchuan, *Mediating the Political Impact of the Internet: The Case of China*. MA. Thesis, University of South California., 1999.

Qiu, Jack Linchuan, “Chinese Opinions Collide Online,” *Online Journalism Review*, http://ojr.usc.edu/content/story.cfm?request=561

Qiu, Jack Linchuan, “Internet Censorship in China (1999-2000),” *Communications Law in Transition Newsletter*, http://pcmlp.socleg.ox.ac.uk/transition/issue2_3/qiu.htm

Reagle, Joshep, “Internet Quotation Appendix,” (26 March 1999), http://cyber.law.harvard.edu/people/reagle/inet-quotations-19990709.html

Reuters, “China Beefs Up Net Crackdown,” *Wired* (29 July 1998), http://www.wired.com/news/politics/0,1283,14099,00.html

Rotenberg, Marc, “What Larry Doesn’t Get,” http://stlr.stanford.edu/STLR/Working_Papers/00_rotenberg_1/index.htm

Ryan, James, “China’s Internet: Boon to Reform or Just a Quick Buck?,” *Online Journalism Review* (11 February 1999), http://ojr.usc.edu/content/story.cfm?request=159

Salis, Richard, *A Look at how U.S. based Yahoo! Was Condemned by French Law*, University of Montreal (November 2000), http://www.law.asu.edu/karjala/cyberlaw/Yahoo(France)Analysis.html#4

Schneier, Bruce, *Secrets & Lies: Digital Security in a Networked World.* New York: John Wiley and Sons Ltd., 2000.

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

Shaw, Joy C., “Internet Censorship in China,” *Online Journalism Review* (6 May 1998), http://ojr.usc.edu/content/story.cfm?request=239

Sheff, David, “Betting on Bandwidth,” *Wired* 9.02 (February 2001), http://www.wired.com/wired/archive/9.02/tian.html

Song Hualin (宋华琳)，“互联网信息政府管制制度的初步研究,” (A First Research of the Internet Regulation System from the Government), 29 December 2000, http://www.etoptoday.net/freebbs/netlaw/messages/32.shtml

Stout, Kristie Lu, “China Police Unleash Net Filterware,” *CNN* (1 March 2001), http://asia.cnn.com/2001/WORLD/asiapcf/east/02/28/hk.policefilter/

Tan, “Regulating China’s Internet: Convergence Toward a Coherent Regulatory Regime,” *Telecommunications Policy* 23 (1999)

Tan & Yurcik, “The Great (Fire)Wall of China: Internet Security and Information Policy Issues in the People’s Republic of China,” http://www.tprc.org/abstracts/tan.txt

Tao, Wenzhao, “Censorship and Protest: The Regulation of BBS in China People Daily," *First Monday* (January 2001), http://www.firstmonday.dk/issues/issue6_1/tao/

Taubman, Geoffry, “A Not-So World Wide Web: The Internet, China, and the Challenge to Nondemocratic Rule,” *Political Communication* 15 (1998), pp.255-272.

Ssu-Yu Teng and John K. Fairbank (eds), *China's Response to the West: A Documentary Survey 1839-1923.* New York: Atheneum, 1963 [1954].

U.S. Embassy, “Beijing, Kids, Cadres and ‘Cultists’ All Love it: Growing Influence of the internet in China,” http://www.usembassy-china.org.cn/english/sandt/netoverview.html

Westland, Christopher “China’s Golden Projects,” *Global Electronic Commerce*, The MIT Press, 2000, http://www.itheadline.com/feat_art/FA8/china_golden.htm

Wong, Bobson, “Improving Internet Access in China,” *Digital Freedom Network*, http://www.dfn.org/focus/china/chinanet.htm

Wright, Robert, “Gaining Freedom by Modem,” *The New York Times* Jan. 28, 2000.

Yang, Dali L., “The Great Net of China,” *International Harvard Review* winter 2001, also available at http://www.mfcinsight.com/article/010209/oped4.html

Yang Guang (杨光），“评论：清除电子游戏违规经营还需深入持久,” (Opinion: The Removal of Businesses that Violate the Video Games Regulations Still Need to be Enforced and Deepened) *Sina* (15 December 2000), http://dailynews.sina.com.cn/s/158698.html

Zhang Mingjie (张明杰），" 政府管理互联网应当遵循的原则,” (The Principles the Government Should Follow with Regard to Internet Regulation), http://www.cass.net.cn/s07_fxs/s07_09_04_08.htm

Yuezhi Zhao, “Caught in the Web: the Public Interest and the Battle for Control of China’s Information Superhighway,” *Info*, Vol.1, No. 2, February 2000.

Yuezhi Zhao and Dan Schiller, “Dances With Wolves? China’s Integration into Digital Capitalism,” *Info,* Vol.3, No. 2., April 2001.

Zhang Junhua, “China’s “Government Online” and Attempts to Gain Technical Legitimacy,” *Asien* (Juli 2001) 80.

Zhang Weiguo, “Evading State Censorship: From the Bible to New Century Net,” *China Rights Forum* (Fall 1998), http://www.hrichina.org/crf/english/98fall/e7a.html

Zheng, Cindy, “Opening the Digital Door,” *Telecommunications Policy* 18 (1994), 236-242.

Zhou, Jamila, “Internet Archive to Snitch on Workers,” *South China Morning Post*, http://prodev.learningnetwork.com/HR_Professionals/News/0000-5077-KEYWORD.Missing.htm

Appendix 1 - Glossary of Terms

Access Provider
An Internet Access Provider (AIP) connects to the global internet via a Backbone Service Provider and sells a service where they get their customers' IP packets to the internet and receive IP packets from the internet and route them to their customers. Today the customer's IP numbers are normally taken from the access provider, but whether that is the case or not is the job of the access provider to see that a route to the customer's IP number range is advertised on the internet. An access provider is traditionally, and still commonly, called an ISP (Internet Service Provider), however that term now carries connotations of also providing additional services.

AN
Access Network – A network that provides access to the Interconnecting Networks; generally an ISP

APNIC
Asia-Pacific Network Information Center – Allocates IP numbers in Asia

Application
An application is a software component that implements some particular use of the network. Typically two sorts of software components talk to each other: a server and a client. More complex arrangements are possible.

Backbone Service Provider (IN – interconnecting network)
Backbone Service Providers are invariably also access providers. Their customers are access providers which they connect to the global internet. BSP typically connect to multiple other BSP at multiple points giving a redundant, and thus reliable connection.

BBS
Bulletin Board System. – in China generally used to refer to an online discussion forum

Binary
The decimal system used by (most) humans has digits 0 to 9. The binary system used internally by computers has digits 0 and 1.

CAnet
China Academic Network – An early (1987) network operated by the Chinese Academy of Science

CAS
Chinese Academy of Science – China's foremost research organisation

CERNET
China Education and Research Network – A national educational network that is operate by the Ministry of Education

ChinaGBN
China Golden Bridge Net – a network operated by Jitong Co., aligned with the former MEI and now under MII.

Client
Software such as a WWW browser or an e-mail user interface, which connects to and uses a service provided by a server.

CNNIC
China Internet Network Information Center – Allocates domain names and keeps network statistics for China

CPIP
Capital Public Information Platform – First internet Exchange in China.

CSTNet
China Science and Technology Network – A national interconnecting network run by the CAS that connects research organisations

DNS
Names in the internet are given a hierarchical structure. So the name ‘www.lokman.nu’ was created by the owner of the name ‘lokman.nu’ which was created by the owner of the top level ‘nu’ domain. The DNS is a total standardised system which support names of this type for internet applications.

Flame
To send nasty or insulting messages, usually in response to someone's having broken the rules of Internet etiquette (called netiquette).

FTP
Original method of information retrieval on the internet. Anonymous FTP allows people who are not registered used on the ftp server to retrieve a limited range of files.

Gateway
When users are cut off from services because of incompatible protocols or security restrictions, a gateway provides a mechanism that as the name suggests, lets the user through. Examples include X.400 and other e-mail gateways. Gateways are increasingly a part of firewall systems and seen as having a security rather than a protocol conversion function.

Headers
Used in two similar contexts. On packets of information headers are fixed size of bits of information in exact positions at the start of the packet. Examples of header information in the IP packet include packet length and destination IP number. The other place it is used is in e-mail where the headers are just lines at the top of a text file such as Subject: or To:.

Host
Computers on the internet are normally classified as ‘hosts’, meaning end-systems and ‘routers’ which fill intermediate positions and pass packets to and fro.

ICQ
Instant messaging system that allows for online chat. Pronounce I-Seek-You.

IN
Interconnecting Network – IP-based networks that connect to the global internet network

IP
The network layer in OSI terms. At this level, computer talk to other computers by sending IP packets addressed by IP numbers.

IP number
Each computer in a TCP/IP network has one or more numbers by which it can be reached. The term ‘IP address’ is common in technical literature. However the word ‘address’ is heavily overused in communication documents and the popular term IP number is clearer. It has been the practice in the past for a computer to have a separate number for each interface, so if it had a modem and an ethernet it would have two numbers. Recently it has become common for some computers, particularly routers, to have multiple IP numbers on one interface or to share an IP number between multiple interfaces.

ISP
An ISP provides the packet-level connectivity provided by an IAP, but also offers additional services such as e-mail service or webhosting services.

MEI
Former Ministry of Electronics Industry

MFRT
Former Ministry of Radio, Film and Television. Now the Bureau of Radio, Film and Television with some functions transferred to MII.

MII
Ministry of Information Industries – Formed by the merger of MEI and MPT and parts of other ministries. Responsible for setting policies and regulations regarding telecommunications, informatics and the internet.

MPS
Ministry of Public Security – Has the responsibility, inter alia, for ensuring that the internet is not used against the interests of the State.

MPT
Former Ministry of Post and Telecommunications

Netiquette
A contraction of network etiquette. The written or unwritten rules of etiquette that govern online interaction between users on the Internet. Note: Some typical rules are a ban on profane or offensive language, a requirement to respect other users, and a ban on floods of unsolicited advertisements. Netiquette rules may be enforced by a moderator or may be self-policed by other users.

OICQ
The Chinese version of ICQ. See ICQ.

Packet
In the internet all communication take place by exchange of IP packets. Each packet has a destination IP number and a source IP number.

POP
The larger ISPs have points of presence throughout the country, which means that most of their subscribers can access the internet without having to pay non-local telephone costs.

Protocol
A protocol is a set of rules that define how entities successfully communicate. It might define the format of information or allowable requests and the meaning of responses.

Router
A router is any computer with more than one interface which is configured to forward packets. This means that when a packet comes in on one interface the router will consult its tables and may as a result send the packet unchanged out on one of its other interfaces.

Server
A computer providing a 'service' on the internet, which has a process waiting for incoming calls. The caller is the client.

Spam mail
Unsolicited e-mail distributed in large quantities, normally using third party bulk e-mail address list.

Appendix 2 – Key Government Bodies

(based on Foster and Goodman, *The Diffusion of Internet in China*, 2000)

Name	***Historical Mission***	***Interest in Internet***
The Chinese Academy of Sciences (CAS)	Scientific research policy maker and host of hundreds of research institutes	Technology transfer; Internet-oriented research and development
Chinese Academy of Social Sciences (CASS)	Provide government decision makers with information and analysis	Research regarding social impact of internet; e-commerce
Internet Information Management Bureau	New body under State Council Information Office	Ensure that ICP conform to government content guidelines
Propaganda Department of Communist Party	Make sure that media are under control of the party	Especially concerned with the influence of Western information and the role of internet as media
State Council	Highest organ of state executive and administrative power	Ensure that internet and the ministries that are involved with it are serving the interest of the state
State Council Information Office	Close ties to Propaganda Department	Oversees much of internet content policy
State Economic and Trade Commission (SETC)	Policy decisions regarding infrastructure and relationships with foreign firms	Foreign investment in China's internet infrastructure
State Planning Commission (SPC)	Control China's economic resources	Funds for infrastructure; pricing of internet services. Some of this responsibillity is being shifted to MII
Ministry of Culture	Control the distribution of cultural products	Music and movies sold on the internet
Ministry of Education	Policy maker and administrator for China's education system	Internet support for university and secondary education
Ministry of Information Industry	Combination of Ministry of Posts and Telecommunications and Ministry of Electronic Industries	Information technology decision maker and regulator
Ministry of Public Security	Police of Chinese society	Ensure internet is not used to leak state secrets, conduct political subversion, or spread pornography and violence
Ministry of Science and Technology	Policy making and financing of China's research and development	Research and development for internet
Ministry of State Security	Protect state security	Encryption; ability to decode traffic on the internet and prevent foreign services from doing so
People's Bank of China	Loans to Chinese firms	Control of electronic currency and certificate authority (CA)

People's Liberation Army	State security; also has ties to manufacturing interests	Security issues
State Administration of News and Publication	Formerly part of Propaganda Department. Gives permission for official publication	Traditional press moving to internet
State Administration of Radio, Film and Television (SARFT)	Manages cable networks	Internet acces through cable
State Press and Publishing Bureau	Regulate publishing industry	Regulate the selling of books over the internet
State Administration of Industry and Commerce	Register businesses	Register e-commerce websites; grant advertising licenses
State (National) Information Office	Disseminate information about government to the public	Internet as a tool for disseminating information
Xinhua News Agency	Monopoly news producer	Leverage and protect monopoly on news
Provincial and municipal bodies	Moving away from central government in pursuit of their own economic development	Develop internet infrastructure; attract investment through internet

Appendix 3 – Key Regulations

(based on Foster and Goodman, *The Diffusion of Internet in China*, 2000 and expanded by author)

1. MPT decision to open up computer information services and e-mail to non-MPT entities (MPT Order #675) (September 1993).
2. MPT notification concerning issues pertinent to examination, approval, and management of organisations engaging in telecommunications industry (October 1993).
3. Security regulations for Computer Industry Security (Order #147) that authorise the Ministry of Public Security (MPS) to be in charge (1994).
4. MPT rules on the management of open market telecommunications (November 1995).
5. MPT rules on examination, approval, and management of telecommunication terminal equipment (November 1995).
6. MPS requirement for users to register with the MPS (MPS #7) (January 1996).
7. The State Council's decision to allow interconnection but only through Interconnecting Networks (Order #195) (February 1996).
8. MPT regulation specifying terms and connection methods of international Internet connections (MPT #492/403) (April 1996).
9. Steering Committee on National Information Infrastructure set up on April 16, 1996 (Order #195).
10. MPT provisional rules on interconnection between special networks and public networks (July 1996).
11. MPT public notice concerning issues on management of content of telecommunications information service (August 1996).
12. MPT measures on the management of China public multimedia communication (September 1997).
13. MPT outlines ISP licensing procedures (MPT #36) (December 96).
14. The State Council Order #218 – amends #195, designates three categories of computer networks related to the Internet (May 1997).
15. MPT requirements for ICP licensing for multimedia "operators" and "providers." (MPT #28) (November 1997).
16. MPS releases regulations for use of the Internet (MPS #7) (December 1997).
17. MII attempts to assert MII responsibility over Internet regulation (MII #573) (September 1998).
18. State Council issues regulations on the use of encryption and puts National Commission on Encryption Code Regulations (NCECR) under the Ministry of State Security (MSS) in charge (State Council Directive 273) (October 1999).
19. State Council's State Information Office issues regulations regarding the release of state secrets through the Internet. The Bureau for the Protection of State Secrets in charge (January 2000).
20. MII issues regulations governing the management of Internet public information-release services (November 2000).

Appendix 4 - The Responsibilities of the MII

(taken from the MII website at http://www.mii.gov.cn)

1. to formulate development strategies, overall policy and plans for the national information industry, the telecommunications industry and the software industry
2. to draft laws and regulations governing the information industry, the telecommunications industry and software industry – to enact administrative rules – to enforce these laws and supervise their implementations
3. to make comprehensive plans for government public networks, broadcasting networks and special networks of military and other public entities and to ensure proper technical and professional administration
4. to formulate technological policies, systems and standards for the information industry and the broadcasting industry and the software industry – to administer entry licenses into networks – to monitor quality supervision and control
5. to allocate, organise and coordinate available electronic bandwidth, domain names and Internet addresses
6. to supervise the telecommunications and information service markets – to implement a business licensing regime – and to formulate methods for interconnection between networks and the settlement of interconnection methods
7. to formulate pricing policies of the telecommunications and information services industries – to supervise the implementation of pricing policies
8. to plan, build and manage special networks that are used by the Communist Party and the government – to coordinate these special networks, emergency networks and other important networks – to safeguard the security of state communications and information
9. to guide and assist the development of the information industry according to the technological development policy – to supervise industry structures, industry products and enterprises – to deploy resources in a rational way
10. to promote research and development in the electronic information industry, telecommunications industry and software industry – to organise large scale technological projects and to assist in the development of a national industry
11. to provide professional administration assistance with regard to military electronic systems and to carry out research on development strategies and policies and plans related to military electronic systems – to coordinate integration of MII plans and plans by the military and the national committee of defense technology and industry
12. to assist the promotion of informatization of the national economy and national key research projects – to guide, coordinate and organise development and utilization of information resources
13. to organise and guide the sending, allocation and settlement of accounts by monetary means through postal and electronic information transfer systems
14. to represent the government in joining relevant international organisations and in signing relevant international agreements – to organise foreign technology exchanges
15. to carry out research on policies in regard to telecommunications and information systems with the HKSAR, Macau and Taiwan
16. to compile statistics on the information industry and to report news about the information industry
17. to deal with matters assigned by the State Council

Appendix 5 - Specific Internet Crimes

(taken from ChinaOnline)
http://www.chinaonline.com/issues/internet_policy/NewsArchive/Secure/2000/October/C00102312.asp

1. Violating relevant state laws and invading computer information systems containing information about state affairs, state defense and the most advanced science and technology of the state;
2. Producing and spreading computer viruses and establishing devastating programs to attack computer systems or communications networks, thus causing damage to such systems or networks;
3. Violating relevant state laws, arbitrarily stopping the operation of computer networks or communications services, thereby interrupting normal operations of such networks or services;
4. Spreading rumours, slander or other information via the Internet for the purpose of overthrowing the state government, overthrowing the socialist system, or breaking up the country and destroying the country's unity;
5. Stealing or leaking state-classified information or military secrets via the Internet;
6. Igniting racial, ethnic hatred and discrimination, and destroying racial and ethnic unity via the Internet;
7. Organising cults or contacting cult members via the Internet to destroy the implementation of state laws and administrative regulations;
8. Engaging in swindles and burglary via the Internet;
9. Selling defective products or making false claims on commodities and services via the Internet;
10. Concocting and spreading false information via the Internet to influence securities trading and futures trading;
11. Establishing pornographic Web sites, Web pages, or providing links to pornographic sites on the Internet to spread such information, including those from books and magazines, motion pictures, video and audio products, and still images;
12. Insulting other people or fabricating stories to slander others via the Internet;
13. Illegally intercepting, changing, or deleting other people's e-mail or other data information, thus infringing upon other people's freedom of communication;
14. Infringing upon other people's rights to intellectual property via the Internet;
15. Damaging other people's business reputation and product reputation via the Internet.

Appendix 6 – Censorship: an Example

(as found on http://aweek.top263.net)
Last visited on 17 June 2001
Translation by author

aweek， 你好,
您的站点内容有关言论
违反了现行国家法律和政策
请尽快和我们联系.

aweek, how are you,
your website has content that violates the current
national law, regulations and policy
please contact us as soon as possible.