Copyright Statement

The digital copy of this thesis is protected by the Copyright Act 1994 (New Zealand).

This thesis may be consulted by you, provided you comply with the provisions of the Act and the following conditions of use:

- Any use you make of these documents or images must be for research or private study purposes only, and you may not make them available to any other person.
- Authors control the copyright of their thesis. You will recognize the author's right to be identified as the author of this thesis, and due acknowledgement will be made to the author where appropriate.
- You will obtain the author's permission before publishing any material from their thesis.

General copyright and disclaimer

In addition to the above conditions, authors give their consent for the digital copy of their work to be used subject to the conditions specified on the Library Thesis Consent Form and Deposit Licence.
Censorship and Everyday Forms of Resistance in Chinese Cyberspace

Xiaojie Cao

A thesis submitted in fulfilment of the requirements for the degree of Doctor of Philosophy in Media Studies

The University of Auckland, 2015
Abstract

Have Chinese netizens been negative targets of internet censorship? Does the internet bring any democratic change to Chinese society? Questions like these have troubled me for a long time. The mainstream Chinese internet studies assert that Chinese authorities have controlled the internet well and made it serve their authoritarian domination. This stance, if not overstating the power of the control system, has underestimated the challenges facing it. Another popular observation is that the internet alone may not introduce significant change (at least, not Western-style democracy) to the existing Chinese political regime. Then, what?

Approaching from a bottom-up perspective, this thesis focuses on various challenges faced by the internet control system in China: various forms of internet resistance that make control less effective or thorough. Increasing numbers of Chinese netizens utilize all kinds of weapons in their online resistant activities: technological weapons (circumvention tools and hacking activities) and symbolic weapons (including discursive, iconic, audio/video and rhetorical weapons). It further argues that various resistant activities can connect together and show a kind of symbolic power to make real socio-political change more possible. Chinese netizens have adopted a remarkably resilient online culture that avoids and manipulates state control, while celebrating a freedom of expression that is globally unique.

Using two main methods of netnography and multimodal analysis, this research collects and analyzes data from social network sites, blogs, micro-blogs, and video-sharing sites, etc. acquired by participatory observation in the cyber field, as well as second-hand data (e.g., news coverage and existing studies).
This thesis applies a resistance framework to explain the struggles and dynamics of the Chinese internet. On the one hand, internet resistance is unlikely to bring fundamental challenges to the political system. On the other hand, internet resistance helps to create fissures in internet governance and make it less effective, echoes other resistant forms domestically and globally, and develops new identity politics for participants. A complex and nuanced understanding of internet censorship and internet politics in China may benefit our research on similar issues in other authoritarian contexts.
To My Parents
Acknowledgements

I would like to express my special appreciation and thanks to my main supervisor Dr Luke Goode, and co-supervisor Dr Xuelin Zhou, for their continual guidance and support, without which this thesis may have needed more time. Thanks for encouraging my research and for helping me to grow as a scholar.

Thanks to the participants of the 12th China Internet Research Conference, ANZCA Annual Conference 2015 and of our department’s PhD Work-in-Progress Days, many of whom have offered helpful comments. I also thank the teachers in Media, Film and Television (known as the Department of Film, Television and Media Studies before 2014), particularly Nick Perry, Misha Kavka, Katherine Sanders, Nabeel Zuberi, Laurence Simmons, and Allan Cameron. My gratitude extends to the organizers of inspiring seminars every Thursday afternoon. Thanks to my PhD colleagues Curt Fu, Yong Liu, Hang Yin, Ting Luo, Jingjing Zhang, Xiaoting Liu, Debjani Mukherjee, Jonathan Albright, and Mark Stewart. Thanks as well to the teachers at the Student Learning Centre, Susan Carter in particular.

There are some scholars to whom I want to show my specific gratitude: Dr Astrid Nordin, Dr Johan Lagerkvist and Dr Xiaochun Zhang. I have not met them physically, but they do not hesitate to email their research on the Chinese internet to me. Astrid has even shared her manuscript of a journal article, and Johan has shared his doctoral thesis. Thanks to Dr Joyce Nip and Dr Bingchun Meng for their advice and support of my future research plans.

My thanks also extend to Jill Perrott, Neil Todd, Nick Mudge, Karilyn Fairburn and other Kiwi friends, who have read sections of my research and made helpful comments.
I deeply thank my family, particularly Jan and Carol, for their mental support for my doctoral research. My daughter Carol, a wonderful Christmas gift for us in 2014, has brought me increased joy and happiness at my final stage of PhD study.

Special thanks to Dr Olivia Macassey for copy-editing this thesis.

Thanks to the joint scholarship award from the China Scholarship Council and the University of Auckland for the financial support of my PhD research from 2011 to 2015.

I would also like to thank my two anonymous examiners.
Table of Contents

Abstract ...................................................................................................................................................... i

Acknowledgements ................................................................................................................................... v

Table of Contents .................................................................................................................................... vii

Lists of Figures and Tables ........................................................................................................................ x

Abbreviations ........................................................................................................................................... xi

List of Publications ................................................................................................................................... xiii

INTRODUCTION ......................................................................................................................................... 1

Background ............................................................................................................................................... 1

Literature Review and Research Focus ................................................................................................. 6

Theoretical Framework .......................................................................................................................... 16

Research Methods .............................................................................................................................. 29

Thesis Structure and Content .............................................................................................................. 37

CHAPTER I. CENSORSHIP IN CHINESE CYBERSPACE ................................................................................ 40

Internet Censorship: Objectives and Regulations ............................................................................. 40

The Architecture of Internet Censorship ............................................................................................ 46

Internet Companies and the Operation of Censorship .................................................................... 55

Cyberculture Characterized by Censorship ......................................................................................... 65

CHAPTER II. CONDITIONS FOR INTERNET RESISTANCE ........................................................................... 69

Changing State-Society Relations ........................................................................................................ 69

The Power of Alternatives .................................................................................................................... 77

Grassroots Resistance ........................................................................................................................... 87

The Making of Resistant Youth ........................................................................................................... 94

Adaptive Control .................................................................................................................................... 101
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>III.</td>
<td>TECHNOLOGICAL RESISTANCE AND TECHNOLOGICAL WEAPONS</td>
<td>107</td>
</tr>
<tr>
<td></td>
<td>Guerrilla Warfare on Existing Platforms</td>
<td>107</td>
</tr>
<tr>
<td></td>
<td>Dimensions of Hacking Resistance</td>
<td>112</td>
</tr>
<tr>
<td></td>
<td>Organized Hacking: Circumvention 1.0</td>
<td>120</td>
</tr>
<tr>
<td></td>
<td>Scattered Hacking: Circumvention 2.0</td>
<td>128</td>
</tr>
<tr>
<td>IV.</td>
<td>THE POWER OF DISCOURSE</td>
<td>139</td>
</tr>
<tr>
<td></td>
<td>Multiple Themes of Discursive Strategies</td>
<td>140</td>
</tr>
<tr>
<td></td>
<td>The Mechanism of Discursive Resistance</td>
<td>149</td>
</tr>
<tr>
<td></td>
<td>Esoteric Writing: Modes of Expression</td>
<td>156</td>
</tr>
<tr>
<td></td>
<td>Discursive Weapons of the Weak</td>
<td>162</td>
</tr>
<tr>
<td>V.</td>
<td>EXTENDING THE SYMBOLIC POWER</td>
<td>168</td>
</tr>
<tr>
<td></td>
<td>Politicizing Images</td>
<td>169</td>
</tr>
<tr>
<td></td>
<td>Historicizing Audio and Video Weapons</td>
<td>181</td>
</tr>
<tr>
<td></td>
<td>Rhetoric of Symbolic Resistance</td>
<td>190</td>
</tr>
<tr>
<td></td>
<td>Silence as Political Rhetoric</td>
<td>195</td>
</tr>
<tr>
<td></td>
<td>The Power and Limitation of Symbolic Resistance</td>
<td>199</td>
</tr>
<tr>
<td>VI.</td>
<td>A TYPOLOGY OF NETWORKED RESISTANCE</td>
<td>205</td>
</tr>
<tr>
<td></td>
<td>Networked Grassroots Resistance</td>
<td>206</td>
</tr>
<tr>
<td></td>
<td>Routine Resistance</td>
<td>215</td>
</tr>
<tr>
<td></td>
<td>Rumor as Resistance</td>
<td>218</td>
</tr>
<tr>
<td></td>
<td>Resistance in the Guise of Entertainment</td>
<td>223</td>
</tr>
<tr>
<td></td>
<td>Politics of Networked Resistance: The Case of China</td>
<td>227</td>
</tr>
<tr>
<td>Conclusion</td>
<td>Everyday Forms of Internet Resistance</td>
<td>231</td>
</tr>
<tr>
<td></td>
<td>Understanding Internet Resistance</td>
<td>234</td>
</tr>
</tbody>
</table>
Lists of Figures and Tables

**Figures**

- Figure 1. Population of Chinese netizens (1995-2014) ................................................................. 2
- Figure 2. The Number of Internet Regulations in China, 1994-2011 .................................................. 42
- Figure 3. Some Images from the Campaign of “Putting Clothing on Famous Paintings” ............. 172
- Figure 4. Esoteric Images Containing Ironic Meanings ................................................................. 176
- Figure 5. Three Cartoons by Rebel Pepper ................................................................................... 178
- Figure 6. A Screenshot of *Interstellar* (2014) on AcFun.tv ........................................................ 187
- Figure 7. Three Types of Silence in Chinese Cyberspace ............................................................... 196
- Figure 8. Images of the Postcards Sent to Guo Baofeng .............................................................. 213
- Figure 9. Everyday Forms of Resistance in Chinese Cyberspace .................................................. 232

**Tables**

- Table 1. The First Generation Circumvention Tools Used in Mainland China ......................... 121
- Table 2. Proxy Server Users in Mainland China (%) ................................................................. 127
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACG</td>
<td>animations, comics and games</td>
</tr>
<tr>
<td>BBS</td>
<td>bulletin board system</td>
</tr>
<tr>
<td>CASS</td>
<td>China Academy of Social Sciences</td>
</tr>
<tr>
<td>CCP</td>
<td>Chinese Communist Party</td>
</tr>
<tr>
<td>CCTV</td>
<td>China Central Television</td>
</tr>
<tr>
<td>CDA</td>
<td>critical discourse analysis</td>
</tr>
<tr>
<td>CDT</td>
<td>China Digital Times</td>
</tr>
<tr>
<td>CERNet</td>
<td>China Education and Research Network</td>
</tr>
<tr>
<td>CIA</td>
<td>Central Intelligence Agency</td>
</tr>
<tr>
<td>CNNIC</td>
<td>China Internet Network Information Center</td>
</tr>
<tr>
<td>CSTNet</td>
<td>China Science and Technology Network</td>
</tr>
<tr>
<td>DDoS</td>
<td>distributed denial of service</td>
</tr>
<tr>
<td>DIT</td>
<td>Dynamic Internet Technology</td>
</tr>
<tr>
<td>DIY</td>
<td>do it yourself</td>
</tr>
<tr>
<td>DNS</td>
<td>domain name server</td>
</tr>
<tr>
<td>DPI</td>
<td>deep packet inspection</td>
</tr>
<tr>
<td>F/OSS</td>
<td>free and open source software</td>
</tr>
<tr>
<td>GAPP</td>
<td>General Administration of Press and Publication</td>
</tr>
<tr>
<td>GFW</td>
<td>Great Firewall</td>
</tr>
<tr>
<td>GIF</td>
<td>Global Information Freedom</td>
</tr>
<tr>
<td>GIFC</td>
<td>Global Internet Freedom Consortium</td>
</tr>
<tr>
<td>HRIC</td>
<td>Human Rights in China</td>
</tr>
<tr>
<td>IBB</td>
<td>International Broadcasting Bureau</td>
</tr>
<tr>
<td>ICP</td>
<td>internet content provider</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technology</td>
</tr>
<tr>
<td>ISP</td>
<td>internet service provider</td>
</tr>
<tr>
<td>LGBT</td>
<td>lesbian, gay, bisexual and transgender</td>
</tr>
<tr>
<td>MII</td>
<td>Ministry of Information Industry</td>
</tr>
<tr>
<td>MIIT</td>
<td>Ministry of Industry and Information Technology</td>
</tr>
<tr>
<td>MOC</td>
<td>Ministry of Culture</td>
</tr>
<tr>
<td>MPS</td>
<td>Ministry of Public Security</td>
</tr>
<tr>
<td>MPT</td>
<td>Ministry of Posts and Telecommunications</td>
</tr>
<tr>
<td>NATO</td>
<td>North Atlantic Treaty Organization</td>
</tr>
<tr>
<td>NED</td>
<td>National Endowment for Democracy</td>
</tr>
<tr>
<td>NGO</td>
<td>non-governmental organization</td>
</tr>
<tr>
<td>PRI</td>
<td>Public Radio International</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>P2P</td>
<td>peer to peer</td>
</tr>
<tr>
<td>PX</td>
<td>paraxylene</td>
</tr>
<tr>
<td>RFA</td>
<td>Radio Free Asia</td>
</tr>
<tr>
<td>PRC</td>
<td>People’s Republic of China</td>
</tr>
<tr>
<td>RSF</td>
<td>Reporters Without Borders (Reporters Sans Frontières)</td>
</tr>
<tr>
<td>SARFT</td>
<td>State Administration of Radio, Film and Television (former name of SAPPRFT)</td>
</tr>
<tr>
<td>SAPPRFT</td>
<td>State Administration of Press, Publication, Radio, Film and Television</td>
</tr>
<tr>
<td>SARS</td>
<td>Severe Acute Respiratory Syndrome</td>
</tr>
<tr>
<td>SCIO</td>
<td>State Council Information Office</td>
</tr>
<tr>
<td>SEO</td>
<td>search engine optimization</td>
</tr>
<tr>
<td>SIIO</td>
<td>State Internet Information Office</td>
</tr>
<tr>
<td>SMS</td>
<td>short message service</td>
</tr>
<tr>
<td>SNS</td>
<td>social networking site</td>
</tr>
<tr>
<td>UGC</td>
<td>user-generated content</td>
</tr>
<tr>
<td>WCP</td>
<td>West-Chamber Project (Xixiang Jihua)</td>
</tr>
<tr>
<td>WOW</td>
<td>World of Warcraft</td>
</tr>
<tr>
<td>WTO</td>
<td>World Trade Organization</td>
</tr>
<tr>
<td>VOA</td>
<td>Voice of America</td>
</tr>
<tr>
<td>VPN</td>
<td>virtual proxy network</td>
</tr>
</tbody>
</table>
List of Publications

During the course of the PhD research, the candidate was the sole author on the following:

**Peer-reviewed Journal Article**


**Peer-reviewed Conference Proceeding**


**International Conference Papers**


INTRODUCTION

Background

In November 2014, China held a state-sponsored World Internet Conference in Wuzhen, a town near Hangzhou where China’s top e-commerce company, Alibaba Group, is located. Top executives from Chinese tech companies, including Baidu, Sina, Alibaba and Tencent, as well as representatives from Apple, Amazon, Microsoft, Samsung, LinkedIn, Facebook, Google, and Line – ironically, the service of the latter three had been blocked by the Great Firewall (the GFW) within Mainland China – gathered to discuss the theme of “an interconnected world shared and governed by all.” This was the first state-sponsored internet conference in China, though China has been connected with the outside world via the internet for over 20 years. Chinese authorities wanted to use this event to show that the Chinese internet is an important (and unique) part of the “world” internet. The conference tried to promote an ideologically-colored concept of “internet sovereignty” (which was one of nine so-called consensuses in the draft of the Wuzhen Declaration, a declaration proposed by the conference Organizing Committee but passed over by the conference attendees) to its Western counterparts, and also attempted to legitimize state control of the Chinese internet as an issue of sovereignty by implying that Western counterparts should not get involved. A very

---

1 The reason why the first letter of the term “internet” has not been capitalized in this thesis is that I treat the Chinese internet as a unique subset of the big whole “Internet.” This is a reminder as well as an emphasis of the fact that nowadays, though they share many similarities, the internet(s) (in the plural sense) in different countries often have different features – particularly when we take into consideration the features of the countries themselves (e.g., democracies, authoritarian regimes).
interesting detail is that conference participants were freely provided with a special “iWiFi-Wuzhen,” via which blocked foreign websites, such as Facebook, Twitter, and Voice of America (VOA), were accessible. This had not happened before. If the holding of a “world” conference has revealed, at least partially, the attempt of the Chinese Communist Party (CCP) to build its internet sovereignty, then this trick of iWiFi-Wuzhen has shown how flexible the Chinese authorities’ internet control policy could be. The cluster of issues that has arisen from this conference thus becomes an epitome of the internet in China.

Figure 1. Population of Chinese netizens (1995-2014)


Not long ago, several relevant things have happened at the state level. In 2011, the State Internet Information Office (SIIO) was set up to coordinate various departments and ramp up the oversight of internet content and activities. The SIIO was one of the two organizers (the other was the local government) of this World Internet Conference. In December 2013, the Central Leading Group for Internet Security and Informatization (which was chaired by the current president Xi Jinping²) was formed, with the purpose of “leading and coordinating

² Chinese names often place surnames before given names. This thesis follows this convention and puts all Chinese names in this order (e.g., Mao Zedong, Deng Xiaoping, and Xi Jinping). I make an exception for those
internet security and informatization work among different sectors, as well as draft national strategies, development plans and major policies in this field” (N. Zhu, 2014). The Chinese authorities have shown increasing emphasis on the internet and its governance in recent years, and the holding of this “world” internet conference is new evidence of such emphasis; while some commentators urged everyone to bear in mind that the Chinese internet was still under severe control by the CCP.

China started its internet project in 1986 and the first email was sent out on 14 September 1987 from Beijing to Germany, reading “Across the Great Wall, we can reach every corner in the world.” (Ironically, ten years later, a digital Great Wall was built, to prevent Chinese people from freely reaching all corners of the world.) In the first decade, the internet was limited to institutions (e.g., universities and research centers) and the elite (mainly political and academic). It was not until 1995 that the internet theoretically became available for ordinary people, despite the fact that the relative expense of computers and internet connections was still very high and internet access before 2000 was still confined to the elite strata in research institutes, state organizations, and foreign companies; penetration rates were below 2% (Taneja & Wu, 2014). Since 1997 the population of Chinese netizens has

---

3 The question of the exact time of China’s first connection to the public internet remains open. Some scholars argue that the starting time was in 1993 (Kalathil & Boas, 2010), others argue that China first established a connection to the internet in April 1994 and about 23,000 Chinese were estimated to have restricted internet access at that time, all government officials and select academics (R. J. Deibert, 2002; MacKinnon, 2008). Here I choose 1995 as the time when ordinary Chinese people were allowed to go online, which has been confirmed by other resources such as J. L. Qiu (2004) as well as my co-supervisor Xuelin Zhou (2015) who mentioned to me that “1995 was the year when I first used email upon return to China from England in November. I was teaching at a university then; internet communication had just started to be a common practice then.”

4 In the early days of the internet development, for those who could not financially afford personal computers, internet bars became a good alternative (Yongming Zhou, 2008b). A computer in later 1990s China could cost $1,000-1,200 dollars, a fact which has also been confirmed by Xuelin Zhou (2015) whose first computer in early 1996 cost him around $1,000 dollars. An ordinary family earned only around $600 dollars per year at that time (according to 1996 government figures); furthermore, in 1999, the monthly cost for an
undergone a stable increase (CNNIC, 1997-2015), becoming the biggest population of netizens in the world, having surpassed the U.S. in 2008. The most recent record of this population is 668 million (which is 48.8% of the whole population of the country). This huge population, along with the changing dynamics of user structure (with more and more ordinary people getting online, and internet access no longer the privilege of the elite), has revealed some far-reaching economical, cultural and political effects on Chinese society. Various domestic internet-related tech companies have appeared; some have disappeared and some others (e.g., Sina, Baidu, Tencent, Alibaba and Huawei) have survived and become magnates. Besides institutions involved in the developing internet in the early days (most of which received public funding), tech companies, targeting mainly commercial interests, have also provided Chinese netizens plenty of platforms and online choices – from email service, bulletin board services (BBS], blogging, and instant messengers in the early days to various recent social networking choices – and helped to cultivate a very distinctive culture in Chinese cyberspace (Damm, 2007; Giese, 2004).5 China has now become the world’s biggest producer of desktop computers (Austin, 2014, p. xiii). The population of mobile internet users, emerging at the beginning of new millennium, has risen steadily since 2006 to a current population of 594 million (CNNIC, 1997-2015). Because of the fast development of high-

internet connection (totaling 60 hours) was about $ 29 dollars, plus the phone line connection fee which was 50 cents per hour (cited from Collings, 2001, pp. 192-193).

5 There are two main reasons why I choose to use “Chinese cyberspace” than the narrowly-sensed one “cyberspace in China” in this thesis. First, “Chinese cyberspace” refers to those Chinese-language cyberspace physically hosted both within Mainland China and overseas. Though censorship and resistance often happens to those in China, overseas Chinese cyberspace may also get involved in the process of censorship and resistance, particularly when they want to extend their readership into those who locate physically inside China. Second, it becomes hard to define “cyberspace in China” nowadays, since cyberspaces often are borderless, particularly considering their readership. Overseas Chinese can access those cyberspaces physically hosted in China, and Mainland Chinese could also access Chinese cyberspaces hosted physically overseas (often through circumvention tools). Yet, in this thesis, Chinese cyberspace mainly refers to those cyberspaces in China.
speed network technologies and cheap terminal devices over this period, more and more online content in the form of texts, images, audio and video materials can be easily and conveniently created, accessed and shared seamlessly via mobile devices (smart phones in particular). The reason why the Chinese authorities express an increasing emphasis on the internet (never-ending regulation and tighter censorship as one of many such expressions, see Endeshaw, 2004) is at least partially rooted here.

The attitude of Chinese authorities toward the rising of the internet is very ambiguous (Kluver, 2005b). On the one hand, the Information and Communications Technology (ICT) industry is becoming the most dynamic sector in China’s economy (Harwit, 2008; Q. Meng & Li, 2002). From the Government’s point of view, the development of the internet, echoing a dominant doctrine that “science and technology is the primary productive force,” can bring a “technological leapfrogging” to the modernization of China (Hughes & Wacker, 2003; Tai, 2006; Zheng, 2008); and in official discourses, authorities at different levels are encouraged to maximize the positive potentiality of the internet-related economy as well as of e-governance (e.g., that of infrastructure for e-governance). On the other hand, the authorities have realized increasingly the potential risks of the internet in the socio-political sphere and its power – the internet may offer new spaces for expressing dissent and opposition, spread negative or even “harmful” information, and erode the regime’s authority and legitimacy. Accordingly, more

---

6 This is particularly true of the bottom-up modes of resistance, which I discuss in this thesis. Various forms and types of technological and symbolic resistance against the CCP and its internet control policies, in return, become reasons for the CCP to extend its control of the Chinese internet. It seems to be a dead-locked control-resistance-control loop. However, what should be pointed out is that this thesis does not take the liberal assumptions for granted. Privacy, free access to information, and freedom of speech are three of many common bases for resistance against internet censorship. But when it comes to pornography, violence and terrorism, these theoretical bases should be questioned. It is often arguable where the line should be drawn between freedom and restriction, and how much privacy (if necessary) users should agree to give up in the name of national security. China undoubtedly goes much further than this and takes close control of topics beyond the scale of pornography and violence. Both the censors and resisters have their own diversities, and it
and more regulations (which will be discussed in Chapter One) have been introduced with the aim to minimize the negative potentiality of the internet. Regulations are just one of many methods of internet control. Over the past 20 years, Chinese authorities have utilized and developed a complicated internet control system and a globally unique internet control philosophy (with the holding of the World Internet Conference as a hidden attempt to legitimate this control philosophy). Although the Chinese authorities’ original understanding of an information society is “less people-centred” and “more in the mould of the materialist and technocratic traditions” (Austin, 2014, p. xv) and is particularly focused on the internet’s “commercial applications” while restricting its “political implications” (Yongming Zhou, 2006, p. 138), the government is also the most active promoter of the development of the internet in China.

**Literature Review and Research Focus**

The Chinese internet has received huge academic attention since almost the very beginning, and this seems never to have weakened over subsequent years. Monographs (e.g., Austin, 2014; Chase & Mulvenon, 2002; Damm & Thomas, 2006; Harwit, 2008; Hughes & Wacker, 2003; Jacobs, 2012; Lagerkvist, 2010; F. Liu, 2011; Ng, 2013; So & Westland, 2010; Tai, 2006; Ventre, 2014; G. Yang, 2009; Zheng, 2008; Yongming Zhou, 2006), special journal issues, edited volumes (e.g., Breslin & Shen, 2010; Herold & Marolt, 2011; Johnson,

---

is this diversity that makes issues about internet censorship and resistance more complicated and harder to make simple judgments about.

---

7 These can be found in journals of Chinese studies and internet studies, in both Chinese and English. There are even journals focusing mainly on the Chinese internet – *Wangluo Chuanbo* [New Media] that has been published monthly in Chinese since April 2004, and *Zhongguo Wangluo Chuanbo Yanjiu* [Chinese Journal of Computer-Mediated Communication] (since 2007).
relevant majors in tertiary institutions, dissertations, and numerous journal articles have appeared that are devoted to Chinese internet studies. An increasing number of disciplines, such as economics, marketing, sociology, politics, and cultural studies, have entered into this field of research. Drawing on the existing literature, including some existing review articles (Herold & de Seta, 2015; Kluver & Yang, 2005; J. L. Qiu & Bu, 2013; J. L. Qiu & Chan, 2004; Wei, 2009), this section illustrates a current research map for the Chinese internet, outlining the ways in which scholars do research about Chinese internet, from what kinds of perspective, main themes, and the tensions between these difference approaches and ideas.

**Chinese internet studies from a non-political perspective**

In the early days of Chinese internet development (approximately 1995-2002), the majority of domestic scholars understood the internet to be a new medium after print, radio and television (e.g., Herold & Marolt, 2011, pp. 7-8; Peng, 2005). Studies from this perspective include the regulation, characteristics and history of this new media (Herold & Marolt, 2011; Kuang, 2001; Peng, 2005), existing communication theories (such as agenda-setting and spiral of silence) in this new information context (Xie, 2004; Yuqiong Zhou, Pan, & Yan, 2007),
media convergence (J. Meng & Zhao, 2006; Y. Xu, 2006), the interaction between mass media and the internet (Tang & Sampson, 2012), and inequality of access and internet literacy (S. Pan & Jordan-Marsh, 2010; B. Wei, 2006). In general, it is unsurprising that mainstream internet research projects at that time were undertaken by scholars from media backgrounds, majors in internet research were affiliated to journalism schools (or departments), and dissertations about the internet (and the Chinese internet) were mainly from media studies. (This situation has not changed much, even today).

The economic dimension of the internet, and market perspectives, have formed an indispensable part of Chinese internet studies (X. Du, 1999; Lai & To, 2012). Commerce-oriented studies focus not only on impacts of the internet on existing economic sectors such as manufacturing, wholesale/retail, and banking (Riquelme, 2002; Tan & Ouyang, 2004) but also on new phenomena such as online shopping and purchasing behaviors (Vuylsteke, Wen, Baesens, & Poelmans, 2010; Q. Ye, Li, & Gu, 2011), e-business models (Q.-Y. Su & Adams, 2005), and online advertising (e.g., word of mouth) (S.-C. Chu & Choi, 2011; Ji & Zhang, 2009). The internet has been seen as a great power in re-organizing China’s economy and providing possibilities not only for existing sectors but also for rising businesses and helping to build a new information economy (Q. Meng & Li, 2002; Wong & Ling, 2001).

The social and psychological perspective is another popular perspective for Chinese internet studies, which suggests the internet as a new source for pathological problems (particularly of adolescent and college students) (J. Gong et al., 2009; R. L. Huang et al., 2009; Mai et al., 2012; C.-X. Shen, Liu, & Wang, 2013; Szablewicz, 2010; D. Zhang et al., 2007). Addiction to online games (Golub & Lingley, 2008), sensation seeking (Mei & Liu, 2012),
and online pornography (Liang & Lu, 2012), among others, have been greatly investigated. The internet is believed to be an important factor for users’ depression and other mental illnesses, with discourses of internet disorder, technostress, poison, and online narcotics being created and used to describe the negative influence of the internet, contributing to an emerging moral panic about new technology. Internet addiction clinics are established and treatments introduced to solve this problem (Funk, 2007; Lin-Liu, 2006). Cyber crimes and the regulation of abnormal internet usage have also gained academic attention in China (Keith & Lin, 2006).

Different platforms at different phases of the Chinese internet (e.g., emails, BBSs, blogs, micro-blogs, and other social networking sites [SNS]) and internet-related companies have attracted academic attention as well (e.g., Batjargal, 2007; Chase & Mulvenon, 2002; Fuchs & Trottier, 2013; L. Qiu, Lin, & Leung, 2013; Sullivan, 2012; H. Yu, 2007a). Other heated issues include the differences between developed and developing provinces (or urban versus rural areas) in China regarding internet development, internet bars (often approaching from anthropological way, such as J. L. Qiu, 2013a; J. L. Qiu & Zhou, 2005; Yongming Zhou, 2006, 2008b), and the mobile internet in China (J. L. Qiu, 2013b; R. Wei, 2006).

Although the non-political approach to the Chinese internet has also been applied by scholars outside China, it is mainly applied by domestic scholars. This reveals an interesting phenomenon among domestic scholars: the majority of them have kept a certain distance from politically sensitive issues. A possible reason is that research activities themselves are under the control of the CCP and many Chinese scholars have long practiced a kind of “self-censorship” in their daily research process (Holz, 2007). They are more likely to touch on non-political issues which are relatively safer for them. However, this does not mean that domestic
The political approach to the Chinese internet

The political dimension of the Chinese internet has become a very important theme of Chinese internet studies, with issues relevant to democracy, civil society and the public sphere having been extensively discussed. Many scholars agree that historically the internet has brought unprecedented freedom of speech to Chinese people (MacKinnon, 2010; L. L. Zhang, 2006) because in the pre-internet era information flow was largely controlled by the authorities and ordinary people were left little, if any, institutional space to speak out. The internet functions as a new alternative channel for speaking truth: many serious social problems which are seldom touched on by traditional media are disclosed in cyberspace. It has also become a convenient method of social mobilization, which sometimes causes changes to social reality (Hand, 2006; K. C. Yang, 2011). Those who see the influence of the internet towards Chinese politics and society as positive, emphasize the power of the internet (G. Yang, 2009) and treat

---

10 In fact, issues such as how netizens use the internet to fight against corruption have actually been heated topics for Chinese scholars recently (e.g., C. Du & Liu, 2011), though such issues are not entirely politically sensitive (since anti-corruption has been a popular political campaign for new leaders in recent years, see the last section of Chapter Two for more discussion). There are even domestic scholars touching on politically sensitive issues. Thanks to Luke Goode (2015b) for reminding me that Hu Yong, a professor from Peking University, has utilized a very critical perspective to look at the Chinese internet and censorship. Scholars like Hu may realize the difficulty in publishing critical research domestically; this is the main reason why many of them turn to international conferences and/or journals. More cases of this happen on a small scale. For example, in the classrooms at tertiary levels, some teachers may frequently present contentious views in their lectures. The authorities, of course, try to control and discipline such teachers by pressuring the relevant universities to talk with them or even dismiss them. A recent case happened in the University of Macau when two professors were fired because of their political views (Hao, 2014).
cyberspace as an online civil society or a virtual public sphere (M. Jiang, 2011; S. Li, 2010; Tai, 2006; G. Yang, 2003b; Zheng, 2008), with case studies of environmental activism (Sima, 2011), non-governmental organizations (NGO) (G. Yang, 2005), anti-corruption movements (X. Zhou, 2009), rights advocacy (Hung, 2010), and dissidents and activism (X. Zhou, 2009). The internet has the potential to empower the weak in the “battle” (Xiao, 2011a) or “cat and mouse game” (Endeshaw, 2004; Thompson, n.d.) between the strong (the authorities) and the weak (e.g., dissidents) and the networking function of the internet is able to bring incremental changes to the Chinese society through “constructing loosely structured networks” (F. Shen, Wang, Guo, & Guo, 2009), or enabling people to “dig the CCP’s grave” (Kristof, 2005b).

The internet may have a liberating potential for some Chinese people, but the Chinese government is very smart in subverting the technological possibilities that the internet offers (Herold & de Seta, 2015). Various methods have been used to control the internet, including infrastructure of censorship (e.g., the GFW) (R. J. Deibert, 2002; Neumann, 2001; Winter & Crandall, 2012), regulations (Harwit & Clark, 2001; Lacharite, 2002; Taubman, 2002) and concrete punishment (Zheng, 2008, pp. 70-78). Bearing these in mind, some believe that the emancipatory potential of the Chinese internet is very limited (Abbott, 2001; Shie, 2004) and others argue that the internet does not automatically bring democracy to China but rather the role of the internet in China is “more likely to involve political evolution – not revolution” (MacKinnon, 2008). Metaphorical discourses such as “flying freely but in the cage” (E. Huang, 1999) and “dancing with shackles” (a phrase once used often to describe the situation of journalism in China) within Chinese internet studies reveal skepticism of the role of the internet in promoting democracy in China or leading to social change (B. Yang, 2012).
Scholars also question the positive theories (e.g., of the public sphere) about the Chinese internet (Herold, 2011b). The Chinese internet, argues Damm (2007), is “more a playground for leisure, socializing, and commerce than a hotbed of political activism” (p.290).

In what seems to be a recent trend, an increased amount of research has focused on specific political issues in Chinese cyberspace, for example issues of online nationalism (Breslin & Shen, 2010; Y. Jiang, 2012; J. L. Qiu, 2006; X. Wu, 2007), political discourse in cyberspace (C. Han, 2013; Thurlow & Mroczek, 2011), internet events and their socio-political influences (M. Jiang, 2011; J. L. Qiu & Chan, 2011), the politics of youth culture and the internet (Clark, 2012; Johnson, et al., 2014), the political usage of different platforms (e.g., BBSs, blogs, micro-blogs) (S. S. Wang & Hong, 2010) and online ethos (S. Li, 2010). These studies have enriched our understandings of the concept of internet politics in China, yet have also provoked new questions: for example, of how to understand the relationship between entertainment-oriented cyberculture and internet politics. Present-day scholars (e.g., Herold & de Seta, 2015; Voci, 2010) are inclined to believe that the entertainment-oriented dimension undermines the political dimension of ordinary people’s online activities. It is right that Chinese people’s online activities are not always about politics (R. W. Chu & Cheng, 2011) but embrace entertainment, personal relationships (L. Guo, 2007) or satirical rhetoric (H. Yu, 2007a). Obvious differences certainly exist between entertainment and real politics, but they also overlap with and become vehicles for one another (Brants & Neijens, 1998; Tryon, 2008; Wilson, 2011), as shown in concepts such as fan activism (Brough & Shresthova, 2012; Earl & Kimport, 2009; Jenkins, 2012). This is also the case in Chinese cyberspace (a closely
controlled space), yet has not been fully investigated.\textsuperscript{11} It may be arguable that in Chinese cyberspace every activity is definitely a political activity, but, as discussed later in this thesis (Chapter Six in particular), online entertainment activities often become objects of internet censorship, thus the entertainment realm becomes a political field in which control, and resistance to control, happens. This thesis will try to provide a new understanding of entertainment and apathy as hidden means of internet resistance.

Internet censorship and resistance represents the most dynamic theme of Chinese internet politics research. The majority of such studies approach this theme from a top-down perspective and are about “control and freedom” (F. Yang, 2014). On the one hand, research has emphasized the vulnerability and inefficacy of internet regulation (Harwit & Clark, 2001; Taubman, 2002), the administrative and technical difficulties involved in internet regulation (Lacharite, 2002), and the roles of counter-filtering technologies as well as anonymity (which enable users to express their ideas) in challenging internet censorship (Clayton, Murdoch, & Watson, 2006; Leberknight, Chiang, Poor, & Wong, 2012; Stevenson, 2007). The potential role of economic imperatives (e.g., China’s accession to the World Trade Organization [WTO] and its need for foreign investment) in encouraging the state to open up internet policies has also been studied (R. J. Deibert, 2002; Endeshaw, 2004). On the other hand, research conducted recently adopts a more pessimistic tone, though in the early days a few studies also adopted this tone (Bamman, O’Connor, & Smith, 2012; MacKinnon, 2008, 2012). Various

\textsuperscript{11} The political meanings of online entertainment phenomena (such as online spoofs) have been investigated by only a few scholars (e.g., B. Meng, 2011) and been defined as “alternative political discourse” which offers political criticism as well as emotional bonding for participants. In Chinese, online spoof is named \textit{egao}, a term which generally refers to all types of audio, visual or textual spoofs in cyberspace. The official English-language newspaper \textit{China Daily} defines this as “a popular subculture that deconstructs serious themes to entertain people with comedy effects” (Q. Huang, 2006), and it is characterized by humor, revelry, subversion, grassroots spontaneity, defiance of authority, mass participation, and multi-media high-tech. See Chapter Five for more discussion on online spoof.
studies have found that in China tolerance of internet censorship runs relatively high, and many Chinese people even show support for internet censorship (e.g., D. Fallows, 2008; S. Guo & Feng, 2012). Moreover, internet monitoring, arrest and imprisonment of those who cross the line, produce the effect of social surveillance and self-censorship, or even a kind of political apathy (Stern & Hassid, 2012). However, as Yang and Liu (2014) argue, existing research mainly focuses on how Chinese netizens’ online behaviors are passively affected by internet censorship, whereas how Chinese netizens actively manage to bypass the restriction in their everyday online experience has been insufficiently studied.

In fact, dimensions of internet resistance have been visited by only a few scholars, though they do not actually refer explicitly in their research to concepts such as “resistant” or “resistance” (terms which, as shown in the coming chapters of my thesis, have rich meanings for many Chinese netizens). They use specific terms such as digital activism (G. Yang, 2003c, 2009, 2014a), contentious internet (Xi Chen, 2012; B. Meng, 2010), contesting cyberspace (R. Han, 2012), or anti-censorship (Leberknight, et al., 2012; Mathieson, 2006). These terms help us to understand the tense dimensions of Chinese cyberspace, but they may not be able to fully explain issues regarding internet censorship and its various challenges. The few researchers who have investigated netizens’ resistance against internet control mainly focus on a small group of people, such as pro-democracy activists who attempt to circumvent internet control policies or the dissidents who are technologically savvy (R. J. Deibert, 2002). The

12 Particularly digital activism, as Gladwell (2010) argues, is mainly based on weak social ties and using corporate platforms, which may induce limits for activism and security risks for the activists, and become slacktivism. Others challenge this and suggest digital interaction and activism are not inherently grounded in weak ties but also can be the basis for socially deep ties (Coleman, 2013a, pp. 209-210), and suggest that digital media has also played a critical role in fomenting and helping sustain more traditional social movements such as the counter globalization protests (Bennett, 2003; Juris, 2008).
often-used anti-blocking and filtering technologies (e.g., email tunneling, mirror sites, and anti-censorship proxies) have been analyzed as well (Clayton, et al., 2006; Leberknight, et al., 2012; Shklovski & Kotamraju, 2011). But how ordinary people resist internet censorship has not been fully investigated in the existing academy. Neither have other issues such as the development of these circumvention technologies (as responses to the update of the GFW), the effectiveness and influence of such anti-censorship technologies. Although a few scholars have touched on issues relevant to encoded discourses (Dong, 2012; Gleiss, 2015; MacKinnon, 2008; Nordin & Richaud, 2014) and rhetoric such as parody (H. Gong & Yang, 2010; B. Meng, 2011; Tang & Bhattacharya, 2011; Xiao, 2011a; G. Yang & Jiang, 2015), approaching these issues from a specific perspective of symbolic resistance remains rare in current scholarship. This thesis will not only cover the discussion of discursive resistance but also extend it to a broader concept of symbolic resistance (by means such as encoded words, resistant images, audio and video materials, and rhetorical means).

**The focus of this thesis**

This research will approach the Chinese internet from a political and cultural perspective, particularly focusing on internet censorship in Chinese cyberspace and the bottom-up resistance faced by such censorship. Based on the previous literature review, there are four general questions I want to answer clearly in this thesis. First, what has been the development of circumvention technologies? How do ordinary Chinese netizens (including internet-savvy users) take advantage of various existing technologies to challenge the internet censorship system? What are the socio-political influences of such technological resistance? Second, how do ordinary netizens utilize symbolic forms of resistance to bypass the regulatory system?
What are these forms, and how do these forms enable Chinese netizens to form alternative ideas (pro-democratic ideas, criticism of the CCP, for example) and communicate sensitive information? Third, can resistance to internet censorship become connected and collective, and if so, how? And fourth, how do we understand the political meanings of resistance to internet control in China? Can netizens create a specific culture of resistance in cyberspace, and potentially make changes to the socio-political status quo? Or, theoretically, how does Chinese internet resistance extend our understanding of internet politics?

**Theoretical Framework**

**Politicizing the internet: politics via the internet and politics of the internet**

There are various theoretical concepts dealing with issues of the internet and politics, such as internet politics (Chadwick, 2006), info-politics (or information politics, Rogers, 2004), online politics (Anderson, 2003; Yongming Zhou, 2006), networked politics (Couldry, 2012; Sey & Castells, 2004), cyberpolitics (Hill & Hughes, 1999), digital politics (Barber, 2001), among many others. As a general description of politics via the internet (though variously named), these concepts are used in similar situations, with some nuanced differences or emphases, and in a quite narrow way: the extension of real-world politics in a traditional, formal, bureaucratic or institutional sense, such as teledemocracy (looking at the role of the internet in reinforcing or undermining democracy, also known as electronic democracy or e-democracy) (Anderson, 2003), e-governance (Backus, 2001; Dawes, 2008), election campaigns via online platforms (Cogburn & Espinoza-Vasquez, 2011; Tumasjan, Sprenger, Sandner, & Welpe, 2010), activism in the internet era, the political power of social media (Patrut & Patrut, 2014; Shirky, 2011), and Wiki government (Noveck, 2009). In short, these
concepts cover various kinds of formal political issues in the era of the internet. The emphasis is the actual effect of the internet on the transformation of the formal political process (i.e., political campaign, debate, choice, representation, and decision-making) and institutions of governance. And this dimension of internet politics can be defined as politics via the internet (Levin, 2002; or “internet-based politics,” see Sey & Castells, 2004, p. 366).

However, this mainstream understanding of internet politics is only part of the story. Internet politics means not only the formal political issues in the new era of the internet, but also the new political issues that appear from the internet itself, such as issues of information poverty and the digital divide (Castells, 2010; J. L. Qiu, 2009), pirate politics (Burkart, 2014), protocol politics (DeNardis, 2009), hacktivism (Goode, 2015a; Jordan & Taylor, 2004), internet control, privacy, surveillance and censorship. This second dimension places much greater emphasis on the politics of the internet itself. This thesis argues that when discussing internet politics these two dimensions are often mixed together and cannot be separated from one another. For example, when doing research into internet censorship and instances of resistance in Chinese cyberspace, we should not only focus on the GFW, keyword censorship system, and anti-blocking technologies, but also bear in mind the censorship institutions, regulations and enforcement, and even the broad political regime and political climate per se. Focusing on one dimension and overlooking the other is not enough to reach a full understanding of the issue.13

Internet politics can also be understood through a binary opposition: hard politics and soft politics. Internet technologies seems to have helped extend or challenge the meaning of “hard”

---

13 For the sake of convenience, hereafter (unless otherwise stated) I use “internet politics” as a general term for these similar concepts to refer to issues of the internet and politics.
politics (which can be roughly described by a cluster of adjectives such as traditional, grand, serious, formal, bureaucratic, institutional, and top-down) to a much more “soft” politics (which may be described by another cluster of adjectives such as individual, micro, symbolic, informal, everyday, and bottom-up). Soft politics focuses more on power relationships between individuals and institutions, and on political implications of ordinary people’s banal activities (such as consuming and entertainment) and identity politics. Though discourses, texts, images, audio and video materials, or various symbols, played important roles in the practice of hard politics before the internet era, they have become an even more important part of soft politics in cyberspace. Soft politics may be disguised in a playful and apolitical (or non-political) way. It is easy to find cases in which netizens tend to engage with the seemingly “non-political” realm in politically consequential ways – expressing political sarcasm and initiating civic discourse as spinoffs of entertainment content (Jenkins, 2014; Taneja & Wu, 2014). For example, Chinese online gamers sometimes perform resistance to internet censorship by producing satirical images and slang (see Chapter Six for concrete examples). Political protests can also be mobilized through social networks in the guise of leisure-oriented activities (Poell, de Kloet, & Zeng, 2014). This makes any website with networking capacities potentially a target of censorship (MacKinnon, 2008; Marolt, 2011; B. Meng, 2011; Xiao, 2011a; G. Yang, 2009), and thus they can become a field of resistance as well. However, soft

---

14 Internet politics focuses more on individuals. For example, networked politics, argue Sey and Castells (2004, p. 378), is individualized politics, which tries to connect to many other individuals, suddenly identified as recognizable citizens. The emphasis of bottom-up within internet politics echoes the concept of infrapolitics of the powerless in Scott’s sense as well (1990, pp. 183-201).

15 The concept of power helps us to understand these two kinds of politics here. The internet has brought a new power relationship between the ruling system and the ordinary people (netizens). Despite the popular preconception that the internet empowers increasing numbers of ordinary people, acknowledging this new power relationship is a good starting point. As discussed later in my thesis, the internet may not be able to provide netizens power in a traditional sense, but it does provide them a symbolic power (more micro, informal, quotidian and bottom-up).
politics cannot be understood only as expressive. It can instrumentally empower some ordinary netizens and cultivate a new kind of political identity.\textsuperscript{16} This soft dimension of politics should, as this thesis will argue in later chapters, be fully recognized particularly in the Chinese internet context (a space often under serious government scrutiny). A more detailed discussion on the issue of apolitical or de- and re-politicization (Nordin & Richaud, 2014) in Chinese cyberspace will be discussed in Chapters Five and Six.

\textbf{Three theoretical turns in Chinese internet politics research}

This thesis focuses on Chinese internet politics, particularly various issues relevant to internet censorship and resistance. Before reaching a theoretical framework for this thesis, it is worth making a general review of theories applied in existing Chinese internet politics research, which has undergone three theoretical turns over the past 20 years: a postmodern turn, a humanistic turn, and a narrative turn.

Firstly, Chinese internet politics research has encountered a postmodern turn, from modern-style discourses such as of democracy, empowerment, public space, civic discourse, civil society and authoritarian, to postmodern-style discourses such as those of carnival, infotainment, playfulness, consumption, everydayness and decentralization.

There are two opposite stances in the modern-style discourses, some insisting that the internet does bring, at least, some democracy to Chinese society (Kluver & Qiu, 2003; Zheng, 2008), others arguing that the internet cannot function as a democratic force simply because it exists in China (MacKinnon, 2008) and the fulfilling of the democratic dimension of the internet will need some very important factors – such as economy (Abbott, 2001; Shie, 2004),

\textsuperscript{16} It should be borne in mind that both hard politics (such as participation in internet-based political activities) and soft politics may of course be practiced by some ordinary netizens at the same time.
regime types and negotiation formats (Drezner, 2009), and participants’ political will and social purpose. However, both schools of thoughts are concerned with democracy and seem to believe that the internet technology (represented by BBSs and blogs, among others) does provide spaces and opportunities for political engagement and to cultivate a new kind of civic discourse. Similarly, research into the Chinese internet from the perspective of public sphere and civil society abounds (MacKinnon, 2008; Tai, 2006; G. Yang, 2003a; Zheng & Wu, 2005), yet, at the same time, has invited lots of challenging criticism as well. Some critics argue that the public sphere is not an idyllic site of participation but rather an arena of continuous struggle (e.g., B. Yang, 2010). Others argue that the existence of an online civil society in China remains more of a working hypothesis, or a collection of potentials, than a well developed reality (S. S. Wang & Hong, 2010). In relation to platforms in particular, some scholars treat examples such as blogs as an ideal platform to form a virtual public sphere (Esarey & Xiao, 2011), while others point out that Chinese blogs are frequently personal diaries and the majority of bloggers show limited interest in politics (S. S. Wang & Hong, 2010). Though we cannot judge the political significance of a platform only by the majority of its users (since a few politically interested bloggers do use blogs as a political tool, and can drive public opinion to challenge the technological dictatorship), defining the Chinese internet as a public sphere provides more questions than answers. Furthermore, although Chinese online opinion formation, based on informal conversations between netizens, can often challenge the status quo power (M. Jiang, 2010), this challenge is unlike that seen in its Western counterparts. Democracy involves participation, yet in China, the participation is
quite different from that in the West – people often have to communicate sensitive topics and content covertly and indirectly (rather than overtly and directly).

Scholars who focus on the theme of authoritarian control via the internet emphasize that the Chinese authorities have long practiced a control policy on the internet in which many Chinese netizens enjoy relative freedom (to choose to use which domestic platforms or services) but the freedom is restricted to a bearable degree (Kalathil & Boas, 2001; Zuckerman, 2014). For this group of scholars, the internet actually serves to bolster regime legitimacy and thus helps to develop a networked authoritarianism (MacKinnon, 2010, 2011a), or an adaptive authoritarianism (T. C. Chen, 2010). The possible (and limited) political deliberation enabled by the internet has been defined as internet “authoritarian deliberation” (B. He, 2012; M. Jiang, 2010). Questions of how the authorities utilize new technologies to create an electronic panopticon (Lyon, 1993; Tsui, 2003) and how some online activism becomes just forms of political “exit” and sucks up political energies (Zheng, 2008, pp. 164-165), can also be found within the authoritarian approach. For these scholars, the internet seems to have helped Chinese authorities to build a cultural hegemony in Gramsci’s (1971) sense, but, as discussed later, it places more emphasis on the powerful system and may overlook the power of the weak (i.e. anti-hegemonic endeavor among netizens) (Dong, 2012).

An increasing number of postmodern-style theories have been introduced to explain Chinese internet culture and politics in recent years. Some scholars apply Bakhtin’s carnival theory and define the majority of Chinese netizens’ online activities as carnivalesque activities which are featured as more playful yet less serious – and can thus hardly be treated as democratic activities (Herold & Marolt, 2011; B. Meng, 2011; W. Wu, Fore, Wang, & Ho,
Others approach from the perspective of infotainment and treat the internet as merely a tool for entertainment rather than a tool for politics (Bachman, 2010; Leibold, 2011; G. Yang, 2011) and *egao* (or playfulness) as a main feature of Chinese cyberculture (H. Gong & Yang, 2010; Yongming Zhou, 2008a). However, the internet as an entertainment tool does not mean that serious political issues are excluded in cyberspace, quite the opposite: scholars (e.g., H. Yu, 2007a, 2007b) find that everyday consumption of internet entertainment, seemingly apolitical, often turns out to be political in the end. The nuanced relationship between mundane online activities and engagement in political issues has provoked new theories such as cute cat theory (Zuckerman, 2008, 2014) and relevant research (Mina, 2014). This postmodern turn in Chinese internet politics research does help to update our concept of internet politics beyond narrow, the formal, institutional definitions. I will take this more quotidian mode seriously in this research.

Secondly, with more and more studies focused on the people who actually use the internet, a humanistic turn has occurred in Chinese internet politics research as well. Since the emergence of the internet, too much research that focuses mainly on either the technology as a whole (X. Du, 1999; Kluver & Qiu, 2003; Q. Meng & Li, 2002; Tang & Sampson, 2012; R. Wei, 2006), or on its various platforms such as BBSs, blogs and SNSs (S.-C. Chu & Choi, 2011; Dong & Wang, 2011; Kissel, 2007; H. Yu, 2011), has left the human dimension (particularly users) largely invisible (G. Yang, 2011). However, more recently, studies about how users use different internet platforms, under what circumstances, and for what purposes, have also received increasing academic attention (e.g., Bei, 2013; W. Zhang & Mao, 2013; X.

---

17 Cute cat theory, proposed by Ethan Zuckerman (2008, 2014), which is more like a metaphor rather than a theory, means that there is a huge gap between those who prefer to share mundane content about cute cats and those who engage actively in political issues. The name itself is very postmodern.
Zhou, 2009; Y. Zhou, 2009). This humanistic turn has been echoed by some meta-reviews of Chinese internet research such as one by Herold and de Seta (2015) that states that one future of Chinese internet research might lie in “how people in China are using the Internet to do what they want to do, be it politics or entertainment, or shopping” (p. 79). This theoretical turn implies that the factor of human agency (e.g., user intention and practice) deserves equal, if not greater, emphasis – both the human factor and the non-human factor (e.g., hardware and software) contribute to a dynamic, multi-leveled, heterogeneous digital culture, and they become entwined with one another.

Thirdly, the focus on a human dimension also echoes a further theoretical turn from grand narrative to micro narrative (or little narrative, see Malpas, 2003) in contemporary Chinese internet politics research. Unlike grand narrative which focuses on grand issues and theories (e.g., modernization), micro narrative focuses more on marginalized, seemingly trivial and banal online activities (i.e., expressions of the quotidian, entertainment consumption, personal stories, pieces of sensation of socio-political problems and identities), yet at the same time, tries to investigate the political-cultural significance underneath them. The micro-narrative reminds us to see the complexity and multi-layered dimensions of the internet and its effects on ordinary people’s everyday lives, and other issues that may be overlooked by grand narrative. Not only do an increasing number of studies pay attention to internet users, but also an increasing number focus on ordinary internet users and their everyday online activities (e.g., McDonald, 2013). The previously marginalized issues of sex and pornography on the Chinese internet have recently attracted increasing academic attention (Farrer, 2007; Jacobs, 2009; McDonald, 2013). Other research also conducted by Tom McDonald (2014) applies ethnographic fieldwork to research on parents in rural China who share photos of their new-born babies with friends in QZone (a popular SNS service provided by Tencent).
2007, 2012), so have the once marginalized communities such as lesbian, gay, bisexual, and transgender (LGBT) people (Ho, 2007, 2009; D. Zhang, et al., 2007), female netizens (J. Feng, 2013; Lo, 2009), migrant workers (Cartier, Castells, & Qiu, 2005; W.-C. Chu & Yang, 2006; Law, 2012; J. L. Qiu, 2009), online game players (Ernkvist & Ström, 2008; Golub & Lingley, 2008; Nie, 2013; W. Wu, et al., 2007), and fan groups (Rowe, Ruddock, & Hutchins, 2010; W. Zhang & Mao, 2013). These studies generally suggest that on the one hand the internet has changed, or at least helped to challenge, the power of the traditional elite; on the other, it has empowered more ordinary people (who have platforms and chances to speak out and be heard). The sharply increasing amount of user-generated content creates a kind of legitimization effect for some ordinary netizens and marks their online activities as an emerging subculture that cannot be ignored. The increasing emphasis on the online everyday activities of ordinary people (or the micro narrative), however, does not mean that marginalized and banal activities are isolated from a broad and grand socio-political context. In this research, I will pay much attention to the interaction between marginalized and seemingly trivial activities and their broad context.

In discussing these three theoretical turns, I do not mean to challenge the theories used prior to them, but rather to suggest that such theories are not sufficient for a better understanding of the Chinese internet. In reality, both theories used before and after these three turns still coexist in current scholarship, which is much likely to be the case in the foreseeable future.

19 Although a new hierarchy may be created, with a small group of people on the top and the majority at the bottom, in the internet era, the majority at the bottom, becoming connected by the internet, can form a new mass power (be it negative, such as e-mobs, or positive, such as contributors to Wikipedia).
A proposed theoretical framework for this research

Acknowledging the above three theoretical turns, this section proposes a “resistance framework” with which to study Chinese internet politics. Approaching from the bottom-up, the resistance framework emphasizes the daily struggles of the users against the relatively powerful, the technologies utilized in their everyday resistance and their online culture (which features such as discourses and images) formed within this digital hierarchy. Internet resistance includes two parts: offline resistance (such as rural land-protection protests, pro-democracy movements, environmentalist activities and other forms of rights resistance) which extends to cyberspace (O'Brien & Li, 2006; G. Yang, 2013, 2014b), and online resistance, which mainly centers around internet censorship, information freedom, piracy, free and open-source software (F/OSS), etc. Since most offline resistance is sensitive for the authorities, when such resistance gets online, it becomes a sensitive issue online as well (thus needs to be censored). Although this resistance framework may not be able to explain everything in Chinese cyberspace, this thesis will try to show that at least many political issues (particularly regarding censorship) within Chinese cyberspace can be well explained by this framework, as the Chinese internet is under close control; and where there is control, there is resistance.

Firstly, in common with the postmodern turn, this resistance framework will treat those issues of carnival, infotainment, or any seemingly apolitical phenomena as practices and rich forms of political resistance.20 When apolitical phenomena (such as a satirical phrase or

---

20 It should be noted here that, with the conceptual resource of Bakhtin’s carnival theory, most scholars emphasize the resistant side of carnival. They assimilate cyberspace to a carnivalesque piazza, seeing netizens’ online behavior as a challenge to the ruling system. The more covert, tricky side is generally neglected, which show the power of the dominant system. See for instance Knight (2004) who analyzes the satirical metaphor behind Saturnalia and finds that in fact “satire, like law, is an agent of social control.” (p. 27) More explicitly, Schechner (1995) claims that “with rare exceptions, today’s festivals and carnivals are not inversions of social order but mirrors of it.” (p. 48) Thus, by way of temporary and ritual overturning, carnival seems to be a covert strategy for social control rather than a real, serious challenge to the existing system. This thesis thus
image) become virally popular, they may become political (or at least partially political) eventually (see Chapters Four to Six for concrete examples). The resistance framework is not a negation of either the democratic framework or the authoritarian framework: it just provides another way to explain the issues with which these two frameworks grapple, but cannot fully explain. For instance, the democratic framework, assuming there is respectful or rational deliberation between the dominant and the subordinated, has greatly ignored the tense relationship between these two groups (with the existence of ubiquitous censorship); while, although the authoritarian (or hegemonic) framework has recognized the tense relationship within Chinese cyberspace, it seems not to have paid enough attention to political possibilities of the weak (the users).

Secondly, in common with the humanistic turn, this resistance framework values both technologies (e.g., anti-GFW tools) and human beings (e.g., resisters). Although this research does not focus on specific platforms, discussions about platforms occasionally occur when discussing issues of censorship and resistance. It emphasizes netizens – particularly low-profile netizens – who use these internet platforms, how they use them, and for what purposes. This emphasis, however, does not mean it is a populist framework.21 Although the majority population of Chinese netizens are ordinary people, a traditional elite such as socially active journalists, human rights lawyers, public intellectuals, pro-democracy activists, dissidents, or sympathetic officials, also take part in digital activities. The generalized viewing of internet

acknowledges the resistant dimension of carnivalesque activities as well as their compliant dimension. For more details, please see Chapter Six of this thesis.

21 Regarding the status quo, the wish to treat Chinese netizens as citizens who can automatically take part in civil or democratic practices, or to treat Chinese cyberspace as a Habermasian public sphere, is one-sided. It is common sense that social and economic status can affect netizens’ ability to access the internet. Since there are many thresholds of accessibility, cyberspace could not be an equal place for everyone. I will bear in mind the political-cultural dimension of the internet, or, the digital divide, in Chinese cyberspace.
users as an undifferentiated populace may miss the “heterogeneity and cacophony of public opinion in Chinese cyberspace today” (M. Jiang, 2010). Similarly, looking at Chinese internet resistance via the theoretical lens and tools of Marxism, labor and class analysis (e.g., J. L. Qiu, 2009; J. L. Qiu, Gregg, & Crawford, 2014) may not be able to fully explain the symbolic dimension of internet resistance. The focus on internet users is a focus on the different groups of participants and the cooperative and competitive relation between each group, on their participation in the rapid proliferation of mashed-up images and insinuations, and their creativity and resilience in their use of Web 2.0 tools for political ends (Zuckerman, 2014).

There are two questionable yet popular approaches that need to be noted here. The first one is that of treating netizens as the grassroots. Though the concept of grassroots has presupposed an oppositional dichotomy between the dominant system and the subordinated group, it misrepresents the subordinated group as a homogeneous group, and furthermore makes the mistake of assuming that the voices heard in Chinese cyberspace are necessarily those of the “grassroots.”

Another one is labeling cyberculture as a kind of youth culture. This approach explains only part of the reality in Chinese cyberspace, since although the majority of users are young people, an increasing number of older people are online nowadays. But both approaches have provided useful sources for my framework – the dimensions of resistance and incorporation of internet politics have been largely practiced by young netizens (via various means) and about problems of the grassroots.

---

22 In this research, the term of “the grassroots” is strictly treated as a reference to those who are socially, economically and politically disadvantaged and at the bottom of the social strata (such as famers and migrant workers); while the term of “ordinary people” is much looser, including “the grassroots” as well as other people who may not be treated as “the grassroots” such as ordinary journalist and lawyers.
And thirdly, in common with the narrative turn, this resistance framework pays much attention to internet censorship resisters (an academically neglected group) and their everyday resistant activities, forms and products (including discourses, texts and images or, more generally, symbols). This thesis will not only treat resistance in Chinese cyberspace as a special kind of narrative event, and the genres and rhetoric of symbolic means to circumvent censorship as crucial parts of a culture of resistance, but will also pay attention to the micro-narratives of some ordinary netizens (considering their daily activities in cyberspace and their interaction with the dominant censors).

This resistance framework has been greatly inspired by some theorists, particularly James Scott, Michel de Certeau and Antonio Gramsci. Internet resistance may vary in form: not only technological forms (e.g., hacking activities) but also symbolic forms. In general, such abundant (and, sometimes, banal) forms of resistance can be understood from the sense of Scott’s (1985, 1990) “the weapon of the weak” or de Certeau’s (1984) “la perruque” (the wig) which challenge the powerful system in minor ways yet makes domination unsuccessful at the micro and everyday level. Gramsci has also sparked my thoughts about the relationship between authoritarian hegemony and resistance, and the consequences of internet resistance: this resistance framework adopts neither a positive nor a pessimistic, but rather a complex, stance to examine and determine the consequences of internet resistance. What is meant here by “complex stance” is that it will take account of both these potential consequences: on the one hand, serious internet control and censorship has helped to form a unique cyberculture, within which both hard politics (for a small group of netizens) and soft politics are cultivated;
and on the other hand, the political dimension of cyberculture in return may cast influence on the authorities’ internet control policies and other relevant political issues.

### Research Methods

One danger in Chinese internet politics research, as there are in many existing studies, is that examples are selected to illustrate a preconceived argument (either positive or negative), with the complex socio-political conditions of such examples being overlooked. In order to avoid falling into this methodological bias, my research will, firstly, look at a range of complex and sometime contradictory examples of ordinary users’ online engagement, and, secondly, observe the political implications of resistant activities within the broader context. It acknowledges not only the technological context (the development of hardware and software) (Grant & Meadows, 2010, pp. 3-6), but also the socio-political and cultural context (e.g., the organizational infrastructures, socio-political system, and the tense relationship between elite culture and popular culture) (G. Yang, 2009). Another problem is that, as mentioned in the previous section, too much research has approached from the top-down perspective and failed to fully cover issues at the micro and everyday level. This research will approach the resistant phenomena in Chinese cyberspace from the ground up and try to invite more academic attention to the political implications of micro, scattered, everyday and low-profile resistance. Approaching from the bottom-up and at a micro level, however, does not mean that only the low end of the spectrum (users of the internet) will be discussed while the other end (the authorities) is left untouched. In fact, since the interaction between these two groups regarding internet censorship is the core theme of this research, activities of both the censors and those being censored will be analyzed (though the latter attracts more of my attention).
It is unrealistic for researchers to conduct surveys or interviews within Chinese borders regarding internet censorship, not only because the political reality there is that they are not allowed to do so, but also because the research subjects may feel very restricted in what they can tell the researchers. I need to use a method that is relatively more naturalistic, adaptable, and focused on context. Real-world ethnographic research seems to be a good choice, but it requires me to be physically in Mainland China, in which case, again, the present-day political atmosphere there might present a significant barrier for me. This has pushed me to switch my research field from the real-world to the internet, though I know that, ideally, both offline and online ethnography will benefit us with a better understanding of the phenomenon of Chinese internet censorship and resistance. I use netnography as the main method for data collection and as the supplementary method for data analysis.

Doing ethnographic research in cyberspace(s) became increasingly popular in the 1990s and it has since provoked many debates in academic circles, about issues such as the definition of the research field and ethical considerations, with consensus hardly being achieved even today. Besides Kozinets’s (2009) methodological promotion of “netnography,” there have been many other suggested terms dealing with computer-mediated ethnography, for example, virtual ethnography (Hine, 2000), webnography, network ethnography, digital ethnography and other terms (see Correll, 1995; Markham, 1998; Markham & Baym, 2008). There are slight differences among these terms. Since there is no physical field for a netnographer to enter, some scholars define netnographic field as the field of discourse (e.g., Markham, 2005) and observe mainly texts, images and audio video materials; meanwhile, others define it as

---

23 This thesis uses the term of netnography for the sake of convenience, but I do acknowledge the slight difference between different terms.
field of relations (Leander & McKim, 2003) and social interactions become more important. At the practical level, some researchers use search engines to locate the research field and often choose to investigate more than one site (e.g., McLelland, 2002). This research treats the research field not only as field of discourse but of relations, and often involves multi-sites observation. It means firstly that I will not only focus on texts, images, audio video materials but also the interactions between different cultural groups. And secondly, I, as a researcher, will often transit from one site to another one and do my observations in more than one site during the same period of time.24 As shown in the Appendix A, I did my netnographic observation from March 2011 to August 2015 (mainly in 2014 and 2015), which involved 28 domestic and foreigner news media sites, 10 blogs, 17 portal sites and 12 social media sites (relatively, more time and attention has been put into social media sites and portal sites). I will not be able to cover every case relevant to censorship and resistance case on these sites – that is not my research goal; neither do I go into much detail about how news media sites or blogs, or online communities are involved in the process of internet censorship and resistance. I try to understand internet resistance in a more general way (e.g. everyday forms of resistance) and the socio-political context of particular cases of resistance case (e.g. the interactions and relations between different cultural groups with an emphasis on the macro rather than micro level).

24 Actually this is one of the main differences between doing ethnographic studies online and offline. In traditional point of view, an ethnographic researcher should stay in a physical site for quite a long time and he/she cannot move from site to another easily; neither can he/she observe in more than one site during the same period of time. However, internet enables a netnographic researcher to overcome the time and space barriers to some degree. On the one hand, this may have some negative influence on a netnographic researcher in regard of deep understanding of a community or a theme or producing “thick description” (Geertz, 1973); on the other hand, the flexibility of doing observation in multi-sites and in different period of times may also benefit a netnographic researcher in terms of thinking in a more comparative way and focusing on the relations between different cultural groups.
Another issue is that though it may, as Kozinets (2010, p. 75) argues, be unrealistic to conduct netnographic research without any participation online, purely “observational” or “passive” netnographic study is sometimes desirable (e.g., Beaven & Laws, 2007; Brownlie & Hewer, 2007; Langer & Beckmann, 2005; Maulana & Eckhardt, 2007). This research prefers to emphasize the observational rather than participatory dimension of netnography, in order to reduce the unnecessary influence of the researcher. This means two things. Firstly, I have made extensive use of search engines such as Google (including Google Scholar) and Baidu to collect publicly available second-hand data (in the form of texts, images, audio, and video), such as news coverage of a case, or background information of specific slang and events, or relevant research.²⁵ (See Appendix A) This has been a snowballing process, with new keywords provoked by previous search results. It should be noted that search results may not be reliable, since the results themselves are politically or commercially charged – sensitive results often being removed from the result list. An alternative yet time-consuming way to locate these “sensitive” results is, to take Weibo for example, by reviewing the Weibo pages of relevant individual users, page by page (Poell, et al., 2014). I have also used Baidu (as well as Weibo) to test if a term has been blocked. Secondly, relatively “inside” and first-hand data has been collected mainly via my observation in online communities, such as online forums (e.g., Strong China Forum, Baidu Tieba), blogs (e.g., Sina Blog), micro-blogging sites (e.g., Sina Weibo), and video-sharing sites (e.g., YouTube, AcFun and Bilibili).²⁶ This has sometimes

²⁵ I acknowledge the differences between Google and Baidu. For example, many politically sensitive phrases (e.g., June 4) that cannot be found on Baidu can be found on Google. An interesting fact is that a search site named BaiGoogledu has been created and enabled netizens to search and compare results from Baidu and Google (results showing on a split screen with Baidu on the left side and Google on the right side).

²⁶ Strong China Forum (Qiagguo Luntan) is an online forum operated by People’s Daily Online. Some scholars translate “Qiagguo Luntan” as “Strengthening Nation Forum” (M. Jiang, 2010; C. Li, 2005; G. Yang, 2003a) or “Strong Nation Forum” (Dunn, 2007; M. Wu, 2008; H. Yu, 2007b) which has a nuanced difference. Here I follow the translation available on the About page of the English version of People’s Daily Online (n.d.).
required me to register as a user before getting “inside” the communities; most often I have just used the inside identities for “silent” observation and data collection. There are a few exceptions, though. For example, in the community of Sina Weibo, I have sometimes forwarded some sensitive posts from other users; some posts were soon deleted while others might stay relatively longer (though they were eventually removed). This kind of “participation” has helped me to directly understand the censorship in Chinese cyberspace. Though there are other factors to determine the fates of these posts (including the degrees of sensitivity of the posts, the discretionary power of internet service providers, availability of human censors at that time, pressure from censors at high levels, etc.), the wording of posts (with obvious sensitive words, or more covert alternatives) should not be overlooked – an issue which will be fully investigated in my thesis. Much sensitive information flows in Chinese cyberspace when it is euphemized by symbolic means, such as homophones, pictographs, encoded words, esoteric ways of writing, or other media forms such as images, audio materials and videos (which are the themes of Chapters Four and Five). However, most of the time, this research emphasizes observation rather than participation.

Besides the above data collection means, I also use other means. Some cases of resistance (particularly those which happened in the early days of Chinese internet history) are taken

---

Baidu Tieba is affiliated to Baidu. For more information about AcFun and Bilibili, please refer to Chapter Five. Sina Weibo is a Twitter-like top social media in China. Weibo has characteristics likely to make its popularity even more sustainable than Twitter. Although the 140 character limit helps both Weibo and Twitter maintain messages within a size that can be very quickly read, much more can be expressed in 140 Chinese characters than in 140 letters or signs (see Liao, 2013). Weibo also includes options such as comments on posts in a classic BBS style and its users can transfer images, video, and sound directly into their Weibo feeds; users who retweet messages can add more characters and Weibo has more metrics encouraging input from Twitter followers, such as retweets and @mentions (as cited in S. Perry & Roda, n.d.). For more comparison between Weibo and Twitter, see Banman, et al (2012).

27 It should be noted here that when citing this first-hand data, I follow the protocol that online pseudonyms are to be treated as real names (Langer & Beckmann, 2005).
from existing research articles, dissertations, books, and academic background English-
language websites managed by Chinese dissidents (e.g., CDT), though the angle of my
analysis is often different from that of the original research. Relevant online news clippings
from magazines and newspapers have been used as data sources as well. Although these news
clippings are collected from both domestic and overseas outlets, they are mainly from overseas
(e.g., *Times*, *New York Times* and *South China Morning Post*). But, again, I bear in mind the
rhetorical and value stances of different media outlets, and try to cite only the facts rather than
be misled by the ideological judgments planted in different media discourses.

The criterion for data collection lies only in that the data is about internet censorship and/or
resistance to such censorship, and that it not be limited to first-hand or second-hand sources.
Again, it should be noted that my investigation may not be able to cover every piece of such
data. To ascertain the strength or amount of censorship and resistance in Chinese cyberspace is
not my research aim. My concern is more about deepening our understanding of the nature of
internet censorship and resistance. Relevant cases of internet censorship and resistance are
collected, which date from the very beginning of Chinese internet history until very recently.
Some cases studied in this research are popular cases in Chinese cyberspace, which means that
they are well-known not only to ordinary netizens but also to academic and traditional media
outlets. Often the popularity of a thing reveals some significance of that thing, but sometimes

---

28 The reason why domestic news clippings are seldom collected here is that issues relevant to censorship
(and resistance to censorship) are sensitive within the GFW; there is very small number, if any, of such news
clippings in domestic media outlets.

29 The ideological positioning in media discourse has long been a heated research topic in media studies.
Chinese journalism (particularly in a traditional sense) has long been Party journalism which is guided by (CCP)
Party principles (Y. Zhao, 1998). This is the reason why hardly any information about internet censorship
circulates in domestic media outlets. Meanwhile, though Western journalism (such as that in the U.K. and U.S.)
is claimed to be guided by the principle of the fourth estate and freedom of speech, it may still plant ideological
judgments when it comes to report international issues, and show positioning in its media representation of the
other (Fang, 1994; Manzenreiter, 2010).
this is not the case. For example, in recent years, official background media outlets have
tended to publish annual lists of popular cyber slang, which attracts much attention from both
scholars and ordinary netizens. But most politically-sensitive phrases (e.g., some euphemisms
for sensitive keywords) are excluded from such lists, despite being at least as popular as those
on the lists. Commercial agencies can also influence the popularity of certain cases. For
instance, a public relations department or advertising agency can easily scheme to create a hot
cyber event. If researchers only have such lists or events (still popular but being manipulated)
as research data, and do not bear in mind the external factors that affect popularity, their
findings are doomed to inadequacy.

This research tries to step inside the culture of censorship and resistance in Chinese
cyberspace. Though I may be somewhat of a digital native, as a researcher I may still
encounter issues, to which Prensky (2001) has alerted us, faced by “digital immigrants”:
researchers nowadays may struggle to update their language (that of the pre-digital age) to
reach a population of digital natives who speak a much different language (p. 2). Speaking a
new language (which is more complex than that in Prensky’s sense, since here the language is
also determined by the controlling atmosphere rather than simply a new information
technology) is part of the Chinese cyberculture. The main problem in doing research about the
Chinese internet is that, as a researcher, one may feel external pressure when conducting
research into sensitive topics. This becomes a barrier particularly for Chinese researchers, who
often practice self-censorship in their academic activities as well;30 those who are brave

30 An increasing number of scholars have realized the difficulties in doing research about the Chinese
internet, with findings such as that: “You could discuss censorship online, but only with people who understood
the pun and knew the code” and that “Dialogs about grass mud horses and river crabs is [sic] confusing to those
who don’t know the code, and it’s difficult to imagine how a serious political essay could be written to evade
censorship using these techniques.” (Zuckerman, 2014) This of course does not mean that there are no scholars
enough have to depend on circumvention tools (e.g., Virtual Proxy Networks [VPN]) to eliminate the influence of the censorship system.\textsuperscript{31}

The data collected are vast and multimodal (i.e., cyber slang, personal diaries, essays, images, audio materials and videos), so it requires the methods of multimodal analysis (such as critical discourse analysis, image and video analysis) to understand and interpret the data (it also helps to select relevant data) (Bell & Garrett, 1998; LeVine & Scollon, 2004; Salway, 2010). My focus on internet resistance lies not only on the circumvention technologies but also the symbolic strategies for dodging the censors. Particularly in relation to the discursive strategies, I treat every euphemistic discourse as social events in Fairclough’s (2010, pp. 21-38) sense. This means that discourse is not only a component of cyber expression, but also a cultural product of social practices (and thus reflects the broad socio-political context in China). Though critical discourse analysis (CDA) (Fairclough, 2010; Van Dijk, 1993) is defined as a complex, multidisciplinary – and as yet underdeveloped – domain of study, it proves to be a useful tool in political studies, cultural studies and feminist studies (Corcoran, 1989; Hall, 1981; Matheson, 2005; Thorne, Kramarae, & Henley, 1983).\textsuperscript{32} Other weapons of symbolic resistance (such as tactical images, audio materials and videos), treated also as cultural products emerging in the censorship context, will be fully analyzed in this thesis.

\textsuperscript{31} Using anti-GFW tools to reach some sensitive data may not be the case for me since I have been located physically outside the GFW while doing this research, but external pressure still exits. To be honest, it would be questionable whether I might have still chosen this sensitive research topic, had I undertaken my PhD research within the borders of Mainland China.

\textsuperscript{32} According to van Dijk (1993), critical discourse analysis presupposes “a study of the relations between discourse, power, dominance, social inequality and the position of the discourse analyst in such social relationships;” while central to this theoretical endeavor is “the analysis of the complex relationships between dominance and discourse” (pp. 249-283).
Thesis Structure and Content

This research tries to provide a new lens through which to understand internet censorship in Chinese cyberspace, by focusing on the bottom-up resistance faced by such censorship. It focuses more on ordinary netizens and their everyday resistant practice in Chinese cyberspace. The potential of this research does not mean to overturn mainstream academic arguments, but tries to provide a complex, nuanced understanding of the internet control and resistance in China. It will include eight chapters in total. This introductory chapter has clarified the existing research on the Chinese internet (particularly internet politics), and the reason why a bottom-up perspective and a resistance framework are very important to understand Chinese internet politics.

Although my research concerns are mainly about the resistant dimension of the Chinese internet and about netizens’ responses to internet censorship, it will benefit the reader to provide a chapter to contextualize my research topic as a whole, and make a general review of internet censorship in China. Chapter One deals directly with this issue. It approaches the topic from the top-down perspective and focuses on internet censorship at both the state (the regulation of internet control and the design of the censorship system) and the corporate levels (how different internet companies apply different censorship methods to balance the political requirements and commercial interests). This chapter tries to make clear the macro (socio-political system) and mesoscopic (the organizational infrastructure) background to why resistant activities are so dense in Chinese cyberspace. While Chapter One focuses on internet censorship itself (which is the main and direct condition for internet resistance), Chapter Two investigates wider socio-political conditions for resistance within Chinese cyberspace. These
conditions include, but are not limited to, changing state-society relations, the influence of alternative powers, grassroots resistance, resistant youth, and the authorities’ adaptive control policies. The conditions themselves are created by the socio-political crises that the CCP has encountered during the era of reform and opening-up, which are the main concerns the CCP and its censorship system try to control, not only in media outlets but also in cyberspace. Thus, although there are various forms of unrest in Chinese society, the reason why such conditions become conditions for internet resistance is because they have been under the serious scrutiny of government.

Chapters Three to Five focus on the weapons many Chinese netizens use to challenge internet censorship. Chapter Three discusses technological weapons, such as creative usages of existing platforms for anti-censorship purposes, anti-censorship software, and hacking the GFW. Though normally technological weapons are applied by a small group of tech-savvy netizens, it does empower some ordinary netizens to bypass the Chinese internet censorship system. Furthermore, there is a trend for technological resistance in Chinese cyberspace in which scattered hacking becomes increasingly popular. Chapters Four and Five deal with the various symbolic strategies utilized by many Chinese netizens to circumvent the top-down censorship in their everyday online lives. Compared with real-world resistance, symbolic resistance in cyberspace is much more discursive (such as using encoded language), narrative (such as using esoteric writing at the textual level) and rhetorical (such as using humor, satire and parody); and, from the perspective of media forms, online resisters may apply various means of texts, images, audio materials and even videos to express and practice their resistance. Chapter Four deals more with the theme of symbolic resistance as discourse (i.e.,
cyber slang and esoteric writing), and Chapter Five investigates image and other media forms as symbolic resistance and the rhetoric of such resistance.

After the discussion of various resistant weapons of Chinese netizens, a natural yet urgent question is how they are utilized in specific resistant activities and how different types of resistance are connected and become networked resistance. Chapter Six presents a typology of networked resistance: networked grassroots resistance, routine resistance, rumors as resistance, and resistance in the guise of entertainment. The question of how networked resistance in Chinese cyberspace may contribute to our understanding of internet politics (and particularly of internet resistance) will also be clarified in this chapter.

The concluding chapter deals mainly with two issues: the initiative of Chinese netizens and their demonstration of non-compliance with the censorship system by creative involvement in various resistant activities, and the political influence of internet resistance against censorship, in the sense of everyday, symbolic and micro politics. Though present-day internet resistance may not be able to fundamentally challenge the Chinese political system, it does function as a certain form of political participation and way of enlightenment for increasing numbers of Chinese netizens. With China as a significant case, this whole thesis tries to provide a complex understanding of the relationship between internet and democracy; findings may be of value in the study of other authoritarian regimes. The limitations of this research will be clarified in the conclusion.
CHAPTER I. CENSORSHIP IN CHINESE CYBERSPACE

Before the investigation into the bottom-up resistance against internet censorship in the coming chapters, this chapter contextualizes the project and makes a general review of internet censorship in China. It approaches from the top-down perspective and focuses on internet censorship at both the state and the corporate levels. At the state level, the regulation of internet control and the design of the censorship system, two prominent issues, are analyzed in the first two sections. The following section specifies how, at the corporate level, different internet companies apply different censorship methods to balance political requirements and commercial interests. The chapter concludes by discussing the general consequences of internet censorship.

**Internet Censorship: Objectives and Regulations**

The CCP has long controlled the cultural products circulated within Mainland China, including traditional media, literature, historical text books, and products of entertainment industries (movies, historical dramas on the state-run television stations and even popular music). By controlling media ownership, the nation’s powerful ideologists govern the personnel system in media organizations and establish strict censorship mechanisms to ensure that the publicized political content advocates the party policy (J. L. Qiu, 1999). The content of almost every publication receives censorship, particularly content relevant to ethnical issues (in relation to Xinjiang, Tibet, and Taiwan in particular), historical issues (particularly

---

33 In 2009 after a riot in Urumqi, the capital of Xinjiang Autonomous Region in northwest China, Chinese authorities shut down almost all the internet service within this area for over one year, expecting to prevent the
sensitive events involving the CCP, such as the famine that followed Mao’s disastrous Great Leap Forward), social issues (including the Falun Gong organization which authorities denounced in 1999 as “heterodox sects”), pornographic, violent materials, and cyber-crime.  

In the early years of Chinese internet development, the authorities utilized the means that had been used to govern traditional media, to govern the rising internet. Censorship colors all aspects of internet activity, not only privacy and law enforcement, but freedom of expression, civil activities, the structure of markets, investments for future internet infrastructure, and much more (Gasser, Faris, & Heacock, 2013, p. 5). Inspired by Leberknight, et al.’s (2012) model, Chinese internet censorship can be understood in terms of two aspects: the socio-political aspect and the technical aspect. The socio-political aspect includes, but is not limited to, information related to “subversive” political movements and controversial actions including the 1989 Tiananmen Incident, support for a free Tibet, the Falun Gong spiritual movement, criticism of China’s human rights and social justice records, independent news media, and pro-democracy ideas. The CCP has listed nine principles to regulate netizens’ online behaviors and urged them to avoid them.  

---

34 In 2002 at the National Conference on Judicial, Procuratorial and Public Security Work, Luo Gan, then a member of the Political Bureau and secretary of the Central Commission on Politics and Law, identified cyber crimes as one of the three most import problems facing the party and the country (Henderson, 2007, p. 110). Furthermore, Jiang Zemin, then president of China, once warned that the Party and the Government should develop, utilize and regulate the internet as a “new battlefield of public opinion and propaganda” (Z. Li, 2003, p. 84).

35 These principles comprise: (1) instigating resistance to and impeding the enforcement of the Constitution, laws and administrative regulations; (2) promoting subversion and the overthrow of the communist system; (3) advocating separatism and secession from the state; (4) promoting racial hatred and discrimination; (5) disrupting social order through fabrication and spreading rumors; (6) promoting superstition, indecency, pornography, gambling, violence and terrorism, etc.; (7) insulting or defaming others; (8) undermining the credibility of state organs; and (9) violating the Constitution, laws and regulations. (Z. He & Zhu, 2002)
from economic changes, or any other “soft” information that may exert a negative impact on China’s international image (e.g., air pollution and the HIV/AIDS issue) (Q. Yang & Liu, 2014). The technical aspect generally involves various anti-GFW tools and discussions about how to breach censorship. However, not all these topics are wiped out from Chinese cyberspace; in contrast, much sensitive information (disguised in various ways) has circulated online, a topic that will be fully investigated in the coming chapters.

**Figure 2. The Number of Internet Regulations in China, 1994-2011**

In order to discipline online activities, the authorities have launched a series of laws and regulations. Since February 1994, internet regulations have been created not only by state council but also by responsible departments at both state and provincial levels, by the four major national internet backbones (ChinaNet, GBNet, CSTNet and CERNET), and by internet companies themselves. Although a detailed content analysis of the regulations published over these years is beyond the scope of this research, a general discussion reveals that the total number of regulations reached 115 during the 1994-2011 period, peaking at 21 in 2000 alone.

**SOURCE: CNNIC’s “China: Overview of Internet Laws and Regulations” (CNNIC, n.d.-a)**
Regulations in the early years focused more on the infrastructure of the internet, shifting in recent years to the content dimension. Not all these regulations are targeted at censoring the internet, but over half of them directly point to issues of internet censorship. (See Appendix B for a list of major regulations regarding internet censorship.) The Telecommunications Regulations (2000) stipulates that users should not evade the state-owned telecommunication infrastructure and use private infrastructure for communication, which means that when connecting to the internet, all users need to apply this rule. In general, these regulations have strict restrictions on foreign capital that aims to be involved in the domestic internet business. Internet content receives especially wide monitoring. For example, the Interim Provisions of Administration of Internet Websites’ Engaging in News Publication Services (2000) tries to limit the right of disseminating online news to only a small number of “trusted” portal websites and central and provincial-level news organizations, which means that unauthorized websites have no right to publish news (and are only allowed to forward news from the traditional media or other authorized websites).

Although resistance challenging these regulations has happened since the very beginning, at least in written law, very limited power has been handed over to the Internet Content Providers (ICP) and ordinary users. Websites are further requested to serve socialism, uphold the interests of the state, and correctly guide public opinion, as shown in the Provisions on Administration of Internet News Information Services (2005). Most of these rules and

---

36 There are several reasons why the number of regulations spiked in 2000. First, the general population of Chinese netizens underwent an increase (from 17 million to 23 million) with around nine million computers connecting to the internet. Second, after the crackdown of Falun Gong in 1999 a huge number of online dissidents emerged, who became active in programming anti-censorship software and disseminating information against the CCP. Third, there were a lot of problems which arose along with the popularity of the internet, such as cyber crimes.
regulations function as responses to the problems emerging in cyberspace (and in the broad social context). After the outbreak of Severe Acute Respiratory Syndrome (SARS) in 2003, many student-run internet BBSs, particularly those that were critical of the government during the SARS crisis, received a tightened control (P. P. Pan, 2005a; Weber & Jia, 2007). In 2006, a real-name register system was introduced to these BBSs with the hope of decreasing online anonymity and preventing participants from speaking recklessly.

Based on these regulations, all four of the major internet backbones in China are controlled by the state. Joint ventures in the telecommunications infrastructure business are required to have a Chinese partner holding at least 51 percent of shares. The regulations are also very specific in stipulating which businesses are permitted. An example where foreign investment (including overseas Chinese capital) is strictly forbidden is the start-up of an internet bar (Castells, 2010, p. 335). Furthermore, enforcement of these guidelines involves a system of penalties (Zuckerman, 2014). The punishment has been specified and many cases have since happened (e.g., Zheng, 2008, pp. 70-78) which could actually produce a kind of chilling effect.

The control of the internet involves organizations at levels of both Central Government and local governments (provincial and below). The central level generally includes, among others, the Ministry of Industry and Information Technology (MIIT), the Ministry of Public Security (MPS), the Ministry of Culture (MOC), the State Administration of Press, Publication, Radio, Film and Television (SAPPRFT), and the State Internet Information Office (SIIO, started in

37 Of course resistance to such regulations has existed from the very beginning. For example, in Zhou’s (2006, p. 140) anthropological research in a Beijing-based internet bar, he found that the owner was a Taiwanese who in principle could not start business relevant to internet bars, but had managed to do so under the name of a local resident. For more information about the status quo and regulation of internet bars in China, see Jenkins (2006a), Qiu and Zhou (2005).
In particular, the MIIT is responsible for infrastructure and the MPS for internet security protection, while the MOC and SAPPRFT are responsible for internet content control. At the local government levels, every province and municipality has their own departments which are under governance of the higher level departments and are responsible for internet control in their jurisdictions.

The Chinese authorities try to persuade the public that monitoring and filtering is basically planned to protect the younger generations and to create a morally healthy online environment. The fact is that the government extends the scale of censorship often and obviously, from pornographic and violent information to dissident ideas, pro-democracy speech and political criticism, and on to any other online activity inciting collective action and provoking alternative thought (which has been defined as subversive information that erodes the harmony of the status quo). Meanwhile, although various regulations have been launched to guide and control the internet, different parts of this huge country (the more-developed eastern areas and the underdeveloped western areas) and different levels of the bureaucracy (the central and the local) interpret and operate these regulations in different ways. Most often,

---

38 The Ministry of Industry and Information Technology (MIIT) was formerly known as the Ministry of Information Industry (MII) before 2008 and as the Ministry of Posts and Telecommunications (MPT) until 1998. In 2013, the General Administration of Press and Publication (GAPP) was merged with the State Administration of Radio, Film, and Television (SARFT) and formed the State Administration of Press, Publication, Radio, Film and Television (SAPPRFT).

39 According to the MPS, the goal of internet control is “to strengthen the security and the protection of computer information networks and of the internet, and to preserve social order and social stability” (see The State Council of the PRC, 1997).

40 Other attempts to legitimize their censorship activities include studying how other developed countries censor violence and pornography; while how these countries use legislative means to impose restrictions on the power abuse of power and censorship are seldom (if ever) mentioned. For example, on the official website (http://www.sarft.gov.cn/) of SAPPRFT, it selectively publishes many such materials. The Snowden revelations, as well as other internet monitoring and filtering projects in Western democracies, became a somewhat useful excuse (i.e. information security) for Chinese censors. The CCP has upgraded its emphasis on information security recently and Xi Jinping, current president of the country, became the leader of The Central National Security Commission and The Central Internet Security and Informatization Leadership Group (established respectively in 2013 and 2014).
local governments have some room to take actions based on their local interests rather than strictly following the line set by the Central Government. Many cases have revealed that regulations and orders from higher levels might fail to take effect, or to be implemented according to expectations, at the lower levels (see more discussion in Chapter Three).

The Architecture of Internet Censorship

Besides legislative and institutional methods, Chinese authorities also use technical methods to censor internet content, which involves various governmental bodies (at both central and local levels), commercial ICPs, and Internet Service Providers (ISP). Research institutions (e.g., the Chinese Academy of Science) and scholars (e.g., Fang BinXing) of information technologies have helped to build this architecture. The most often used technical filtering methods include IP address blocking, DNS hijacking, website blocking and content filtering, among others, some of which emerged as early as in 1999 (e.g., Dong, 2012; J. Fallows, 2008; Farrell, 2007; Q. Yang & Liu, 2014). The operation of censorship has varied in both precision and density over these years. From the technical perspective, the more perfect the machine, the more money it costs; the authorities have to make a balance between the budget and the expected effectiveness (Leberknight, et al., 2012). For example, although blocking precisely sensitive websites and content may be technologically available (by human censors), the authorities may still choose to use a relatively crude approach – simply blocking the sensitive IP address. This of course may block innocent websites and content which shares the same IP address with the sensitive ones. However, as believed by many researchers (J. L. Qiu, 1999; Tai, 2015), a very massive, fluid, sophisticated (both technically and institutionally) and effective censorship system has since gradually been built.
The building of the GFW

The project of building a virtual Great Wall, named the Great Firewall of China (GFW), was launched by the Chinese authorities in 1996, only one year after the internet became publicly available.\textsuperscript{41} In 1999, it reportedly started to block foreign websites which were incompatible with the CCP’s requirements (Collings, 2001, pp. 187-188); and in 2001, its general infrastructure was finished and gradually matured.\textsuperscript{42} In the beginning, the Chinese government received various technological supports from Western companies (e.g., Cisco System) who sold both filtering technologies and software to the former. In order to work out an effective solution, the authorities also gathered a group of domestic hardware engineers and software developers to do research on building a nationwide firewall.\textsuperscript{43}

It was around 2002 that the GFW implemented the keyword filtering system. Based on this system, censors could automatically monitor sensitive words, or articles containing these words, and thus get them blocked. The list of keywords has been updated from time to time, with words going on and off the blacklist. The criteria defining which words are sensitive (and

\textsuperscript{41} It is commonly agreed by scholars of the Chinese internet that the concept of the GFW originated in Geremie Barme & Sang Ye’s article (1997), according to which the project of the GFW started in 1996. This date is confirmed by Thornton (2010, p. 180), though some suggest 1995 as the starting year of this program (R. J. Deibert, 2002).

\textsuperscript{42} But according to an official interview with Fang Binxing in 2011 by the Global Times, a Beijing-based nationalist tabloid which is affiliated to People’s Daily, the GFW project was officially claimed to be launched in 1998 and it was not until 2003 that it really started. This same interview also mentions that Fang used six VPNs on his computer at home, by which he could test the GFW system, and notes that what happened between the GFW and the VPNs is “an ageless war” (Huanqiu Shibao [the Global Times], 2011).

\textsuperscript{43} Fang Binxing, one of such researchers, was named as the chief designer of this censorship system, and eventually received the infamous title of “the Father of the Great Firewall.” Because of his involvement in building the GFW, he has received huge criticism from the general netizens. In later 2010, Fang started to use Sina Weibo, which attracted huge number of netizens who soon burst into a storm of abuse; about one day later, his Weibo account became inactive until one year later when he resumed it and turned off its comment function. Other anecdotal stories included that Fang was welcomed by a shoe from a protester before his lecture at a university; a related website was hacked and its homepage was changed into a web game named “Angry Shoes,” similar to “Angry Birds” with shoes as the weapons and Fang’s head as the target. In June 2013 when Fang declared his resignation as present of Beijing University of Posts and Telecommunications because of health problems, he again received fierce words along such lines as “Wish the illness beat the president as soon as possible.” With a background as an official and as a researcher of the GFW, Fang has become a symbol of the restriction of the internet in China, and a predictable target of ire from some ordinary netizens.
which are not) seem to be decided by high levels of the censorship system and hardly known
to the public, which itself becomes a heated topic for researchers (e.g., Ng, 2013). Many terms
have become sensitive due to offline events.\textsuperscript{44} And one certainty is that, within the GFW,
content with sensitive words can never be published (unless these words are disguised by
symbolic tactics which will be fully discussed in Chapters Four and Five); neither can any
website access requests with sensitive word(s) succeed in connection with the target server(s)
or sensitive emails be sent (unless these activities have been performed via circumvention
tools or encrypted in the first place, as Chapter Three will show).

Besides this keyword filtering system, the GFW also tries to either technically block or
attack most (if not all) circumvention tools.\textsuperscript{45} Although some VPNs – which are widely used
to tunnel under the firewall – may be bearable, as they are needed by foreign businesses with
branches in mainland China, the GFW has reportedly begun more intensive disruption of
VPNs since 2012 (Epstein, 2013). The censors create, and continue to update, a list of
sensitive websites that are considered “dangerous” websites (most are politically sensitive, and
some pornographic and violent).\textsuperscript{46} The GFW blocks all the websites on this blacklist while

\textsuperscript{44} For example, after the Wenzhou high-speed train accident in July 2011, messages containing the name of
Sheng Guangzu (then the Minister of Railways) were not able to be published on Sina Weibo.

\textsuperscript{45} As discussed in Chapter Three, much anti-GFW software would be blocked by the GFW (sometimes)
shortly after its invention and circulation. For example, some anti-GFW programmers believe that the GFW has
employed a group of human censors to collect the updated information of TOR’s bridges from its official
websites so that the GFW is able to block TOR promptly (see Biancheng Suixiang, 2012).

\textsuperscript{46} More than 18,000 overseas websites were blocked in Mainland China before 2003 (Zittrain & Edelman,
2003), and this number is now bigger than before. Twitter has suffered a similar fate to that of Facebook,
LinkedIn, Blogspot, WikiLeaks, YouTube and other familiar U.S.-based social media services, and has been
blocked by the GFW since mid-2009 (Blanchard, 2009; Sullivan, 2012). Other foreign websites or portals blocked
in China include, but are not limited to, Human Rights Watch, Amnesty International, Reporters without Borders
(Reporters Sans Frontières, RSF), VOA (particularly its Chinese service), and the Washington Post. Bloomberg’s
English-language website and The New York Times’ website (including its Chinese-language edition) were
directly blocked by the GFW in 2012 after issuing reports about the crony capitalism (i.e., the finances of
leaders’ relatives) in Mainland China. In July 2014, the Chinese authorities tightened the control of the mobile
internet and blocked a series of foreign mobile apps (such as Line, Flickr, KakaoTalk, OneDrive and the picture-
sharing site Instagram). The publicly available reason why websites of some traditional media such as VOA and
Radio Free Asia (RFA) get censored by the GFW is that these media are believed by Chinese authorities to be (at
giving the green light to those not on it.\textsuperscript{47} Sometimes, rather than directly block the sensitive websites, they choose a more covert method – slowing down users’ surfing speed on such sensitive websites.

The Chinese firewall system is known to work entirely “symmetrically” which means that any content that passes both inside outwards and outside in can be detected and filtered (Clayton, et al., 2006; J. Fallows, 2008; Q. Yang & Liu, 2014). Although this mechanism focuses more on the netizens who are physically inside Mainland China, it can also stop outside IP addresses from accessing sensitive information within the GFW (Q. Yang & Liu, 2014). However, differences do exist between these two types. For example, searching “June 4th” from the outside of the GFW on s.weibo.com will be blocked while searching “Falun Gong” will not; while within the GFW, both searching attempts will be in vain. Since the data exchange between China and the outside world is fulfilled mainly by three international internet gateways (submarine cables), which serve as gatekeepers for the four major national internet backbones, it is technically possible for the Chinese government to monitor cross-border information by mainly monitoring these three gateways.\textsuperscript{48} If Chinese people outside the country, such as academics or exiled dissidents, want to look for data on Chinese sites

\textsuperscript{47} A whitelist of websites is also widely believed (particularly by dissident netizens) to exist, which means conversely that the GFW gives the green light to all the websites on the white list while blocking those not. Though there is no authentic way to confirm this, like other skepticism popular in Chinese cyberspace, it reveals the popularity of conspiracy theories (about the authorities) among many Chinese netizens – which is definitely a negative consequence of heavy internet censorship.

\textsuperscript{48} The Beijing gateway connects the Beijing-Tianjin-Tangshan region in northern China with Japan, the Shanghai gateway connects the Shanghai region in eastern China with Japan as well, and the Guangzhou gateway connecting Guangzhou region in southern China with Hong Kong.
(e.g., public-health figures or news about a local protest), the censorship system, theoretically, can monitor what they are asking for, and, if necessary, censor their findings accordingly (J. Fallows, 2008). The financial reason for censorship in reverse is copyright issues, due to which, most movies, TV shows, and video clips involving possible copyrights and license issues on Chinese content-sharing social media are also blocked to international IP addresses.

**The Golden Shield Project and other censorship designs**

Functioning technically as a crucial gatekeeper between two worlds, the outside one and the inside one, the GFW is just a part – albeit an important part – of the whole system of internet censorship in China. In fact, the CCP also tries many other means such as the Golden Shield Project, which started in 2001.49 This massive, ubiquitous surveillance project, operated by the MPS, is claimed to monitor only “superstitious, pornographic, violence-related, gambling and other harmful information” (as cited in Lum, 2006) and to guarantee a secure internet environment for Chinese netizens. It has since been active, at least partially, on censorship tasks and functions as an indispensable supplement to the GFW.

Besides these automatic censorship technologies, human censors have been greatly utilized as well (Xiao, 2011b, p. 207), in roles including that of cyber police and internet opinion analysts. It was believed that in 2010 alone, China had 30,000 full-time cyber police (e.g., Thornton, 2010, p. 194), a claim which has been supported by King et al. (2013) who asserted that approximately 20,000–50,000 wang jing (internet police) and an estimated 250,000–300,000 paid online propagandists are employed at all levels of government.50 Furthermore,
some two million internet opinion analysts have been reportedly employed to monitor China’s vast online population (Boehler, 2013). And almost every internet company operating in Mainland China has their own content censors to monitor, filter, and manipulate online expression.\(^5\) Human censors are greatly needed where the machine fails, such as for sensitive content carried by images which could not be recognized by the existing censorship technologies, and sensitive internet accounts (of dissidents, pro-democracy journalists, and activists, among others) that need specific attention (K.-W. Fu, Chan, & Chau, 2013).

The real-name registration system functions as an important component of the entire censorship system.\(^5\) Early in 2003, all internet bars in China were theoretically required to check the real identities of the customers, with the intention to discipline netizens and remind them not to cross the line. It was soon used to control speech in virtual spaces such as BBSs and blogs (blogs having gained popularity in 2006). Students needed to provide their student ID cards when registering with popular BBSs that were hosted within universities, and bloggers had to register with their real identity (with an ID card or a mobile phone number, or other identifying information) before publishing anything (S.-D. Liu, 2006); although in both cases, screen names could still be used. In 2009, the real-name system was extended to some news portal websites as well; without registration, readers were not allowed to comment on the news. After the nationwide dissemination, this policy was officially launched on 16 March 2012. Under this policy, registered users must release their identity numbers or indirect

---

51 For example, Sina Weibo, China’s most popular micro-blogging platform, was believed to hire at least 1,000 censors in 2011 to monitor its users’ activities (2011b) and in 2013 this number was estimated to be roughly 4,200 (Dewey, 2013), although its CEO once publicly admitted in a conservative way that only 100 censors had been employed for such work (Bamman, et al., 2012).

52 South Korea was reported to be the first country to enact policy requiring the use of real identities on the internet (Cho, Kim, & Acquisti, 2012); but its government finally abolished this policy in 2012.
identifiers to the internet providers for government verification, but users are allowed to choose to remain anonymous at the front-end. The real-name system may have some influence on disciplining the netizens; for instance, it might cause micro-bloggers to stop writing on politically and socially sensitive issues using the same account. But it does not prevent users from breaching the policy itself, since, theoretically, micro-bloggers can change accounts and continue to post (K.-W. Fu, et al., 2013), or in other situations users may provide an unused cell phone number for registration purposes, and internet providers seldom check the validity of such numbers.  

Besides these tactics, the authorities launch periodic movements aimed at “purifying the internet,” which are claimed to wipe out pornographic and violent content from cyberspace while simultaneously taking harsh action towards politically sensitive materials. The authorities are also believed to use “honey pots” (Thornton, 2010) to monitor netizens’ anti-GFW activities. For example, fake IP-addresses for proxy servers are potentially circulated by these censors, so that attempts to get round blockades might end up being routed directly to the traps (Hughes & Wacker, 2003, p. 71). Further means include promotion censorship-software. A significant case of this method happened in 2009 when the authorities declared that all new computers sold after 1 July 2009 should have pre-installed the filtering software called Green Dam Youth Escort or the setup files on an accompanying compact disc. This software was claimed to filter out pornographic images and violent information and thus could protect youth from harmful content; however, it was soon widely suspected that this was nothing more than

---

53 The Chinese government once issued a regulation to limit phone-card sales, according to which, sellers had to check buyers’ ID cards. But the authorities soon found that this regulation was extremely difficult to enforce. Limiting phone-card sales to just a few shops with the ability to process registration requirements would be a blow to mobile-phone companies and the huge number of private vendors who thrive in such business. Competition between the market and politics becomes intensive (see Zheng, 2008, p. xv).
a new way of monitoring individual user performance (Faris, Roberts, & Wang, 2009). Economical restriction functions as a further way to control online public opinion. For those activists (e.g., pro-democracy journalists and human rights lawyers) who are active in cyberspace and cause trouble for the authorities, intransigence can lead to delays in their license renewals, or job loss and consequent pressure to find a new employer and earn a livelihood.

**Issues of time and geography**

After the perfecting and modification process over recent years, the entire censorship system is generally capable of responding immediately to any heated topic shared within Chinese cyberspace; when necessary, it often takes censorship action “within hours or days not weeks” (Zuckerman, 2014), or within “the first five minutes to half hour” (T. Zhu, Phipps, Pridgen, Crandall, & Wallach, 2013). The system will tighten the control of online expression for sensitive days every year. Observation in 1999 (J. L. Qiu, 1999) found that every year in early June, most BBSs hosted by universities were denied network connection for a week or so due to the anniversaries of the Tiananmen Incident in 1989 and the control remained loosened for the rest of the year. This policy seems not to have changed in recent years. For instance, in the run-up to the twentieth anniversary of June 4, a great number of domestic websites were temporarily closed down in the name of “technical maintenance;” so were foreign websites such as Twitter, Flickr, Wikipedia, Bing, Hotmail, and Facebook (Xiao, 2011b). The tolerance for online dissent is also reduced during high-profile public events such as the annual meeting of the National People’s Congress, the National Congress of the CCP, the 2008 Beijing Olympics and the 2014 APEC CEO Summit. However, the authorities’ tolerance of sensitive
materials has also undergone a change in recent years. According to an early report from RSF (2003), no criticism of the CCP’s decisions was allowed online at that time; while recent research (King, et al., 2013) has found that the authorities will sometimes even allow vitriolic criticism of the state, its leaders, and its policies – a governmental strategy to legitimize the state and help the regime maintain power.

Given the physical size of China, geographical factors also apply to internet censorship (T. Zhu, et al., 2013). Early observations have found that the magnitude of censorship varies from place to place (Zittrain & Edelman, 2003). For instance, websites located in Beijing generally receive more strict and frequent censorship than that in remote areas of the country such as Yunnan province (J. L. Qiu, 1999). Even today, geographical locations still affect the magnitude of censorship. The majority of Chinese websites are registered in Beijing; censors at both the state level and the provincial level may become directly involved in regulating these websites, while those websites registered in remote areas may face relatively loose regulation and thus enjoy a relatively free environment. Other evidence proves that the GFW responds differently to different websites hosted overseas. For example, one netizen (Yao, 2012) found that the surfing speed was slow when changing his personal blog’s host server to Hong Kong or to the U.S., while the speed would be faster when his blog was hosted on a server in South Korea. Some Chinese netizens may also take advantage of the geographical differences in internet censorship, and find strategies to bypass the censorship system.

54 However, there are exceptions. For example, messages originating in the outlying areas of Tibet and Qinghai, according to Bamman, et al. (2012), exhibit much higher deletion rates than those from eastern areas like Beijing. This might because of religious or ethnic reasons.
Internet Companies and the Operation of Censorship

The censorship system may be divided into three levels. The highest level involves law and policies, regulatory institutions, the GFW, and other technological means. Since the ruling party is never a monolithic group and competitive factions always exist within it, the top-down control of the internet is rarely as it is expected to be. Because of the overlapping responsibilities of different regulatory institutions and the complexity of information networks, internet censorship can be “inconsistent and unpredictable” (H. Yu, 2009, p. 115), and requires constant negotiation and modification. The lowest level denotes a kind of self-censorship practiced by ordinary netizens. On the one hand, self-censorship reflects a hidden acceptance of the status quo and the difficulty of radical responses to censorship. On the other hand, it also means the practice of how to resist censorship: that is, the acknowledgement of what is unacceptable itself defines what is acceptable. In other words, netizens gradually get to know how to push the envelope, how to strategically get their voice heard, and eventually breach the censorship system (Stern & Hassid, 2012).

The middle level of the censorship system may be defined as intermediary censorship, including both the internet censorship practice of the corporate sphere and that of local government. For a given internet incident, it is often the case that the authorities at the state level have different attitudes from that of the local authorities. The local authorities sometimes enjoy certain degrees of discretion. For example, when mass incidents happen in a given local

---

55 Different ministries (with different interests and responsibilities) become involved, and internet censorship becomes even more complicated, sometimes internally contradictory. A detailed case will be seen in Chapter Six. When it comes to dealing with the industry of the online game World of Warcraft, the conflict of interests between MOC and SAPPRFT is exemplified.

56 It has to be pointed out that the rule of self-discipline is not only practiced by ordinary netizens but also by internet companies (who are held responsible for the content and behavior of the users on their sites).
jurisdiction, the relevant local authorities will undoubtedly try their best to limit media coverage, monitor relevant civil activities and block unbearable information. The current cadre system of the Chinese political regime can be explained by the phenomenon of “wushamao” (black gauze caps), a term referring to how Chinese people view the selective processing of government directives by local authorities, who attempt to protect their own positions and interests at the expense of those in society for whom they are responsible (Weber & Jia, 2006, p. 100). This illustrates that, within a specific incident, the censorship attitudes of directly relevant officials are often very different from that of authorities at a higher level (and, sometimes, even that of other officials at the same level). This chapter does not go into much detail about how different their attitudes can be, but this issue will be mentioned sporadically in the coming chapters. This section focuses mainly on corporate intermediary censorship.

The role of ICPs and ISPs in censorship

To deal with the tremendous scale of online content production, the state relies increasingly on internet companies (both ICPs and ISPs) to keep an eye on their own users, which makes domestic censorship largely fragmented, decentralized and heterogeneous (Bamman, et al., 2012; MacKinnon, 2008, 2009a). Informal or formal instructions are frequently sent out by propaganda ministries to tell the internet companies (ICPs in particular) what can and cannot be discussed on their platforms. Furthermore, domestic internet companies play crucial roles in policing their own content under threat of penalties including

---

57 In 2004, a district-level Bureau of Justice in Sichuan issued a document prohibiting lawyers from representing water pollution victims along the Tuo River. This case demonstrates that although not all local protests are bearable for the Central Government, the latter often selectively uses citizens as an oversight mechanism on local leaders, which imbues citizens with the ability to sanction lower level leaders, and push the latter to govern in a more effective way.

58 The frequency with which internet companies receive instructions from either SCIO (State Council Information Office) or other provincial-level propaganda officials could be at least three times a day (Xiao, 2011b, p. 207). For further examples see J. Fallows (2008).
fines, shutdown and criminal liability (Jedidiah R. Crandall, Zinn, Byrd, Barr, & East, 2007; MacKinnon, 2009a; 2009). Chinese authorities tactically delegate censorship to private business and seem relatively unconcerned with the detailed means to “manage” user content as long as the end result is successful (MacKinnon, 2008). All ISPs and ICPs in Mainland China have to comply with the restrictions placed by censors and, ICPs in particular, show responsibility for all content they display (which seems to be the case from the very beginning, see Tao, 2001), since if they fail to do so they will face revocation of their business licenses or even arrests (Tkacik, 2004). To comply with their license conditions, ISPs must act as censors, to screen users’ messages or disable undisciplined accounts. As mentioned previously, Sina reportedly set up its own censorship department of a thousand people, who are termed “online public opinion analysts,” to monitor Weibo pages. Other domestic internet companies (such as Sohu, Renren and Netease) have signed self-discipline acts (which can be seen in Appendix B) and set up “discipline staffs” to monitor and discipline their users’ online activities.

The authorities try hard to control the key personnel of most, if not all, big domestic internet companies, and have consistently worked on keeping their CEOs loyal. Internet executives reportedly attend a weekly meeting with government officials, in which potentially “sensitive” topics are discussed and instructions are offered as to which conversations should be censored (Zuckerman, 2014). The bosses of big internet companies have been invited on annual red tours of historic communist sites since 2003 (Epstein, 2013), and to have training courses together, as hidden ways to cast influence onto these internet companies.

---

59 Bamman, O’Connor, and Smith (2012) found that no less than 16% out of a random sample of 1.3 million Weibos had been deleted. Not surprisingly, they also discovered that messages containing politically sensitive terms were characterized by anomalously higher rates of deletion.
Internet companies often implement their own monitoring and filtering functions. Different platform providers vary widely in their willingness to censor texts, with some censoring more regularly than others. Each company, as MacKinnon (2009a) has found, has its own internal set of rules and uses a set of automatic processes (blocking specific keywords) and manual reviews to censor controversial material before it appears online, or to delete it after it has appeared. For example, Baidu can censor its results carefully to follow Chinese government guidelines based on its technologies of search engine optimization (SEO). Some internet companies apply censorship software to “screen and delete posts according to different keywords and categories, as well as block posts based on user, length of post or time of day” (Mozur, 2013); and account blocking is widely used by platforms such as Weibo and BBSs to cope with undisciplined users. When it comes to message deletion, different companies have different patterns of deleting as well. Take Sina Weibo and WeChat, two currently popular social networking platforms in China, for example. When Sina Weibo deletes a post of a user, the deleted information will be replaced by a notice “Sorry, this post has been deleted. Refer to [a webpage of further explanation] for help.” This notice will be seen on the homepages of this user’s followers as well; by contrast, deleted information will not be shown on the homepages of a WeChat user’s followers. Sina Weibo’s censorship is more transparent than WeChat from this point of view.

60 Song Shinan, for example, was blocked from using his Weibo account after he had re-posted information about a dissident artist’s [Ai Weiwei] return from detention (Sullivan, 2012). Similar cases append to Pu Zhiqiang, a human rights lawyer who was blocked every time he published sensitive content on his newly-registered blog.

61 WeChat, affiliated to the Chinese internet giant Tencent and a clone of WhatsApp, is a popular mobile messaging application that has become a new superstar of social media in China; in 2013 it claimed to have more than 300 million accounts.

62 WeChat’s censorship seems to be much smarter and more hidden in this case, since a notice of deletion might not only irritate its users but also decrease the user experience of the relevant followers of the users, and
In addition to monitoring and filtering, methods such as encouraging users to report any piece of “untrue information” are also developed to counter the dissemination of sensitive information, which may enable the internet providers to delete “harmful” information within several minutes (K.-W. Fu, et al., 2013). Because this method assigns, to some degree, the censorship task to ordinary netizens and saves costs for internet companies, it has been widely used since development. This control strategy damages the internet sphere because it encourages an attacking culture among netizens. If censorship activities from the internet providers irritate directly the users, then this mechanism redirects anger to the users themselves – from those being reported to those anonymous whistleblowers; two groups are divided by this symbolic violence of reporting. For internet companies, encouraging users to report “harmful” content is a double-edged sword, since on the one hand it eases the pressure from users and on the other hand it encourages users to anonymously attack one another and thus deteriorates the communication environment.

Domestic internet companies can be easily controlled simply via pressure on their management. This is also the case for foreign internet companies with branches in China, though different methods may apply and degrees of censorship may vary. For example, in 2004, a Chinese journalist was sentenced to jail for ten years because of his leak of a government e-mail to a New York organization. Yahoo! was criticized for complying with the Chinese authorities to provide information about this journalist, who had used a Yahoo! email.

Furthermore, although Sina Weibo tells its user (and his/her followers) that something has been deleted, it never specifies the specific reason why the deletion happens. Reporting literally means that every user is encouraged by the ICPs/ISPs to check other users’ posts; and if any post steps across the line, readers can report to administrators and administrators will decide to delete the post or not (depending on the results of double-checking the relevant post). This mechanism has also been utilized by corporate censors from as early as the BBS times. The user reporting mechanism was actually not created by Chinese social networking platforms but by Western counterparts, and the Chinese authorities (and internet companies as well) utilized it as an online social control mechanism.
to leak that sensitive information (Ng, 2013, pp. 62-63). The Chinese version of Yahoo!’s search engine service not only filters content by keyword and removes certain search results from their lists, but has also hired supervisory staff for the teams of censors assigned to every Yahoo!-hosted internet chat room in China (see Tkacik, 2004). Microsoft would send an error message to Chinese users who used its search engine for sensitive words. YouTube promised to geographically filter some videos. Google removed controversial search results, and Twitter set up a program to block the materials which Chinese authorities deemed sensitive (Gasser, et al., 2013, p. 21). For interests relevant to market shares, before entering the Chinese market, Western internet giants have to make changes according to localized policies (Farrell, 2007; S.-D. Liu, 2006), cooperate with the Chinese authorities and become, objectively, the accomplices of the Chinese authorities in limiting freedom of speech.

**Conflict between political requirements and commercial interests**

As described above, internet companies engage deeply in the operation of internet censorship. However, the degree of censorship varies according to different types of internet companies. Criticism of the CCP is barely seen on the websites of *Xinhua News Agency* and *People’s Daily*; while on commercial websites such as Sina and Sohu, users can quite often come across sensitive information. In order to understand this difference, the dimension of commercial interests of internet companies should be taken into consideration.

The commercialization of Chinese mass media began in the 1990s (Fung, 2008; Y. Zhao, 2008), which is also the case of various internet companies. Today, most Chinese ISPs and ICPs finance themselves through advertising revenues, they are profit-oriented, and, if they are listed companies, their shares are publicly traded on the stock market. But this does not mean
that they are limitedly affected by political power; most of the time, these internet companies still need to comply with all kinds of censorship requirements from above. When discussing the censorship happening at this level, we should bear in mind both commercial considerations and political requirements. These internet companies compete fiercely with each other over audiences, users and advertising revenue (Poell, et al., 2014). In order to attract more web traffic, sometimes internet companies will apply a similar hidden rule in Chinese journalism called “da chabianqiu” (push the envelope, literally meaning “play the edge ball”): they first let sensitive content run as it is and then, when higher level censors engage, they will delete the relevant content.64 This time lag provides users a chance to know, discuss and share the sensitive content. This strategy has become a kind of hidden culture for domestic internet companies who want to balance political requirements with commercial interests.

In some situations, commercial websites may even try to decrease the number of checks on who is writing what, which marks a crucial difference between political organizations and commercial internet companies. In July 2014, Li Chengpeng was blocked and forbidden from using his Sina Weibo account. Li had been a popular micro-blogger who was active for a long time at Sina Weibo and attracted for the latter huge web traffic. Most his posts were politically sensitive, and Sina selectively deleted some of these posts and tried its best to make him remain active there. However, on this occasion it chose to entirely block Li, which seemed to contradict its long-used commercial strategy of inviting famous people (e.g., entertainment celebrities, public intellectuals and popular journalists) to use its services (particularly

64 There are, of course, differences between different types of users. In general, high-profile users enjoy a higher level of freedom of speech than ordinary users. For example, Sina would strategically give several minutes’ green light for popular online celebrities such as Li Chengpeng and Han Han and their controversial posts in order to attract more web traffic.
blogging and micro-blogging) to attract web traffic. The only reason Sina did this is that Li had angered top level censors (who had just launched a serious nationwide movement to discipline online celebrities – or “daji da-v xingdong”) and Sina had to comply with the authorities, thus Li was blocked entirely. An other case happened in 2009, when a post of “Jia Junpeng, your mom wants you to go home to eat” became popular (a case which will be fully discussed in Chapter Six); Baidu’s Tieba service deleted this post and its millions of comments (partially because its comments are “pornographic and violent” thus needing censorship) several times, but every time the post recovered, partially due to its users’ fierce protests. This incident provided heavy traffic for Baidu (too heavy to afford). Although we should be wary about the role of internet companies in internet resistance, the conflict between political censorship and commercial interests potentially provides some room for internet resistance to censorship.

**Censorship as business**

Western capital did help the Chinese authorities to build a grand censorship machine (MacKinnon, 2012); for this reason, the relevant companies (e.g., Cisco System and Google) faced fierce criticism from the public. Hewlett Packard’s Autonomy unit reportedly programmed an internet public opinion monitoring system for the Chinese market in 2006 and had some takers in government (see Epstein, 2013). Meanwhile, some other companies who

---

65 This is termed “celebrity strategy” for Sina’s commercial promotion. For example, Sina invited Xu Jinglei, a famous Chinese actress, to start blogging at Sina Blog service and soon Xu became “the Queen of the Blog” in 2006. When it came to micro-blogging services, Sina applied the same strategy to invite Yao Chen, another famous Chinese actress, to register her Weibo account there and made her “the Queen of the Weibo.” Although Sina has to block some of its famous users, it has sometimes recovered their accounts later. For example, the Weibo account of Zhang Ming, a pro-democracy historian who is active at Sina Weibo and has over 390,000 followers (at the time of writing), became blocked for over one year and then was restored in 2014.

66 Unless otherwise noted, all translations from Chinese in this thesis are my own.

67 The Global Times commented on Li’s case afterwards, warning that “people like Li should show respect for the law, otherwise they should bear the consequences of their activities” (Shan, 2014).
provide VPN service for users within the GFW gain a relatively high-profile both financially and morally. In 2008, the average price for a VPN service was $40 per year (J. Fallows, 2008). Almost all the international businesses that branch in China depend on this technology to operate and communicate. VPNs are also available for research institutions such as universities, and even individual consumers. On Taobao.com, a top Chinese online shopping website similar to eBay and Amazon, various circumvention tools have been sold, some of which are as cheap as ¥10 (less than two dollars) per month. The Chinese authorities have to put up with these tools to some degree.

In order to dominate the internet, the authorities encourage state-monitored businesses to get involved in the process of internet censorship, particularly official background media groups (e.g., Xinhua News Agency and People’s Daily). For example, People Online, a subsidiary company to People’s Daily Online, has focused on online public opinion monitoring and analysis since 2007 and devoted itself to software for monitoring purposes. People Online has contracts with some departments of the Central Government (e.g., the Ministry of Human Resources and Social Security) and its monitoring software has even been on the shopping lists of Central Government departments (Botong, 2014). Increasing demands

---

68 The price seems to have not changed too much over the recent years. For instance, Astrill, a Seychelles-based internet company and self-portrayed as “the leader in the global Personal VPN market” (see https://www.astrill.com/about.php), provides VPN service that charges about 70 dollars per year. It gains Chinese users as well.

69 In November 2001, China signed the WTO agreement and opened its doors to foreign investment by guaranteeing its domestic economic structure more transparency such as openness of information. Since then, China has gradually built a close relationship with the outside world, and many international companies have branches in Mainland China. These companies depend much more on foreign internet services, some of which are on the GFW’s blacklist. Services like VPNs thus have opportunities to flourish.

70 It is not new that Chinese authorities tolerate such “exceptions.” Before the internet era, when television still dominated the media landscape, ordinary people were forbidden to receive signals of foreign TV programs (which is still the case today), but TV sets in five-star hotels (particularly those used often for foreign affairs) were allowed to freely access foreign TV programs. These hotels reportedly have the ability to freely access foreign websites as well. In 2013 when the Shanghai Free-Trade Zone was officially built, commentators wondered if this zone would be GFW-free and become a new kind of “political concession” in the internet era, a guess which finally proved unfounded.

63
of methods for monitoring online opinion are from local governments – who utilize these tools for “weiwen” (maintaining social harmony) in their jurisdictions – control negative information about the local authorities and manipulate a positive image of themselves to present to higher level government (J. Wu, 2014). With its annual income reaching ¥ 100 million (about $ 16.26 million) in 2013, People Online contributes the major portion of income for its parent company.

One of the initiators of censorship business in China is Fangzheng Jituan (the Founder Group), which started research on monitoring online public opinion with requests from relevant departments of the Central Government.71 Since then, many other players have appeared in this field, such as Beijing TRS Information Technology Company, Xiamen Meiya Pico Information Technologies Company, and Guangzhou-based Barfoo Software Company (Bangfu Ruanjian Gongsi), among many others.72 In particular, Meiya Pico, which started in 1999 and was listed on the Shenzhen Stock Exchange in 2011, has many contracts with government departments at both local and central levels, with an incredible annual income in 2013 of ¥ 390 million ($ 63.41 million). An increasing number of “shantie gongsi” (post-deleting companies) have appeared which sell deletion services for individuals, small businesses and even local governments in small cities.73 The price for deleting a negative

---

71 Similar cases have happened elsewhere. In the U.S., the Department of Homeland Security reportedly hired commercial companies to monitor news outlets, online forums, blogs, and social networking sites via social-media monitoring internet-based platforms and information technology infrastructure. (Vijayan, 2012) What is quite interesting though in China is that although many such companies claim to be only doing online public opinion research (rather than monitoring individual users), since they often get involved in providing technologies and solutions for negative information in cyberspace, monitoring online public opinion seems to be a euphemism for surveillance.

72 According to the Economist’s special report on 6 April 2013, more than 100 Chinese companies had made a total of at least 125 products for monitoring and filtering public opinion online. The most expensive of the publicly disclosed government purchases was reportedly bought by Beijing’s internet propaganda office for $ 4.3 million (see Epstein, 2013).

73 These black market internet companies include Yage Times Advertising, Beijing-based IWOM company (Koubei Hudong) and Erma Hudong Yingxiao, among others.
Internet companies are able to delete articles on various websites, such as commercial portals, popular forums, SNSs, as well as media websites with an official background (e.g., Xinhua and People’s Daily). Software systems for monitoring and filtering are sold as well by these companies, some of who also engage in selling zombie followers, planting negative posts (and then charging a fee for deleting them) and making fake public opinion by retweeting relevant posts to make them flourish.

Internet companies profit from censorship as well. For example, Baidu (China’s top internet search engine) is widely believed to provide deletion service for customers (e.g., commercial institutions and local governments) who wish for no negative results to appear when users search for information about them. During the Sanlu milk scandal in 2008, as Yang (2013) discusses, Sanlu offered Baidu ¥ 3 million (about $ 490 thousand) to censor negative information about Sanlu on the internet, although Baidu allegedly rejected this offer.

With various internet companies involved in the censorship process and providing an indispensable supplement to the legislative, institutional and technological censorship designs, the internet control system in China becomes even more systematic and complicated.

**Cyberculture Characterized by Censorship**

The all-around censorship system in Chinese cyberspace has generated vast influence on Chinese cyberculture and even the real-world culture and politics. Internet censorship becomes a barrier for foreign internet companies and accentuates Chinese netizens’ consumption of

---

74 Take Google for an example. For two months in 2002, Google’s website in China received a different kind of bad-address treatment (DNS poisoning), which shunted users to its main competitor, the dominant Chinese search engine, Baidu (J. Fallows, 2008). The Google service was restored later, but its cache pages, which had
domestic websites (Taneja & Wu, 2014). It also limits the average Chinese netizens’ knowledge about their media choices and shapes their picture of the world (MacKinnon, 2008). The majority of Chinese netizens have reportedly agreed that they “have full access to all of the information that is available on the internet,” which is further supported by studies claiming that “many Chinese people are either unaware of the GFW or unconcerned by it” (Damm, 2007; F. Liu, 2011). Only those netizens who are internet-savvy or who have the relevant technological means (such as VPNs or other circumvention tools) could access these censored platforms (an issue which will be fully discussed in Chapter Three); although, at the same time, they have to bear the slowness and unreliability of using such tools. The Chinese internet looks basically like “a heterogeneous, sophisticated intranet” (Stevenson, 2007; Taubman, 1998).

been a convenient way for Chinese users to find banned content (see the Chapter Three for more discussion), remained inaccessible and its search engine was subtly throttled and slowed down. Eight years later, Google withdrew its market plan in Mainland China. But Google has never entirely withdrawn its service; conversely it still has a close commercial relationship with Chinese technological companies. In August 2014, Google announced plans to work together with China Mobile International, China Telecom Global, Global Transit, KDDI and Sing Tel to build and operate a new Trans-Pacific cable system “FASTER” connecting the U.S. and Japan. The GFW did not entirely block all Google’s services; for a long time, Mainland Chinese netizens could still access Google search engine with a host server which had been shifted to Hong Kong, although the service has not been consistently stable. Since late May 2014 (shortly before the anniversary of the June 4 Event in 1989), some of Google’s popular services (e.g., search engine, Gmail, and Google Scholar) have been blocked by the GFW. Many commentators had attributed this blockage to the sensitive date of June 4 and they believed that after this day the Google service could be used again, as had happened before. But the blockage of Google this time seemed to be much longer. Meanwhile, Baidu launched its Baidu Scholar (Baidu Xueshu) service, the timing and title of which, unavoidably, invited huge criticism that it not only mimicked Google but also take advantage of unfair competitive means (the power of censorship) to deal with its commercial rival. It is believed that the Chinese government may use the GFW as a tool to block Western internet companies to protect domestic internet companies (Faris, et al., 2009; Leberknight, et al., 2012). It is interesting that within Mainland China, Google’s public image (particularly amongst public intellectuals) is that of “the brave resister against an evil system,” partially because of Google’s emotional narrative of its standing against the censors, and the Chinese public intellectuals’ rhetoric of this withdrawal. A group of users went to Google’s Beijing headquarters and left flowers on its sign. It would be correct to argue that this nuanced emotion reveals a hidden anger towards internet censorship (rather than a true love of a foreign company such as Google).

75 Over the past two decades, China has already developed a series of internet providers, most of which are merely mimicking their Western counterparts. This is unlike other countries such as Thailand, Pakistan, Turkey and Vietnam who block many international platforms but have seldom produced domestic platforms as substitutes.
Although censorship does not sweep away political discussion in Chinese cyberspace, organized and collective online political activities have been tightened (King, et al., 2013; King, Pan, & Roberts, 2014). Also despite the fact that a good degree of general political debate is allowed to continue (Gasser, et al., 2013, p. 23), online political discussions about sensitive topics have been greatly limited. Those who do touch on sensitive political topics have to disguise their discussions by various means (as shown in Chapters Four and Five). Partially because free discussion about political issues is unavailable, many people may be switched to apolitical or less political areas; the prevalence of apolitical or less political content such as internet novels, fan culture, and entertainment may be a consequence of internet censorship.

Websites hosted inside China can be warned or shut down if they violate rules of acceptable content; and individual netizens who post or distribute information deemed harmful by authorities have been threatened, intimidated, or thrown in jail, most often on national security charges such as “subversion” (Xiao, 2011b, p. 207). The control on the internet includes a tangle of restrictions and warnings backed by a formidable police force. Other penalties include confiscation of computers, mobile phones, and modems, or temporary suspension of network connections, license revocation, message eradication, account blocking, and so on.

---

76 Too many cases of people being punished for speaking or writing thoughts that are deemed illegal or harmful have happened since the internet was introduced (Cheung, 2005; R. Deibert, Palfrey, Rohozinski, Zittrain, & Haraszti, 2010, p. 458). In 1999 a businessman named Lin Hai was arrested by police in March 1998, accused of a “subversive act”, and sentenced to two years imprisonment on 20 January 1999 (J. L. Qiu, 1999). In 2002 a university student was detained because of her pro-democracy posts. This student, who has the screen name “Stainless Steel Mouse” began surfing the internet in 2000 and before her arrest, gained a good publicity from her personal writings. She was finally released a year later, mainly because of international pressure and criticism of the Chinese government (see Yardley, 2004). In 2004, a journalist was sentenced to jail for ten years because of his leak of a government email to a New York organization (Farrell, 2007). In 2010, a woman was sentenced to a year in a labor camp for sharing a Twitter post (Ng, 2013, pp. 62-63); and in 2013 some Chinese bloggers and micro-bloggers were detained. It was reported as early as in 2004 that China had the largest prison population of cyber dissidents in the world (Tkacik, 2004). 15 bloggers were detained in 2005 (S.-D. Liu, 2006), and one year later, the number reportedly increased to 50 (2006).
etc. This has produced a kind of chilling effect. A potential uncertainty often exists in the ill-defined and flexible border between tolerated and forbidden; and mysterious visits or calls from officials have intensified a climate of self-censorship. Because of the risks of sanctions, sticking to well-trodden areas makes sense (Stern & Hassid, 2012). Users have to bear in mind the guidance from the authorities and to know the threat of financial ruin or time in jail.

Serious internet control polices and enforcements have also contributed to a unique resistant culture in Chinese cyberspace. Although the censors watch closely over the Chinese cyberspace, many netizens, using either circumvention tools or the cover of anonymity or encoded euphemisms (and other symbolic tricks), are creative at expressing themselves in much bolder language and views than would be permitted in traditional media. The resistant dimension of Chinese cyberculture has been provoked by censorship, and in return challenged censorship. This emerging subculture seems to have been able to legitimize itself by deeply entangling in various socio-political and cultural processes.

---

77 This echoes the concept of political fear, which as Robin (2004) argues, “relies upon bystanders, whose passivity paves a path for elites and their collaborators, and the targeted community of victims, who transmit didactic tales of fear among themselves, thereby increasing its reverberating effects” (p. 181).

78 A co-founder of a non-profit organization which undermines the GFW is quoted as saying, “Censorship makes it harder to do simple tasks – but it’s way more complicated than that ... Many students complained after Google was blocked because they could not access a lot of information that was important for their studies. The point of the censorship is to make finding information hard for people and then to frustrate them to the level where they give up” (as cited in C. S. Yi, 2014).
CHAPTER II. CONDITIONS FOR INTERNET RESISTANCE

Despite the fact that the Chinese Government has closely controlled the internet in China, there are various forms of resistance to such control as well – a theme that has received insufficient academic attention to date. Internet resistance is directly provoked by internet censorship. Regarding those politically sensitive issues that cannot be spoken about in Chinese cyberspace, as discussed in the previous chapter, some are historically sensitive, and some are directly relevant to current socio-political crises (such as crony capitalism of the CCP, corruption, grassroots protests, or even the feminist movement\textsuperscript{79}). From this point of view, internet resistance not only challenges internet censorship per se but also echoes – and is sometimes consequential for – current socio-political crises faced by the CCP in a wider sense. Before a full discussion of internet resistance per se, this chapter focuses on the wider cultural and socio-political conditions for such resistance in Chinese cyberspace, which can be understood by examining five dimensions: changing state-society relations, the power of alternatives, grassroots resistance, the making of resistant youth, and the authorities’ adaptive control.

Changing State-Society Relations

A discussion of the cultural and socio-political origins of internet control and resistance in Chinese cyberspace may benefit our understanding of internet control and resistance. Three

\textsuperscript{79} A recent case happened in early March 2015 when five Chinese feminist activists were detained by the authorities on charges of disturbing public order.
issues will be discussed in this section. First, the current Chinese regime had long encountered various crises (most significantly, a legitimacy crisis) even before the internet era (Ding, 1994; Zhong, 1996). The starting of reform and the opening-up policy in the 1980s may have helped to resolve some problems, yet generated new ones: the Tiananmen Incident in 1989 and ten years later the Falun Gong Incident are symbols of the fierce outbreak of these crises. More social controls, and more censorship, have been placed on the free expression of the Chinese people (particularly dissidents); which, in return, deepens the political crisis and invites increasing bottom-up resistance. Second, the changes within Chinese intellectual elite and the elite culture, including their activities and ideas, may have functioned as a kind of enlightenment which has had a lasting influence on the general public (including the resisters in Chinese cyberspace later on). And third, with the rise of popular culture paving the road for the emerging cyberculture, some resistant elements of Chinese cyberculture have appeared.

Changes in the socio-political realm

The CCP encountered a legitimacy crisis soon after the Cultural Revolution.80 The pro-democracy movement in Tiananmen Square in 1989 is emblematic of its violent outbreak. This incident, eventually put down by military force, and officially denounced as a “counter-revolutionary riot,” has since become a political taboo in Mainland China. This incident has given the CCP a very poor international image and marked a “watershed in Chinese contemporary history” (Béja, 2011, p. 1). One significant consequence of the crackdown is that it has created some vigorous opponents of the regime. Many participants of this incident

80 This decade-long social-political movement (1966-1976), formally known as the Great Proletarian Cultural Revolution, was started by Mao Zedong (the founding father of PRC and former leader of the party) and aimed at wiping out capitalist and traditional elements from Chinese society and re-imposing Maoist thought as the dominant ideology within the Party. It ended soon after Mao’s death in 1976. The Cultural Revolution has a lasting influence on Chinese society as well as on social movements in Western countries. (Kraus, 2012)
have since exiled themselves overseas and been active in anti-CCP activities (H. Wang & Karl, 1998). With the development of the internet, these overseas dissidents, as well as dissidents remaining in China, have been greatly empowered and provided with a good space – publicly visible but anonymous – for spreading anti-CCP ideas and becoming connected with each other. Their voices comprise the main calls for freedom, democracy and mental emancipation in cyber China; calls which have resonated mainly with intellectuals and students, as well as attracting close monitoring from authorities.

Meanwhile, various “social fevers” have happened not only in socio-economic realms but also in cultural realms (D. Zhao, 2001, pp. 44-45).81 These fevers had the potential to function as a resistant power.82 A good example is the “Qigong Re” (Qigong Fever, or Qigong Boom) in Mainland China. Qigong became extraordinary popular in the 1980s and attracted millions of practitioners; it ended symbolically in 1999 when Falun Gong, one of the most popular Qigong organizations during that time, was banned by the CCP (Palmer, 2007). A huge population of Falun Gong followers have been pushed underground and out of China, and have become another group of vigorous opponents of the regime, involved in various anti-CCP activities both online and offline (see Chapter Three for discussion of Falun Gong’s hacking resistance).

The ruling political elite have tried to precipitate these crises by encouraging economic reform while preventing political reform, which marks the core characteristic of Chinese

---

81 Fever (“re” in Chinese) means “wave” or “tide”, referring to a sudden increase of interest in the same subject on the part of a large population (D. Zhao, 2001, p. 43).
82 As Wang (1996) finds, “what accompanied the onslaught of various ‘fevers’ in writers, artists, and intellectuals (the fever about One Hundred Years of Solitude in 1984, the fever for root-searching and new methodologies in 1985, Culture Fever in 1986) – in sum, post-revolutionary fevers about knowledge (zhishi re) and enlightenment – was the rise of new anti-cultural heroes such as the rock star Cui Jian and the post-Bei Dao generation of young poets who sneered at the myth of humanism and the politics of resistance that he once sang for” (p. 38).
modernization. Deng Xiaoping’s southern tour in 1992 helped to push marketization further (S. Zhao, 1993).\textsuperscript{83} This marketization trend has had a lasting influence on Chinese society. It empowers the ordinary people with more choices of products; yet at the same time, it generates new problems such as social inequality (e.g., H. Wang & Karl, 1998), ideological vacuum and moral decline (T. Yu, 2008) and cultural nihilism (Y. Guo, 2004; Steinmüller, 2011). Marketization has affected every aspect of Chinese society, with consumerism a new ideology guiding people’s everyday lives. Internet technology has deepened this trend.\textsuperscript{84} Although consumption of various products and content may become a hidden substitute for public protests (Stockmann & Gallagher, 2011), with more netizens involved in producing content (as prosumers), consumption itself may also function as a significant means of self-awareness. Through this process, netizens can feel the pleasure of identity, and in some circumstances, the process of consumption may eventually become politically significant (H. Yu, 2007a).

Other social movements, such as feminist movement, environmental movement and civil rights movement have gained an increasing popularity in China. With the rise of the internet – particularly the rise of SNSs such as Weibo – the resistant and liberating dimension of these

\textsuperscript{83} Deng Xiaoping was the leader of Mainland China between 1978 and 1992, who started a far-reaching market economic reform. He was famous for his pragmatic “cat theory,” claiming that “it does not matter whether the cat is white or black, as long as it catches the mice, it is a good cat” – with the metaphor of the cat’s color here referring to either socialism or capitalism.

\textsuperscript{84} Particularly after the rise of online shopping and the emergence of e-commerce companies such as Taobao, the trend of consumerism has been pushed further. Taobao, operated in China by Alibaba Group, is the dominant online shopping sites for Chinese (particularly youth). It set a record for highest single-day transaction volume during a special promotion on 11 November 2012, with the sales of goods on that day totaling ¥ 19.1 billion. The combined gross merchandise volume Taobao exceeded 1 trillion yuan for the year ended 31 March 2013. According to *The Economist* (Epstein, 2013), in 2012 China had more than 200 million online shoppers who spent going on $ 200 billion (not counting food and travel), ten times as much as in 2008; and Taobao was responsible for almost 60% of the parcels delivered by courier in China.
activities and ideas, as a challenge to mainstream discourses, have attracted many followers in Chinese cyberspace, which provides the background for internet resistance as well.

**The oppositional dimension of Chinese intellectuals**

Although it may not be necessary to date Chinese internet resistance back to Chinese intellectuals in the 1980s, the activities and ideas of the latter do have an indirect influence on the former which should not be overlooked.\(^8^5\) This section does not intend to cover every aspect of the Chinese intellectual’s political role in modern China – which itself has filled volumes (e.g., Ding, 1994; Gasster, 1969; Goldman & Gu, 2005) – but focuses mainly on the oppositional dimension of Chinese intellectuals.

Intellectuals in the Maoist era (1949-1976) were officially discriminated against as “choulaojiu” (stinking ninth, the penultimate of ten social categories); while in Deng Xiaoping’s era (1978-1992), they enjoyed relative freedom and were capable of creating quasi-autonomous associations to voice criticism and dissent against communism (Ding, 1994, p. 77). Two official campaigns in the 1980s further pushed many intellectuals to the opposite side of the political spectrum: the 1983-1984 Anti-Spiritual Pollution Campaign and the 1987 Anti-Bourgeois Liberalization Campaign.\(^8^6\) Many Chinese intellectuals have since separated themselves from the ruling ideology and engaged in political activities that exist outside the

---

\(^8^5\) It should be pointed out here that the category of “intellectuals,” as Ding (1994, p. 36) argues, has a much broader coverage in the Chinese context than in the Western, with professionals or white-collar workers and university students all included in this category. I follow the Chinese definition of intellectuals in a similar broad sense, which means that netizens with professional backgrounds, such as tertiary teachers, lawyers, and journalists are treated as intellectuals as well. Another issue is that we should not treat Chinese intellectuals as a homogenous group, which can sometime be explained by schemes of such as “Left versus Right” or “conservative versus liberal.” Sometimes, reality is much more complicated than these schemes.

\(^8^6\) The 1983-1984 Anti-Spiritual Pollution Campaign, started by conservative factions within the CCP, aimed to curb Western-inspired liberal ideas such as humanism, alienation, modernism and realism (Larson, 1989). Similarly, the 1987 Anti-Bourgeois Liberalization Campaign was an ideological movement opposing tendencies related to Western freedoms and defending the official ideology of “four cardinal principles.” Some prominent intellectuals (including journalists, writers and scientists) were expelled from the ruling party for their “bourgeois liberalization.”
political system, such as organizing independent salons and other activities colored by the terms of civil society (Gold, 1990). They may be directly involved in pro-democracy activities such as the Movement in Tiananmen in 1989. Various political ideas, including democratic, liberal, and neo-liberal ideas, criticism of the one-party regime and authoritarianism, have been introduced by these intellectuals and function to enlighten the general public (for university students in particular). Their voice has become the main voice urging the authorities to start a political reform (in addition to ongoing economic reforms) according to Western democratic principles (Castells, 2010, pp. 328-329).

After the flourishing of the internet (since 2003), these intellectuals soon found cyberspace to be an ideal place in which to speak out and to influence more ordinary Chinese (urban citizens in particular). Some of these intellectuals, such as neo-liberal Lang Xianping, have gained high profiles in cyberspace (see Thornton, 2010, pp. 186-190); they skilfully use all kinds of internet platforms (particularly blogs and micro-blogs) to air their ideas, attract huge numbers of followers in cyberspace, and gain the label of “public intellectuals.” In general, their ideas and activities in cyberspace might not have direct relations to internet resistance, but they do provoke some debates and cultivate an alternative space which is different from what the authorities plan to cultivate. Some of them go much further and their speech quite often runs counter to what the authorities will accept. The online activities of these public intellectuals have reportedly received close monitoring.87 From this point of view, the oppositional dimension of Chinese intellectuals should not be overlooked when discussing issues relevant to internet control and resistance.

87 An example of a closely monitored individual is He Weifang, a legal scholar at Peking University (Beijing, China) and an outspoken right-wing party member, who has argued that the CCP is an unregistered and therefore illegal organization in China (Y. Zhao & Chakravartty, 2007, pp. 47-48).
The rise of popular culture

The rise of popular culture marks a significant change in the Chinese cultural sphere. There are at least three reasons that have helped this to happen. Firstly, an increasing number of intellectuals (e.g., writers and film makers), waving farewell to elite culture, have shown an increasing emphasis on needs from the general public, as consumers of their ideas and publications, and have helped to provide an opportunity, and an alternative space, for the rise of popular culture. Secondly, commercial films and pop music which were previously unimaginable and inaccessible (at least publicly) have now poured in. Thirdly, the population of popular culture consumers has kept on increasing during recent years. Under these circumstances, Chinese popular culture gradually establishes itself in the cultural realm previously carved up between mainstream official culture and traditional elite culture.

Popular culture in China had enjoyed some flourishing time before the internet (e.g., in the 1980s), but with the help of the new technological platform – the internet – it has shown further, vital development, particularly since the late 1990s (Kang, 1997). Although in the later 1990s, the main actors in the cyberculture were elites, such as scientists, researchers, and university faculty in urban areas (Yongming Zhou, 2006, p. 136), with the striking increase in the population of ordinary netizens, there have been more and more discussions about popular culture (e.g., Hong Kong TV dramas, martial novels, foreign pop music and movies). The significant socio-cultural process through which southern dialects became diffused in northern

---

88 For example, the wave of popular music from Hong Kong and Taiwan has worked as a covert resistance against mainstream political music – the so-called “decadent voice” against the revolutionary and ideological music produced by party artists (X. Zhou, 2007, pp. 106-107). Jin Yong’s martial arts novels have catered for ordinary people’s dreamlike imaginations and expectations. Stephen Chow’s black humor spoof films, such as A Chinese Odyssey (1995), have blazed a path for a culture that challenges the traditional and mainstream culture. The popular trends of Korean and Japanese culture have also influenced many young Chinese fans.
China seems to have been sped up by internet technologies. English words can also influence the everyday language usage of ordinary Chinese netizens, with a huge number of homophones of English words becoming popular in Chinese cyberspace.

Meanwhile, popular writing has become an increasingly important part of Chinese popular culture (particularly after the rise of blogging). In the internet era, publishing, previously an elite privilege, has become a quotidian behavior of many ordinary netizens (Brokaw & Reed, 2010; Y. Feng & Wei, 1997, p. 8). As a result, online literature has blossomed, which is partially revealed by new terms such as “wangluo xiaoshuo” (online novel), “wangluo xieshou” (online writer) and “wangluo wenxue” (online literature) (J. Guo, 2014; Hockx, 2015; Ouyang, 2011). Online literature is relatively informal, light-hearted and loose, and focuses more on themes of love, absurdity, sex and violence (e.g., J. Feng, 2013; Henningsen, 2011). In a broad sense, it signals a rebellion by popular writing against classical literature and by cyberculture against elite culture. The rise of blogging makes the resistant dimension of popular writing even more obvious; blogging generally accelerates the rise of citizen

---

89 In Chinese history, Beijing dialect (a northern dialect) has long been promoted by the authorities as the official language (known now as Mandarin); other dialects are much marginalized. This landscape of Chinese dialects is mainly produced by the political power (as an agenda for ideological unification). In the tide of the reform and opening up, Mainland Chinese showed great enthusiasm in learning from the already-modernized Hong Kong and Taiwan, discourses being a part of this learning. The market shows some power in reconstructing the landscape of Chinese dialects. For instance, the popular online epithet “Konglong” (dinosaur), referring to ugly female netizens, originates from Taiwanese universities; “I Fule U (I admire you, with “fule” meaning “admire”)” was the result of a Hong Kong film A Chinese Odyssey (1995).

90 For example, “hongbeiji” (baked chicken) refers to “homepage,” and “mao” (cat) refers to “modem.” New sentences of greeting such as “Have you used yahoo?” or “Have you been online?” were even more popular than the traditional greeting “Have you eaten?” Two reasons might have determined these bilingual or multilingual phenomena. The first is that, because English was the dominant language on websites – reportedly 85% of web pages were in English, Chinese netizens had to follow this habit in the early days of the internet. The second and more important reason is that there had long existed a deep admiration and longing for Western modernization. Following foreign popular culture and using English phrases became a symbol of fashion and modernization. These online discourses mirrored this socio-cultural transition in contemporary China.

91 This is why Wang Shuo, a popular writer of hooligan literature, once spoke very highly of online literature as “it represents the future of literature” (see G. Yu, 2001a, p. 202). For more information about the resistant dimension of Chinese online literature, see C.S.-M (2013).
journalism and has the potential to empower increasing numbers of Chinese netizens to get involved in political discussion and activities (Bei, 2013; Hassid, 2012; X. Zhou, 2009). As discussed in Chapter Four, netizens (bloggers in particular) may use various esoteric ways of writing in order to breach the censorship system.

The Power of Alternatives

Increasing alternatives in the socio-political realm may not necessarily cause direct challenges to the ruling party, but they do help to cultivate a dynamic environment in which new forms of resistance (including internet resistance) may arise. This section focuses on three main kinds of such alternative – alternative media by dissidents, activist professionals, and the possibilities provided by the West.

Dissident media

Since the Tiananmen Incident, many overseas Chinese newspapers, mainly located in North America (partially because it is one of several main destinations for Chinese immigration), have been published, which are used by dissidents as tools to continue with the unsuccessful democratic goals of the 1989 Incident. Various Chinese news portals were afterwards launched overseas, aiming mainly at providing uncensored news for (and extending their influence to) Chinese readers within the Great Firewall. Boxun (boxun.com) and Duowei (dwnews.com) are two of many such portals which became virtual camps for overseas Chinese dissidents after 1989.\(^92\) Much news that was censored within the GFW could be accessed via

\(^{92}\) Boxun News was launched by Shi Wei in 2000 with its main server located in North Carolina, U.S. Although it has claimed several times that this news portal was operated independently with a citizen journalism model and had no political bias, it has reportedly received financial support from National Endowment for Democracy (NED). It reportedly has a close relationship with Jiang Zemin’s Shanghai Gang within the CCP; particularly after the Bo Xilai event in 2012, some commentators believed that Boxun News was the overseas mouthpiece of Jiang’s faction, via which they potentially leaked bad news about their political
these portals. Some Mainland activists have formed close relationships with these portals and when they are unable to publish sensitive materials on domestic websites, they will leak them to these portals. A recent case of this kind happened in 2014 when an activist name Xiang Nanfu was arrested by Beijing police for “selling false stories” to the foreign media (BBC, 2014).

These overseas Chinese news portals, along with other Chinese websites such as U.S.-based Wenxuecheng (wenxuecity.com) and online liberal tabloids produced by Hong Kong or Taiwan media, are not tolerated by the Chinese authorities and have received fierce blockage by the GFW.93 However, the relationship between the Chinese authorities and these “dangerous” overseas Chinese online media has been dynamic over recent years. Since being acquired and controlled by an anonymous capitalist owner from Hong Kong in 2009, Duowei’s editorial policy has changed gradually, with more and more news citing China’s official media resources such as Xinhua News Agency or The China News Service. It has been reported that “for many mainland readers nowadays, when they successfully breached the Great Firewall and reached Duowei, they would doubt if they were still inside the firewall.”94 Besides such covert control, appointing key personnel is another common strategy for the Chinese authorities to control the media – a strategy often used towards Hong Kong-based opponents within the party and thus discredited them. This news portal became known to ordinary Mainland Chinese in 2014 for after the Xiang Nanfu case. Duowei News was a New York-based portal. Launched in 1999, it claimed a position of political neutrality. Official news from Mainland China, Hong Kong, Macao and Taiwan, news of overseas Chinese pro-democracy activists, dissidents and Falun Gong could all be seen here. It was one of the earliest overseas Chinese websites to be blocked by the Great Firewall. 

93 However, some Chinese versions of English news portals such as Wall Street Journal and Financial Times are accessible in Mainland China. At the time of writing, searching with the keyword of “boxun” on Chinese search engine Baidu, only a brief introduction of this news portal could be shown, with no result of its domain name or website address provided.

94 My translation. The original text refers to (Yu Zhou, Duan, & Li, 2010), a report made by the Hong Kong-based Phoenix Weekly. This article is now unavailable within the firewall; only some overseas Chinese websites which had forwarded it have the text (see for example Boxun Wang, 2010).
media (H. Fu & Cullen, 2011), which has invited suggestions that the CCP has tried to control foreign Chinese news media and that the methods seem to be extremely covert and tactical.

There is no evidence so far that these dissident media cooperate harmoniously together to resist the CCP and its internet censorship policy. According to the relevant editor statements on their websites, the relationship between Boxun and Duowei, at least, seems not harmonious at all, since they quite often criticize each other for “having a vague relationship with the CCP.” Despite the CCP’s endeavor to control the overseas dissident media, either by overtly blocking them or by covertly casting some influence on them (Q. He, 2008), these media – news portals in particular – still have the potential to function as alternative media for Chinese readers.

**Activist professionals**

Various recent studies about “the relationship between elite and the state regarding governance and social control” (e.g., Schatz, 2009; Wedeen, 1999) show a rising consensus that “rules for daily behaviour” are not handed down from the pinnacle of the state but jointly written (and rewritten) by public professionals and their government overseers (Migdal, 2001, p. 11). Even in a place where freedom of speech is decidedly limited, the boldest public professionals have some room for a “critique within the hegemony,” particularly cloaked in allegiance to party and nation (Scott, 1990, p. 106). Although in China only a small group of public professionals such as journalists, lawyers and other public intellectuals, as well as some ordinary protestors and activists, are touched on by the triad of state coercion (administrative punishment, imprisonment, and violence), the uncertainty about boundaries of the permissible could magnify the effect of any isolated incidents (Stern & Hassid, 2012). Many recent
incidents are disseminated, at least partially, in cyberspace; in fact, some of the public professionals are internet celebrities. Though it is hard to tell the extent of their influence, public intellectuals have tried hard to influence as many ordinary netizens as possible with democratic ideas and other modern ideas (such as liberal ideas, freedom of speech, human rights, and other ideas mentioned in the previous section). From this point of view, when discussing internet resistance, the power of public professionals, particularly activist professionals, should be taken into consideration.

The commercialization of traditionally party-controlled media has significantly influenced the Chinese media landscape. Journalists from commercial media organizations have more motives and ability to follow the principles of news and treat the media as the fourth estate. For example, when the SARS epidemic broke out in 2003, it was a journalist from Southern News Media Group (which is the most commercialized media group in Mainland China) who first reported some of the truth about this epidemic. Some local news media choose to play their cards safely: they cooperate with their local authorities in order not to irritate them by uncovering “bad” local news (see P. P. Pan, 2008, pp. 235-267). This does not prevent some newspapers from standing out by reporting “bad” news about other local governments (from

95 Apart the scholars mentioned in the previous section, there are more loose intellectual organizations formed in Chinese cyberspace. For example, Potu Wang (http://www.groundbreaking.cn/), a rising website created collectively by some young scholars from universities of Mainland China (Beijing in particular) and Hong Kong, has attracted a group of high-profile intellectuals to publish articles about grassroots issues and critiques of new liberalism. Another case is Zhengjian Wang (http://cnpolitics.org/). Created in November 2011, it claims to devote to introduce contemporary Western political ideas to Chinese readers and has since become an emerging virtual camp for some young political scholars in China.

96 However, at the same time, the business model of Chinese journalism has some dark consequences such as corruption. It is a hidden culture that some Chinese journalists accept money to cover up “bad” news or even threaten relevant parties by blackmailing and asking for bribes. For details see (Epstein, 2008; Y. Hu, 2014).

97 It should be pointed out that all the commercialized media in Mainland China are still under the control of the party and a complicated censorship system still functions in this commercialization context. From this point of view, journalists cannot publish whatever they like; quite the opposite: they still receive forms of pressure from the censors at a higher level. The Southern Weekend case in 2013 fully explained this dilemma (see Ng, 2013, p. 57).
other neighborhoods), which is relatively safe to do, and may attract more attention from the
general public (a signal of commercial success). To publish investigative stories in
newspapers outside of the provinces where these “bad” stories have happened is a common
strategy for investigative journalists. Moreover, an informal journalistic culture of publishing
investigative journalism in local, rather than national, news channels seems to have formed in
China (K.-w. Fu & Chau, 2013). Some journalists are good at “playing the edge ball” (da ca
bian qiu), pushing the boundaries of acceptable coverage and expanding media’s right to
participate in public discussions and policy issues.

Since blogging technologies were introduced into China in around 2003, more and more
Chinese journalists have acquired their own personal blogs, either within the media outlets’
websites or in public sites (Clayton, et al., 2006). With a number of strategies to deal with the
emerging internet censorship, many bloggers of the time believed that the Chinese
blogosphere was slowly pushing back the boundaries of what was defined as sensitive. This
optimistic view was shared by overseas observers. In May 2005, a New York Times columnist
wrote an op-ed titled “Death by a Thousand Blogs,” in which he concluded that “it’s the
Chinese leadership itself that is digging the Communist Party’s grave, by giving the Chinese
people broadband” (Kristof, 2005b). Within their personal blogs, journalists addressing
sensitive subjects usually exercise caution and carefully choose their words. Therefore,
compared with censorship pressure from traditional media, they can be less affected in
cyberspace (Clayton, et al., 2006), though internet censorship does exit.

---

98 This journalistic culture can be explained by the Sanlu case. When the Sanlu Milk Company in Hebei
province was involved in a milk scandal in 2008, the first newspaper story on it was published in Shanghai-based
Oriental Morning News (G. Yang, 2013).
Some professional investigative journalists are well aware of tactics to eliminate risks and to protect themselves. One journalist revealed on his blog that he would strategically hold back some sensitive information for the reason of self-protection when reporting certain cases involving legal and political risks (see Hand, 2006). Other strategies include making some sensitive articles visible only to trusted people, changing their blogging hosts frequently or blogging at several hosts at the same time, or even blogging on overseas websites. Discursive tactics are also greatly used within professional blogging spheres. After unsuccessful attempts to post a sensitive topic, a professional blogger then might use Pinyin to replace the original sensitive title and repost it (see Clayton, et al., 2006). Similar to the discursive tactics used by some ordinary netizens (which will be fully analyzed in Chapter Four), clever ways to get information published have long included symbolic “weapons of the weak,” such as replacing sensitive words with similar, non-sensitive words or abbreviations. Meanwhile, reporters use implicit, sometimes satirical, wordings which are comprehensible to readers and which may help them to escape external censors and avoid potential troubles.

Because of their activities, professionals in the internet age have gradually shown their ability in deconstructing the top-down digital domination within Chinese cyberspace. Numerous self-appointed journalists emerge in cyberspace (Kristof, 2005b), so do feminists and LGBT activists who can find like-minded people more easily with the help of internet technologies (Ho, 2007; D. Zhang, et al., 2007). Rights-advocacy lawyers (weiquan lâshi) more easily receive sympathy and support as well (Stern & Hassid, 2012). The online activities of activist professionals have increased the authorities’ fears about “citizen
journalism” which is treated as a challenge to their digital domination, and numerous censorship cases exist in Chinese cyberspace as consequences of this fear.99

Different rights-advocacy lawyers may have different reasons for becoming dedicated to field of law they work in. But many of them share some general features, for example focusing on news events which are relevant to human rights, providing legal aid for disadvantaged groups, and using legal institutions and other platforms to make positive change within China’s authoritarian system.100 Through these activities, a group of rights-advocacy lawyers became famous both domestically and internationally. They have attracted attention from foreign media, NGOs and governments, and have received overseas funding, which makes cooperation with the Chinese system gradually impossible. They seek alternative channels through which to legitimize their activities, for example, organizing academic conferences over a law case, and campaigning for support in the media and the general public. For these purposes, the internet has become an important field for these lawyers to disseminate information and raise their profiles.101

99 I use “citizen journalism” here in Luke Goode’s (2009) sense – citizen journalism, including “metajournalism” as well as the practices of journalism itself, is not an exclusively online phenomenon and cannot be confined to explicitly ‘alternative’ news sources. But what should be pointed out here is that this concept has never entered the Chinese official discursive system (partially because of its underlying political metaphor—democracy and beyond—and partially because its relevant practices often involve sensitive issues). Other politically neutral yet filtered concepts such as “wangluo xinwen (online news)” and “wangluo jizhe (online journalist)” are introduced. This is not an issue of semantics or of translation, but rather a discursively political activity. As shown in the first chapter, the authorities have kept tight control on online news and online content by passing a series of regulatory laws and policies. The filtered concept “online news” in the Chinese context thus is much different from “citizen journalism” in the Western context.

100 Some currently active lawyers, such as Pu Zhiqiang, are themselves participants of Tiananmen Incident and have personally been involved in the democracy movement; others such as Teng Biao and Xu Zhiyong became active in social events (e.g., the Sun Zhigang incident in 2003) (H. Fu & Cullen, 2011; Hand, 2006).

101 For example see Liu Lu’s book Weiquan lvshi: yige weixian de zhiye (Weiquan Lawyers: A Dangerous Profession). A lawyer has shared his media strategies: “Being vocal means to make comments on every public event, including not only publishing articles online, but also making comments in influential media in China and overseas, such as Voice of America, Radio Free Asia, Radio Taiwan International and others; it also means to lead and organize as many signature campaigns as possible. In an era with advanced information technology, this method may give you instant fame. The authorities dare not to touch you once you have become internationally famous” (as cited in Hand, 2006).
Many other types of professionals have gained high profiles in Chinese cyberspace, too. With millions of followers, businessmen such as Charles Xue (11 million followers), Pan Shiyi (17 million followers), Ren Zhiqiang (24 million followers) and Kai-Fu Lee (51 million followers) have become opinion leaders on Sina Weibo, and occasionally touch on sensitive issues such as air pollution (Lu, 2013). The majority of Chinese entertainment celebrities, too, apply internet technologies to gain publicity, and some of them tweet quite often about sensitive issues relevant to human rights, food safety, environmental protection, and so on. And a group of university professors, such as Zhang Ming from Renmin University of China and Zi Zhongyun from Tsinghua University, who have become public intellectuals, have attracted a huge number of followers online.

The Western influence
The collapse of the Soviet Union and Eastern Europe around 1990 means an end to the old Cold War (between the U.S.S.R. and the U.S.) and the possible start of a new Cold War between China and the U.S. (see Suettinger, 2003, p. 358). With China as the biggest of the remaining five socialist states, the Chinese authorities (as well as mainstream media discourses) have become very alert towards Western cultural products, since many of them believe that such products can bring “peaceful evolution” (Ong, 2007; S. Zhao, 1993) to China.

---

102 A unique phenomenon in Chinese cyberspace is that, particularly on the Sina Weibo platform, a small number of high-follower-counts contribute a majority of the posts and draw the most attention (K.-w. Fu & Chau, 2013).

103 In February 2013 Kai-fu Lee’s account on Sina Weibo was briefly suspended when he blogged about the troubles of a party-sponsored search engine, Zhongguo Sosuo (chinaso.com), which has hardly any users.

104 It is common for some university teachers to criticize the authorities’ censorship and propaganda policy in China nowadays. Besides talking on media (including online), they more often communicate some sensitive content in classrooms. Some have received personal punishment. For example, in 2005, a university professor lost his job after posting an article criticizing the propaganda department. Again, in 2013, two teachers, Xia Yeliang and Zhang Xuezhong, from Peking University and East China University of Political Science and Law respectively, were fired because of their criticism of the political regime and the CCP. A more recent case in 2014 was a Uighur scholar who received a life sentence for allegedly promoting “separatism” for his homeland.
and thus endanger the domination of the CCP. This acknowledgement of “hostile foreign forces” has greatly impacted the attitudes of Chinese authorities towards Western cultural products and their activities in Mainland China. VOA, RFA and many other broadcasting platforms have worked actively to provide “freer” information for the Chinese audience, and the authorities have accordingly blocked, or attempted to block, their signals. A similar fate happened to endeavors by various U.S.-based TV stations to enter the Chinese market, with the failure of Murdoch’s Star TV in Mainland China as the most significant, even though the latter had practiced self-restraint to avoid losing such a large market (see Castells, 2010, p. 328). In terms of the internet industry, many Western internet companies such as Microsoft, Yahoo!, and Google have been allowed to operate in China, but most of them have subsequently had to declare their failure.105 An annual report on China’s new media published by the Chinese Academy of Social Sciences (CASS), a top Chinese think tank, suggested in 2010 that Western nations (including the U.S.) use SNSs such as Facebook to foment instability and thus threaten state security in China (Yin, 2010).

Meanwhile, in order to develop the country’s market economy and attract more Western investment in China, the authorities work hard to manage the country’s image, in the eyes of the international world, as an open and free one. As a result, many Western newspapers and journals are allowed to build reporter stations within Mainland China, although they are under strict control and some of them remain underground. They hire Chinese who are fluent in English (and/or other languages) to collect information for their news stories; under some circumstances, articles are directly written by these Chinese journalists. Some Western

---

105 Despite this, some liberal minded employees within the Chinese system are reportedly often providing information about its shortcomings to overseas websites. Refer to Epstein (2013).
journalists and researchers are also active in promoting human rights, freedom of speech, and democracy in Mainland China. They not only build strong links with the activists located within China, but also give both moral and intellectual support to them. Again, there is strict control on this population. For example, evidence showed in 2005 that simply in several months’ time, a dozen journalists (including for example Shi Tao, Zhao Yan, Zhang Lin, and Huang Jinqui) who had relationships with Western media had been arrested in Mainland China (see P. P. Pan, 2005b). It is impossible to have a precise number of how many reporters are arrested, but China reportedly imprisons far more journalists than any other country (Kristof, 2005a).

Foreign NGOs have marked their presence in China by giving support to domestic NGOs and criticizing China’s environmental and human rights record, and their record on other issues, which has annoyed the Chinese authorities greatly (as does the U.S. Government’s publishing of annual reports on human rights in China). Furthermore, Western capital enters China as financial support for democracy movements and activists as well. For example, the U.S. non-profit National Endowment for Democracy (NED), has funded Chinese human rights activists, pro-democracy freelancers and other resisters to the regime, and has also been active in promoting civil democratic activities in China. Overseas Chinese dissidents involved in developing anti-GFW tools also reportedly have financial relationships with such organizations (as will be discussed in Chapter Three).

---

106 Similar cases have happened in other authoritarian regimes as well. For example, Muslim youth activists in the Egyptian uprising in 2011 received both U.S. government funding and NED funds (see Herrera, 2014).
Cultural products such as American movies and TV dramas have also become prevalent in China over the past two decades. The increasing proportion of imported programs to the total programming time has provoked fierce conservative responses, such as serious control of the amount of imported programs. In 2014, the Chinese censors placed a new policy on domestic streaming video websites, obliging them to remove some popular American TV shows (such as *The Big Bang Theory, The Good Wife, NCIS, and The Practice*). This activity seems to have annoyed a huge number of fans of American TV shows, and thus received fierce criticism from them. These fans mocked this activity as “the Big Ban Theory.” Similar bans may have worked well in a pre-internet era; in the internet era, the answer may not be so obvious. The entertainment field has become a resistant space for fans, game-players, and so on, who often find ways to challenge the censorship system and make it less effective (as Chapter Six will analyze in more detail).

**Grassroots Resistance**

How to deal with social problems, as the unavoidable price of modernization, has long been a key priority of the Chinese authorities, although in the official discourse it is often expressed as “minsheng wenti” (problems regarding people’s livelihood), which include issues of education, employment, income, welfare, housing and health care, among others. In addition to media and academic discourses on these issues, which set the agenda for the general public, many ordinary people themselves also show an increasing concern about these

---

107 It was in 1994 when Hollywood blockbusters were first officially imported and had exerted tremendous impacts. A handful of Hollywood imports took over 50% of the annual box-office revenues. This trend was somewhat changed in 2002 – partly because of the success of Zhang Yimou’s *Hero* and other Chinese “big pictures.”
issues, based on their quotidian experience. Although Chinese officials have long controlled the information about social protests which make it very difficult to get reliable statistical data (Kuah-Pearce & Guiheux, 2009, p. 26), anecdotal data does suggest that social protests have undergone an sharp increase in recent years (Cai, 2010, pp. 208-213; Jae, 2004; Lee, 2007, p. 5). This section deals with the issue of general grassroots resistance and its strategies in the internet age.

**Social problems**

The first tide of unrest which arose across the whole country happened in the 1990s after the Chinese Government carried out the reform of state-owned enterprises involving millions of laid-off workers (Cai, 2002; Lee, 2010a, 2010b; Rocca, 2009; Solinger, 2001), and more recently there have been rural conflicts (Friedman, Pickowicz, & Selden, 2007; Ying, 2010) and peasant resistance (Herrold-Menzies, 2010; O'Brien, 2009). After entering the new millennium, food safety has become another crucial everyday concern for many ordinary people and provoked huge counter-hegemonic practices such as diffused contention or direct protest (G. Yang, 2013). Pollution and environmental protection movements (e.g., anti-paraxylene [PX] chemical production project protests in various cities), and various other issues, such as slave labor in a brick kilns in Shanxi, and the “nail house” case in Chongqing in which property rights against developers were claimed (more cases see Cai, 2005), attract huge media coverage and provoke heated public discussion (including online discussion). Besides all kinds of sensitive social events, issues relevant to governance (such as corruption,
and social injustice), police violence, public health, judicial reform and natural disasters also become main concerns for many ordinary people.  

Many of these issues have received tightened control (at different levels of the political system) and are not able (or at least, not expected) to threaten the CCP’s stay in power. Some cases may not be sensitive at the central level but may be sensitive at the local level. With the local authorities too involved in, and trying to manipulate, the circulation of information online, censorship (and accordingly resistance to censorship) does happen in almost every grassroots protest. In a more indirect way, these social protest cases do help to cultivate an informal culture within which resistance to the powerful can be practiced. These social problems and events provide the material and atmosphere for online resistance. For some ordinary Chinese people, publicly appealing for rights and justice might not be the first choice. In many cases, they may easily accept private and peaceful ways to solve their problems, partially because, as they are located at the bottom of the social-economic hierarchy, they may encounter risks when displaying collective and public defiance. This, however, does not prevent some ordinary people from using some radical means to express their demands, which has been revealed by an increasing number of cases in recent years. I will come back to this theme in Chapter Six.

---

108 For example, in 2010, a 22-year-old driver killed one person and injured another in a speeding road accident. After being stopped by the angry crowd, he said that “Go ahead, sue me if you dare. My dad is Li Gang!” (a deputy police chief in a nearby district). This event spread virally on social media and attracted fierce criticism of “guanerdai” (children of privileged government officials) (Bamman, et al., 2012; Tai, 2015).

109 At a time when spending on maintaining stability (weiwen) rivals the defense budget in China. See (Stern & Hassid, 2012). This observation was supported by a report (K. Xu, Chen, & Li, 2011) by Caijing, a top financial magazine in China, which suggested that the Chinese government’s spending on public safety (with maintaining stability its main priority) surpassed the military budget by reaching ¥ 624.421 billion (equal to $ 100.25 billion). For further evidences see Q. He (2012).
A bottom-up perspective

In order to maintain their power, in an authoritarian regime, the authorities may respond positively to the rational appeals behind grassroots protests. For example, in research (J. Chen, Pan, & Xu, 2014) into the attitudes of county level governments in China towards grassroots protests, the researchers find that one third of the governments have responded somehow constructively to online protests (regarding issues of social welfare). Particularly when the grassroots threatens to perform collective protests and threatens local governments with disclosure to upper levels of government, the local governments are more likely to respond to grassroots protests and do it publicly (rather than privately). But cruel suppression, such as detention of protestors, may still be applied at the same time (Y. Zhao, 2007).

In the Chinese political system, the lower level cadres need to balance their relationships both between the upper levels of government and between people within the jurisdiction. Towards the upper levels of government, they display their loyalty and show the effectiveness of their governing; they want to control the image they present to their superiors in order to improve their advancement prospects within the CCP. While towards bottom-up unrest, they mitigate social controversy, in order to complete their terms peacefully and smoothly, and to avoid any significant collective protest.

---

110 China’s current formal administrative hierarchy includes the national, provincial, prefecture, county, and the town or township levels of government. Villages are not part of the formal administrative structure, but, according to the 1982 PRC constitution, are self-governing units. A town is more urbanized than a township. (Joseph, 2014, p. 295).

111 According to China’s cadre evaluation system, also known as the nomenklatura system, a CCP institution that controls cadres’ access to positions of power, if there is any massive incident which has happened within an individual’s jurisdiction, it means a political taint for him or her, and his or her progress within the cadre system might be negatively affected. The magnitude of massive action both online and offline, becomes an index for upper levels of government to assess the local governments’ performance, which could eventually decide whether relevant cadres are promoted to higher positions of power or not.
These two issues together decide which kind of response the lower levels of government adopt towards protests – positive response or negative suppression – although more often, both these approaches may be used at the same time. The increasing population of grassroots activists who apply the means of petitioning to upper levels of government has accordingly invited the local authorities to place an increasingly tight control on these petitions, which includes using massive surveillance services and censorship tools (both automatic and manual, as discussed in Chapter One). Though there are no directly available statistics about the number of grassroots protests that have circulated online and been monitored by the relevant authorities, as discussed later, it is likely to be a significant number.112

The Chinese political system is never a monolithic system. The relationship between the central and the local has long been tense (T. Gong, 2006; X. Guo, 2001); some forms of civil disobedience which are tolerable for upper levels of government may be unbearable for lower levels of government. In fact, although not all grassroots protests are bearable for the Central Government, it may tolerate (and even encourage) some protests that target local leadership and local practices (e.g., G. Yang, 2009, p. 34), which imbues citizens with the ability to sanction lower level leaders, and push the latter to govern in a more effective way. Protesters have increasingly recognized this nuanced difference between upper and lower levels of government, and have gradually formed a useful protesting strategy – only protesting against the local government and carefully avoiding challenging the central authority (see the foreword in E. J. Perry & Selden, 2014). For instance, in the Wukan protest (Hess, 2015), a massive anti-corruption protest in Guangdong province in September 2011, the protesters put

---

112 According to the Blue Book (Lin Li & Tian, 2010) published by the CASS, an uncompleted statistic revealed that in 1993 there were 8,700 grassroots protests, which was ten times the number in 2005 and has kept increasing since.
up a banner reading “Please tell the government in Beijing to save Wukan.” Banners like this, at many protest events, invite not only the Central Government to place some administrative pressure on the relevant local government, but also invite media to generate public pressure.

The weak also form some informal organizations to enlarge their voice. For example farmers in China, Y. Zhao’s (2007) research finds, have built collaborative relationships to gather and share information (e.g., communicate official documents to farmers), define issues, and set the substantive agenda for their resistance. It is unsurprising that these unofficial unions and other forms of autonomous organizations often operate under harassment and violent repression from local officials (see J. Yu, 2003).

**Strategies for seeking publicity**

The relationship between grassroots resistance and the media has become a heated topic recently (e.g., Y. Zhao, 2007). Since most instances of grassroots resistance in China nowadays are against the lower levels of government (as discussed above), some liberal media operating at national or provincial levels may sometimes produce sympathetic coverage of these protesters. Conversely, media at the municipal level are more likely to stand together with the local authorities and act as a mouthpiece, for example, by trying to quell rumors and showing the efforts local authorities have made. The tone of such biased coverage is often that “an uninformed village mass had been misled by a few individuals with ‘ulterior

---

113 These media are often more commercialized with professional and “brave” journalists. However, some very official media at a national level could also touch on sensitive issues about lower levels of government (traditionally as a control strategy of the CCP to deal with the relationship between the state and the local), with the investigative news program “Jiaodian Fangtan” (Focus) by China Central Television as a good example (see Chan, 2002).

114 The reason why in China the local media and local authorities often stand together to each other is, at least partially, because the media has long been a party-run mouthpiece. The staff in media organizations often have good personal relationship with local authorities. Local media is used by local authorities as a selective performance show (to emphasize good news yet at the same time hold back bad news) to upper levels of government.
motives.’ The biased coverage does not help to solve problems; rather, it is more likely to provoke more negative responses from protesters (and public sympathy for them as well) and thus unintentionally encourage more protests, both in that county and in other counties with similar problems.

Another common strategy for grassroots protesters is that of leaking protesting information, and/or “bad” news about their local government and authorities, to the media in areas outside the jurisdiction of the relevant authority, since within the Chinese media landscape, media outside a given jurisdiction has less pressure than local media over uncovering sensitive stories (about the local governance in that jurisdiction). The media that have bravely reported similar stories (functioning as the fourth estate) have even been treated as media versions of “qingtian laoye” (literally “blue sky grandpa,” a Chinese term meaning a righteous official in ancient times), and attract more grassroots people to turn to them to seek help. In order to attract media coverage (communicating their resistance and desperation) and thus pressure relevant authorities to solve their problems, several extreme cases have recently occurred in which petitioners have committed suicide right outside the newspaper building of Beijing-based *China Youth Daily* (Cao & Chang, 2014).

Leaking to foreign media has also become very popular for grassroots resisters. When published in international outlets, the stories will more easily gain attention from domestic media and thus form a dense pressure on Chinese authorities to solve relevant problems. This can be termed a “boomerang strategy” (as will be discussed in Chapter Six). Similar to this

---

115 It is common that local authorities have some conflicts of interest between one other (particularly those which share borders, rivers, mines etc.). Schisms like this between local authorities can often be triangulated and exploited by public professionals, including media professionals, pushing an agenda. The state is certainly aware of this possibility; to prevent such strategizing, journalists are officially banned from reporting outside their region although this restriction is often ignored (refer to Stern & Hassid, 2012).
media strategy, many cases have shown that petitioners also protest outside the U.S. Embassy, rather than relevant Chinese departments, in order to criticize the Chinese departments’ breach of duty, with the hope that the U.S. Government may pressure the Chinese authorities through diplomatic means. Seeking help either from the foreign media or from foreign services in China, typically denounced by the authorities as “gao yang zhuang” (petitioning foreigners) (Lianjiang Li, Liu, & O'Brien, 2012), is believed by the protesters to mean more chance of problems being solved.

With the rise of the internet, venues for grassroots protests have expanded and possibilities for connected political action have increased (King, et al., 2013; T. Meng, Pan, & Yang, 2014; G. Yang, 2013). Grassroots resisters in the internet era can easily connect with rights-protection activists, who often gain high profiles via internet activities, because digital activists have relatively mature networks with each other and the media (both foreign and domestic), and, more importantly, they have experience and are willing to offer help. Help from digital activists not only gives resisters more opportunities of gaining publicity from the media and public, and of exerting pressure on relevant parties; but also can more easily unite resisters with similar appeals regardless of geographical barriers (as Chapter Six will analyze in more detail).

The Making of Resistant Youth

Cyberculture, which has long been dominated by the youthful, represents a dynamic aspect of youth culture. While much evidence could be found in other cultural contexts as well, in the

---

116 There is no official statistics on internet protests, mainly because of political sensitivity. But as Zheng (2008, p. 41) argues, we can observe internet protest via an indirect indicator - internet arrests – which have taken place frequently since the late 1990s.
specific case of China, the population of netizens in 2013 who were aged 20 to 29 was 192.82 million people (about 14.2% of the entire Chinese population and 31.2% of its netizen population). If taking into consideration the age group of 10 to 19, the population of young netizens rises significantly, to 341.75 million – about 25.1% of the entire Chinese population (CNNIC, 2014). To achieve a better understanding of the cultural features of internet resistance, we should have a close understanding of the features of youth in China today.

**The youth generation**

The current young Chinese netizens are generations of the one-child family policy. Introduced in 1979, the one-child policy has proved to have significant influence on Chinese social lives (Ebenstein, 2010a; Fong, 2002; Hesketh, Li, & Zhu, 2005; Y. Zhang & Goza, 2006). One of these effects is hidden problems among the youth group. This policy not only results in an excess of boys (Ebenstein, 2010b; W. X. Zhu, Lu, & Hesketh, 2009) but also brings psychological consequences for the large number of only children (Hesketh & Zhu, 1997). For example, the phenomenon of “xiao huangdi” (little emperors) or “wo shidai” (me generation) has once been very heated in media discourses, and coverage on behavioral problems of this “spoiled” generation abounds (Rosen, 2010). The first generation of the single child also happens to be the first generation brought up with the rapid development of mass consumption, and such children enjoy much better economic conditions than their parents did (B. Zhao, 1997). The consequences of the one-child policy have marked young Chinese netizens with unique features (compared with their Western counterparts).

Another crucial factor that shapes Chinese youth is the education system. In 1993, Chinese policy makers approved “Reform and Development of Education in China,” which officially
“made a firm commitment to the abolition of the job assignment system, and called for rapid expansion of both formal and adult higher education systems in response to escalating economic change, and an apparently more stable political situation” (Hayhoe, 1996, p. 241). A sudden increase in the enrolment numbers of universities and colleges has begun since then, with the number of tertiary education students growing at approximately 30% per year since 1999 and the number of graduates at all levels of higher education in China almost quadrupling during 2005-2011. In July 2014, a record 7.26 million Chinese graduated from universities – more than seven times the number 15 years ago (Sharma, 2014). An official rate for new graduate unemployment in 2013 was 17.6% (7.6% higher than that in 2012) (see CCTV, 2013). A higher level of education is supposed to be one of several limited means for people – particularly those at the bottom of society– to change their fate (by, for example, acquiring a higher position in the social hierarchy). However, for a huge population, higher education now seems not to guarantee them a better future (Y. A. Li, Whalley, Zhang, & Zhao, 2011; N. Yu, 2004). For the policy makers in China, this huge population could be a potential risk and be turned into a crisis under certain circumstances.

The popularized higher education in contemporary China also has a crucial impact on the rise of popular youth culture. Firstly, more and more educated young people have been transformed into consumers and producers of popular culture. Unlike their parents’ generation, who received less education on average, the current younger generation (who have a relatively higher level of education) participate in a more cooperative yet competitive and critical relationship between elite culture and popular culture. Secondly, an increasing number of young people, having finished their education in college or universities and holding positive
and bright expectations, step into a “grand society,” and may find no positive and bright future waiting there. This disappointment not only suggests a deep reason for the prevalence of disenchanted online discourses but also helps to cultivate a resistant culture.

**The control of youth**

The control of youth (particularly tertiary students) marks the crucial part of the CCP’s social control policy, especially after the Tiananmen Incident in 1989 which showed the authorities the power of the youth. The activities of youth, and the functions of youth organizations, are important factors in the history of contemporary Chinese political movements. Early in 1919 when the May Fourth Movement broke out, and later, during the anti-Japanese war (1937-1945) and the civil war (1946-1949), young people such as tertiary students showed a massive power in both destructive and constructive dimensions. In Mao’s era (1949-1976), particularly during the period of Cultural Revolution (1966-1976), youth (titled “Red Guards”) were used by the leaders as a tool for political purposes. For a long time youth were under the control of the CCP, but in 1989 they were out of control, and eventually targets of bloody repression by military power.

The CCP has tightened its control of tertiary students since then. All tertiary freshmen are ritually required to finish compulsory military training (which normally takes two weeks) in order to make them hew to the line. The Communist Youth League has also extended its branches to almost every college and university in Mainland China.117 The structures, habits, bureaucracies, and promotion system of the ruling party are incorporated in these tertiary

---

117 The Communist Youth League, run by the CCP and organized on the party pattern, functions as an official organization for youth between the ages of 14 and 28. With the aim of using online games to make propaganda, the Communist Youth League reportedly helped fund “red” games such as “Resistance War Online” in which users can play Red Army soldiers killing Japanese invaders, and “Learning from Lei Feng” in which users can play the role of moral hero Lei Feng.
institutions. Some outstanding students who are active in this system receive rewards such as an honorable title of “Communist Youth League Cadre” and/or economic benefits such as scholarships; these rewards eventually prove to be a great advantage in the job market. A group of students are selected and recommended to the university branches of the CCP to become party members; to be a party member is a basic requirement if they want to become politicians. This does not mean that all student party members are earnest political players; in fact, some of them are not at all in earnest – they may mock party language in private situations (Nordin & Richaud, 2014) and are very pragmatic about the reasons why they have joined the CCP. An even bigger population seems to be very apolitical in the present-day China.

**Youth get online**

In the early days of the internet in China, the majority of netizens were teachers in universities and colleges, researchers and officials; the general public, similar to their Western counterparts, were basically excluded from internet development. The use of computers at that time required long-term systematic learning, and programming, typing and code-reading were all beyond many ordinary people’s ability and imagination. These factors determined that under such less developed conditions, computers and accesses to the internet were only a priority for the educated minority. The later development of internet technologies made access easier. Educational diffusion also empowered many ordinary young people to become familiar with this new technology and its relevant knowledge. Chinese universities have obtained internet access since the very beginning of Chinese internet and been interconnected in the CERNet under the auspices of the Ministry of Education (J. L. Qiu, 1999). Many students had
the opportunity to become the early netizens; from about 2003 onwards, young students have become actual participants in Chinese cyberculture. In addition to homes and offices, the dormitories of colleges and universities have surpassed internet bars and become the main surfing places of youthful netizens.

Regulations were soon introduced, particularly after 2003 when the SARS epidemic and Sun Zhigang case happened.\textsuperscript{118} During the process of these two cases, young students engaged actively via BBSs and showed their power in fighting for transparency and justice. A real-name register system has since been required for every BBS which uses the CERNet, and operators have been urged to censor more online content. In March 2005, the authorities turned down a number of university BBSs as well as some commercial BBSs.\textsuperscript{119} Other platforms, such as blogs, SNSs, and micro-blogging sites, have all been heatedly embraced by the youth (H. Huang, 2014), becoming an increasingly important field for various cultural practices (including anti-censorship practices). The online youth may have their personally favorite websites or platforms; they seldom focus on a single site or platform – using email services, surfing news websites, logging in to SNSs, and more importantly, participating in the

\textsuperscript{118} On March 2003, 27-year-old Sun Zhigang died in the medical clinic of a detention center in an area of southern China that depends on migrant labor. After finishing college, Sun went to Guangzhou (in Southern China) and became a fashion designer. One day, on his way to an internet bar, police asked for his temporary living permit and his identity card. He had not applied for the permit and he had not carried his ID card at that time. He was arrested by the police and three days later was reported to have died while in police custody. According to Custody and Repatriation, an administrative procedure established in 1982, the police in the People’s Republic of China (PRC) could detain people who did not have a residence permit or temporary living permit, and return them to the place where they could legally live or work. The incident received massive attention in newspapers and on the internet in China, and finally this policy, that discriminates against migrant workers, was ended by the Central Government in 2003. See Xiao (2004) and Hand (2006) for more information about this case.

\textsuperscript{119} The earliest case happened in September 1996 when Untitled BBS, an online forum at Peking University, was shut down after nationalist students tried to mobilize demonstrations against Japan after a right-wing Japanese group had made a provocative display at Diaoyu Islands (or Senkaku Islands), which Japan claims as its territory.
process of content production via various forms. This may increase the difficulty of monitoring and censoring their online activities.

While some young people are enthusiastic about “hard” political issues and engage actively in various socio-political activities, as shown in the Liu Di case, majority university students do not go to so far as Liu has gone, but prefer to use this technology for entertainment, such as enjoying music, movies and other popular cultural content (both domestic and abroad), forming similar-interest groups and connecting with fans, sharing pictures and chatting with friends (Clark, 2012). If some of them do like to engage in socio-political issues, as described by the phrase “fenqing” (angry youth), they are careful not to use radical means (such as, the rebellious forms taken in the Egyptian Spring in 2011). Although in the era of globalization, some Chinese netizens may easily acknowledge resistant activities in other social contexts, they consciously keep a safe distance from “hard” political issues and carefully word their criticism to remain within areas – and degrees of harshness – that are acceptable to the authorities. (See Chapter Six for more discussion about youthful resistance in less obvious guises.)

---

120 Liu Di, a then fourth-year psychology student at Beijing Normal University, was arrested by Beijing security agents from home in November 2002 on charge of “being detrimental to state security.” At first, Liu like her peers in college spent her spare time surfing online and posting her thoughts in BBSs. In 2001, Liu started her own chat room after her favorite one was closed down by police. She gradually became famous for her comments on social and political issues, under the screen name of “Stainless Steel Mouse.” And it was her politically sensitive posts that annoyed the authorities, which finally got her detained. She was not free until one year later (refer to Zheng, 2008, pp. 125-127).

121 Such as the Tunisian Revolution in 2011, which provoked a pro-democracy Jasmine Revolution in China (Jasmine, a name has meant too much for me personally); the Occupy Movement which began in 2011, the Hong Kong students’ Occupy Central movement in 2014, or broadly the Arab Spring. All of these have had some hidden influence on the Chinese people as well.
Adaptive Control

From the perspective of the authorities, some factors make the control system less effective (Zheng, 2008, pp. 68-69). On the one hand, well-designed censorship rules and regulations sometimes may not be practically enforced because of bureaucratic reasons such as the conflicts of interest between different departments within the government. On the other hand, at the same time the censorship system applies an adaptive control policy (Kalathil & Boas, 2010; Tsui, 2003), either because of economic considerations (e.g., the operation of the censorship system needs money) or political ones (e.g., too hard and rigid control may provoke fierce resistance). The internet control policies and philosophies of the Chinese authorities have undergone a shift over these years, from political control (direct, rudimentary and less wise) to social control (hidden, adaptive and more strategic) and economic control. But the more the CCP depends on social institutions which are not directly under its control, and individuals (for whom self-censorship is the main characteristic), the more spaces are provided for resistance. Resistant spaces are also provided by the political culture of the CCP. The promotion of nationwide anti-corruption campaigns has become a common method for top leaders (i.e. Hu Jintao and Xi Jiping) to establish their power in the political system. The internet has usually been incorporated into these campaigns by means of such methods as reporting the corruption of local officials via human flesh search engine or word of mouth.

---

122 See for example the conflict of interest between the then SARFT (now SAPPRT) and the then MII (now MIIT) (H. L. Hu, 2011). In fact, the SAPPRT and the MOC also conflict with each other quite often.

123 Human flesh search engine, or Renrou Sousuo in Chinese, aims to “track down offline individuals by employing as many computer users as possible in the search” and it is believed to be more reliable than “normal” search engines such as Google and Baidu (Herold, 2011a, pp. 129-130). This search mechanism, first known to the public in 2006 in Tianya (a popular Chinese BBS) has since been greatly utilized in anti-corruption movements in Chinese cyberspace.
or even strategically leaking negative stories about political opponents in online communities. This political culture provides room for internet resistance.

Combining a strong authoritarian state with limited, yet real, space for activism (Stern & Hassid, 2012), China’s authorities are well aware that high-profile coercion may not only exacerbate poor international diplomatic relations, but also boost public sympathy for protesters and radicalize participants (Sidney, 2011, p. 222). Balancing openness and control has long been a party principle (MacKinnon, 2008). On the one hand, a huge amount of the budget has been spent on maintaining stability over recent years; on the other hand, “steady pressure” and lower cost of everyday control would make sense sometimes. In fact, there are certain party members who themselves hold a sympathetic attitude to some of the activists and their activities. This has provided a gray zone for activists (as well as ordinary resisters), where politically inclined professionals in China now navigate the border between the tolerated and the forbidden. Meanwhile, many ordinary people use various forms of everyday resistance as responses to such control.

The domestic online landscape is not at all monolithic in terms of ideology and information (Taneja & Wu, 2014). Besides majority commercial websites, a list of political websites has been allowed to exist within the GFW. The virtual camps for the leftists consists of Wuyou Zhixiang (Utopia, www.wyzxsx.com, blocked in 2012 by the authorities after the Bo Xilai event\(^{124}\) and now re-hosted under a new domain name), Jinbu She (The Progress, www.jinbushe.org), and Siyue Wang (April, www.m4.cn) among others; while for the

\(^{124}\) Bo Xilai, a former member of the ruling Politburo of the CCP, was accused of corruption and abuse of power while serving in the provinces (most recently as leader of the south-western region of Chongqing) in 2013. Bo had gained a huge number of followers who can be labelled as the Left. Some commentators believe Bo’s downfall was that of a victim of the power struggles within factions of the CCP. For more details see J.M (2013).
rightists, the popular websites include *Gongshi Wang* (Consensus, www.21ccom.net), *Kaidi Shequ* (club.kdnet.net), and *Yanhuang Chunqiu* (www.yhcqw.com). Most of these websites are supported by intellectuals, and some ordinary netizens who may take part in the discussions too; some of these discussions are socio-politically sensitive and even very radical.

A proper explanation for why sensitive or even radical discussions may be tolerated by the authorities is that the state tries to selectively foster some free domains where people can vent frustrations (and have fun at the same time), and where it can observe public opinions and adjust relevant policies (Hassid, 2012; MacKinnon, 2011a; Zheng, 2008). Since the early days of internet development, the Chinese Government has strategically used online mechanisms for citizen feedback, complaints and suggestions, etc. as part of a strategy to bolster regime legitimacy (Kluver, 2005a). Popular online communities (such as BBSs, chat rooms and blogs) also serve as a “safety valve” by allowing enough room for a sufficiently wide range of subjects that people can let off steam about government corruption or incompetence, thus giving people more options for airing their frustrations before considering taking their gripes to the streets (MacKinnon, 2008). Further evidence shows that the authorities may tolerate criticism of the CCP and government but not those that could provoke collective protest (King, et al., 2013). This control strategy echoes Gramsci’s (1971) notion of hegemony whereby control is sought not through total domination but by allowing very limited opposition.

The reason why resistance by the majority group of commercial internet companies – arising from their endeavors to ensure the market prevails over the political – has not received

---

125 A similar case existed in the Soviet Union (1922-1991). *Krokodil* (Crocodile), a popular magazine which was famous for its humorous and satirical cartoons about the political and ideological issues, was used to entertain the people as well as a social control strategy.
harsh punishment could also be explained in a similar way. The authorities may well know that ISPs and ICPs are reluctant to follow the instructions of closedown during sensitive dates. Resistance such as using “technical tricks” to keep a BBS open to ordinary users while appearing closed when the cyber police supervise it (J. L. Qiu, 1999) causes no fundamental risk for the regime, and thus is nothing more than a public secret shared by both the authorities and internet companies.\footnote{\textsuperscript{126}}

Further evidence shows the Chinese authorities’ engagement with the internet and attempts to establish diverse yet controlled channels of public discourse. Many official background accounts have become active on SNS to manipulate public opinion. Posts of these accounts are sometimes very radical and “cross over the line.” For example, the chief editor of the \textit{Global Times} (with a reported circulation of 2.4 million per issue in 2013) registered on Sina Weibo in February 2011 under his real name “Hu Xijin” and a profile description reading “a reporter of complex China,” and has since been active in commenting on various socio-political issues. Although most of his posts are met with fierce criticism (full of dirty words and personal attacks), he chooses to ignore the verbal abuse and keep on sharing his ideas. Hu, among many other people with online accounts who have official backgrounds, is well aware that “The comments of my Weibo have already been a virtual platform for releasing all kinds of anger” and “Normalizing criticism is helpful for the state to maintain its stability.”\footnote{\textsuperscript{127}} The existence

\footnote{\textsuperscript{126} The resistance of the local censors or commercial internet companies themselves may make for a fascinating inquiry that could fill volumes. While I have described some aspects of their resistance as it relates to local bureaucratized behavior and public offence from the bottom, it takes many other forms that contribute to their domination of both local institutions and the local opinion agenda setting. Whatever place resistance in this larger sense might justifiably occupy, in a full account of power relations in this cyberspace, it is marginal to my main objective in this thesis.}

\footnote{\textsuperscript{127} Translation my own. For the original posts, refer to Hu’s Sina Weibo posts (X. Hu, 2012a, 2012b). More cases like Hu’s will be analyzed in Chapter Four.}
of such online spaces helps to lower, at least partially, the possibility that people go out into the streets.

The creation of “legally regulated channels” (Ding, 2002) through which some ordinary netizens can routinely express their political (and non-political) demands for social and economic justice, thus characterizes it as an adaptive control strategy. This is not to argue that adaptive control of the internet has been designed as such from the very beginning. As a large and complex society, China has various differences both horizontally and vertically, which makes it hard to govern (E. J. Perry & Goldman, 2009, p. 1). Hegemonic systems of control are filtered through dominant cultural practices (Gramsci, 1971, p. 12). Through the long and dynamic practice between the governor and the governed, for the governors, the only practical way to control this society is to occasionally leave some room for the uncontrolled. It is, at least partially, this minor freedom within a broadly controlled society that provides spaces for internet resistance.

Of course, there are many other cultural, socio-political circumstances that could be listed here; this chapter has focused mainly on the above five conditions. Other relevant conditions will be touched on in case analyses in the coming chapters. However, in general, it is possible to say that these five conditions have formed the background of internet resistance, and have produced a vastly different situation from that of the cultural space previously inhabited by ordinary Chinese people. Also, the generalization of these conditions is only for the convenience of analysis in the coming chapters, and I bear in mind that a real case of resistance may involve more than one of these conditions. Not only have these conditions
profoundly altered the relationship of ordinary Chinese people to the elite and to the state, but the homogeneity of ordinary Chinese people as an ideological group no longer exists. In the new era of the internet, Chinese netizens have responded to these transformations in various ways: one significant response is internet resistance.
CHAPTER III. TECHNOLOGICAL RESISTANCE AND TECHNOLOGICAL WEAPONS

While there is abundant research that approaches this topic from a top-down perspective, and focuses on how many Chinese netizens’ online behaviors are passively affected by internet censorship, the topic of how netizens actively manage to bypass restriction in their everyday online experience has been insufficiently covered (Q. Yang & Liu, 2014). In fact, some Chinese netizens, far from being passive self-censors, have long been trying to find ways to get around the censorship machine. While the next two chapters investigate symbolic resistance to internet censorship, this chapter concentrates on how some Chinese netizens use internet technologies to circumvent internet censorship. It firstly discusses the netizens’ creative uses of existing platforms for anti-censorship purposes, and then investigates hacking as resistance. The third theme is the first generation of censorship circumvention technologies that are programmed by Chinese dissidents (particularly Falun Gong). After a case study of the second generation of anti-GFW hacking, Xixiang Jihua (the West-Chamber Project [WCP]), and a detailed investigation into new circumvention tools, this chapter concludes by suggesting that technological resistance in Chinese cyberspace has become much more scattered, small-scale, low-profile, and quotidian, and that its political influence should not be overstated.

Guerrilla Warfare on Existing Platforms

Internet companies play some crucial roles in anti-censorship activities. In China, all ISPs and ICPs need to comply with censorship requirements from the authorities; but, as discussed
in Chapter One, with consideration of commercial interests, internet companies have to meet
 demands from their users as well. Given the possibility of gaining good publicity from
some sensitive materials circulating on their platforms, it is common for internet companies to
strategically wait for a few minutes before deleting them (Epstein, 2013). This slight time-lag
does provide users some room for free speech. Complying with the authorities in an overt and
overall sense while at the same time performing a tiny and nuanced resistance against them
seem to have become a hidden culture in Chinese cyberspace (J. L. Qiu, 1999) and, more
broadly, in media space.

Some Chinese netizens (dissidents in particular), accordingly, seem to have creatively
made the most of this culture and used existing platforms and services for anti-censorship
purposes. For example, mobile phones and Short Message Services (SMS) have long been
used for anti-censorship purposes. This was the case in 2003, when the authorities tried hard to
keep back news about the SARS epidemic: curious yet worried people shared “stories” they
heard about or happened to know via SMS (Tai & Sun, 2007) – this phenomenon has been
termed “the power of the thumb” (H. Yu, 2004). Another case is the Xinjiang riot in 2009:
when the Chinese authorities shut down the public internet service in the whole autonomous
region for over one year, mobile phones and SMS become an important way for citizens to
circulate relevant information. Mobile phones and SMS function well in massive events, such

128 Research also finds that compared with long established internet companies, newly rising private
entrepreneurs have more chance, and intention, to “articulate their voices over and above government
policies” (Zheng, 2008, p. 35).

129 The role of internet companies in resistance to censorship should not be overestimated, since they also
apply technical tricks to cheat their users as well. For example, Sina Weibo is widely believed to use technical
tricks to keep sensitive posts visible only to the users themselves (not to their followers or the general public).
By this means Sina Weibo not only meets the requirements from higher level censors but also expects not to
irritate its users. Internet providers may not be able to challenge the censorship system fundamentally, but
being connected together, they are politically significant in some cases, and provide users spaces to speak out
their minds, or even to practice resistance to censorship.
as during anti-PX events in many metropolises, where protesters use mobile phones to share information, and organizers use them to announce the time and place of collective “sanbu” (leisure walk, a euphemism for expressing demonstration).

This of course does not mean that the authorities cannot do as much to SMS; technically speaking, they can find out which messages have been circulated between whom, if they want to do so. However, local authorities can hardly access users’ data, since they have no direct right to give such orders to the mobile networking service providers – which is quite different from the authorities at the central level who can easily get mobile networking service providers to comply with them. This is the reason why mobile networking plays a more important role for local-level resistance. After the popularity of communication apps (e.g., WeChat) among Chinese cell phone users, cell phone networking has played an even more significant role in shaping Chinese cyberspace. A good recent case is the Hong Kong protest in 2014. When the authorities tightened control of the cell phone information communication between pro-democracy protesters – a majority of whom were students – by shutting off the WiFi network and cell signals, the protesters strategically used the FireChat app, which enabled them to connect via Bluetooth.

Email services have also been used to share sensitive information in the early days of internet development. This was technically easy to do, since the GFW at that time was still concentrating on filtering websites and web pages and had not yet updated its technologies to monitor emails. Many overseas Chinese dissidents such as pro-democracy exiles and members of Falun Gong used a spam-like means of “massive, unsolicited emailing” to send sensitive
materials to the Mainland Chinese.\textsuperscript{130} In order to avoid being monitored and filtered by the
censorship system, the senders of these emails strategically changed their email addresses and
the times at which they sent these emails so that there was no predictable pattern (Collings,
2001, p. 189). However, since the technology of deep packet inspection (DPI) has become
available for the authorities, using encrypted email to communicate sensitive material now
also carries the risk of being caught. Along with email services, remailers, and mirror sites,
secret Usenet groups also enabled some Chinese netizens to breach censorship mechanisms in
the early days (Lacharite, 2002).

At around the start of the new millennium, blogs became an important tool for dissidents,
allowing information to be easily updated and re-blogged (Esarey & Xiao, 2008). After the
authorities’ tightening control over the domestic blogosphere, many users have turned to
international servers to host their personal blogs and to avoid censorship – though this means a
relatively slower speed, and a higher cost of expenditure, and requires that readers who are
located within the GFW use circumvention tools.\textsuperscript{131} Such stories of guerrilla warfare have
become an attractive theme of everyday narrative for some netizens; by sharing their personal
stories of struggling with the GFW, they also invite others to do it in the same way.

\textsuperscript{130} \textit{Dacankao (VIP Reference)}, an underground electronic newsletter compiled in Washington by Chinese
advocates of democracy and free speech, started in 1997 using an email system to send out sensitive
information to hundreds of thousands of Mainland Chinese. Its editor, Li Hongkuan, treated the GFW as no
great impediment since he can “just go over it.” A number of close to one million emails was claimed to have
been sent each day to recipients in China by the end of 1999 (Collings, 2001, p. 189). \textit{Suidao (Tunnel)}, another
dissident newsletter which began on 4 June 1997, also used a similar technique of massive, unsolicited emailing
to disseminate uncensored information to Mainlanders.

\textsuperscript{131} For example, a Chinese netizen named Yao Youwei mentions that he built his personal website early in
2000 when free access to foreign websites was still available. It changed after the GFW became active, which
pushed him to use circumvention tools to look for censorship-free information. However, one day in 2007, his
personal website was hacked because it had sensitive words. Since then he had changed virtual hosts four
times, and finally turned to an international server. His story represents a good population who started using
the internet from the very beginning (refer to Yao, 2012). Another case happened to \textit{Niubo Wang} (Bullog.cn), a
liberal blog created by an English teacher; after encountering blockage in Mainland China, it changed its server
to an international one in April 2009 (see R. Deibert, et al., 2010).
SNSs may also be involved in internet resistance. For example, Twitter functions as a virtual enclave for some Chinese, particularly those who are located outside the GFW or whose expression is often censored within the GFW. There is no precise number of Chinese Twitter users so far. Although some scholars (e.g., Zuckerman, 2010) suggest a population of 1.5 million, active Chinese Twitter users may be as low as 18,000 (Zhai, 2013). Most Chinese users in the Twitter community follow (and are followed by) other Chinese users; they tweet and retweet in Chinese, and discuss issues about China (particularly those being censored within the GFW). The popularity of Twitter among Chinese dissidents and activists might be risky for the users, since the Chinese authorities – if they wish – can easily identify the network of contacts between these dissidents and activists. However, for Chinese Twitter users, according to Sullivan (2012), choosing Twitter itself is often a “conscious and explicitly political act” and this small number of Chinese users is generally “progressive, critical and activist” (p.774). Foreign SNSs such as Twitter and Facebook, as discussed in the coming sections of this chapter, do provide convenient tools for dissidents and activists to become connected.

Furthermore, search engines may also be utilized to bypass censorship. Though Google (when it was still available in China) and Baidu have been subject to tight control of the results shown to their users, this does not mean that no sensitive materials could be accessed. Both search engines have a cache function which provides users with a cached version of a page instead of its current live version. Mainly for reasons of censorship, many pages on Chinese websites have been removed and are unavailable for viewing, so the function of cached pages
works as a relatively simple (though not very effective) means for some Chinese netizens to find banned content.

It needs to be noted that what has been defined as sensitive per se is a continually changing concept. In the early days, ordinary users might not realize that their activities were politically sensitive; only after the official laws and regulations have defined what is sensitive and what is not, the resistant dimension of netizens’ activities have gradually become clear. In other words, resistance in the early days of the internet was more likely to be an unconscious activity; while in recent times, it has become a more conscious one, with hacking (particularly the creating of circumvention tools) as good evidence of such consciousness.

**Dimensions of Hacking Resistance**

Hacking has a longer history as a resistant power in the Western context than it does in China. When it comes to Western hackers, scholars often mention some general terms such as freedom, F/OSS, liberalism, anarchism, or civil disobedience (Coleman, 2011, 2013a; Fuchs, 2013; Taylor, 2005). Hackers use hacking activities to express themselves. Sometimes code itself is speech (Coleman, 2013a) while in other situations, hackers may also make use of street protests and direct offline activities (Jordan, 2001). Whether hacking activities really erode political power or not is still arguable, as suggested by terms such as clicktivism (White, 2010) or slacktivism (Christensen, 2011; Morozov, 2009), and facts such as that hackers may cooperate with the authorities as well (Norton, 2012). Furthermore, hackers are far from a monolithic group – they are diverse both in thoughts and in actions (Goode, 2015a).\(^{132}\)

---

\(^{132}\) Take the currently most crucial hacktivist group, Anonymous, as an example. It is not a shadowy organization but a loosely knit collection of activists all over the globe, fighting for government and corporate transparency (2014).
Although no public resource is currently available to identify how often, and on what scale, hacktivists participate in resistant activities in Chinese cyberspace, there is evidence that hacking is one form of technological resistance here (or in Coleman’s sense, “the weapon of the geek”). Functioning as one of the main types of networked resistance in China, hacking resistance can be understood in terms of three dimensions.

A foreign dimension

Various circumvention tools created by foreign programmers circulate in Chinese cyberspace, such as Anonymizer, Tor (which has been blocked by the GFW), Circumventor, I2P (reportedly safer than Tor from the perspective of the GFW), Coral, Hamachi, Psiphon (Canadian-based, released in 2006), Relakks, JAP, GhostSurf, and Hotspot Shield. Most these tools are open-source, and thus are freely provided for internet users behind national firewalls; some of them, such as GhostSurf, are only commercially available. The developers of Psiphon, besides releasing free tools, have also created a for-profit company that offers media companies (including VOA and RFA) an opportunity to deliver digital content and advertising to internet users in repressive environments. Despite the fact that many of them are not intentionally targeted at Chinese netizens, these tools compete with those released by Chinese dissident developers (as shown later in the case of Tor and UltraReach) and have gained some popularity in Mainland China. In particular, they are much more popular among groups of foreigners in China. The daily operation of foreign companies in Mainland China depends on such circumvention tools (including commercial VPN services) which are cheap and technically easy to use.

133 From Coleman’s perspective, hacking is “the weapon of the geek” (a utilization of James Scott’s concept of “weapons of the weak”) and hackers “don’t necessarily have class-consciousness, though some certainly do, but they all tend to have craft consciousness” (Coleman, 2013b).
Foreign organizations such as Citizen Lab of the University of Toronto and Paris-based RSF have long focused on issues surrounding the GFW and information freedom in China. Citizen Lab is itself responsible for the anti-censorship tool Psiphon. With some research interests in the GFW, this lab has cast its influence on some Chinese hackers (Lemon & Gohring, 2006). RSF may not be directly involved in developing any circumvention tool, but it continues to publish reports on China’s internet censorship, an activity which gains both academic and public attention. These two groups have produced how-to guides for Chinese netizens to get around the GFW as well. Besides these two groups, there are other organizations involved in challenging the GFW, such as GitHub, a U.S.-based private company that provides online code repository hosting service. F/OSS projects can be freely hosted here, which helps some Chinese hackers to program anti-GFW software. It thus seems unsurprising that GitHub was blocked by the GFW in 2013 and underwent a DDoS (distributed denial of service) attack in early 2015 which reportedly originated from China (Perez, 2015).

Foreign hackers have also become involved in Chinese censorship and other political issues. An example is the recent case of the 2014 Hong Kong protest, in which the international hacktivist group Anonymous declared its support for pro-democracy students and started a cyber war against the Chinese authorities. Hundreds of phone numbers, names, IP addresses and email addresses from Chinese government websites have since been leaked online and some government websites have been shut down by these hackers (Cuthbertson, 2014). Such support from foreign hackers does make its political presence felt in China, and shows the power of technological resistance to the Chinese authorities. Anonymous China, a
branch of Anonymous, has formed a virtual community on Facebook (www.facebook.com/anon.china1), where it has not only archived its hacking activities in China, but also included much wider political issues such as environmental protection, human rights, and the Tiananmen Incident.

The control of domestic hackers

Hackers within the GFW have long existed and they have been known to the general public because of several famous hacking events: the attack on Indonesian websites after Indonesia’s anti-Chinese agitation in 1998, the hacking war on U.S. websites after NATO’s bombing of the Chinese Embassy in Yugoslavia in 1999, the incursion into Japanese websites after the Japanese right wing’s anti-Chinese gathering in 2000, and the cyber war between Chinese and American hackers in 2001 after an American spy airplane trespassed in Chinese national airspace and collided with a Chinese airplane (see Ximu Chen, 2001, pp. 1-52; S. Shen, 2007, p. 175). After the 1999 hacking event, China Youth Daily, a Beijing-based national newspaper, coined the name “Hongke” (“red guest” or “Honker” which is equivalent to the English idiom “white hat”) – to refer to this group of patriotic hackers. Patriotic hackers were technically accepted by the Chinese authorities because most of their activities were claimed to defend the interests of China and thus to match the authorities’ attitudes of “online nationalism.”

The convergence of Chinese hackers and online nationalism differentiates hacker culture in China from that in Western contexts (Coleman, 2013a, p. 19; Henderson, 2007, pp. 69-78). According to Henderson, patriotic hackers are represented by the Red Honker Alliance, and others such as New Hacker Alliance (with site server based in Shanghai), Student Hacker
Union (based in Beijing), Yaqu163 (based originally in Beijing and then shifted to Wuhan), and Hx99 (based in Sichuan). Those Falun Gong, Free Tibet movement, Hong Kong activists, and foreign hackers who are responsible for attacks threatening China’s national sovereignty and challenging the legitimacy of the ruling party have received return attacks from the alleged patriotic Chinese hackers (Henderson, 2007, p. 109). Patriotic hackers reportedly invade various targets from governments to commercial companies, defense contractors, newspapers, think tanks, NGOs, Chinese human rights groups, and dissidents, but it is impossible to confirm these reports (Beech, 2013; Hvistendahl, 2010; Walker, 2011).

Unlike most of their Western counterparts, for whom anonymity is the top priority of their hacking activities, patriotic Chinese hackers are sometimes proud of being known to the general public. Wan Tao, one of China’s first patriotic hackers, who joined China’s first hacking group Green Army in 1997, was engaged in two famous hacking events; one involved crashing the email box of the Japanese Prime Minister’s website, and the other was a cyber-war with American hackers in 2001 (Hughes & Wacker, 2003, p. 145). Wan reportedly designed a software system in 1999 to help the police to find out who had written anonymous subversive posts on BBSs (Epstein, 2013). Many hackers like Wan strategically choose to follow the line set by the government and become “Honkers,” meaning that their hacking activities often are not penalized when caught.

Though these hackers may not threaten the censorship system after being incorporated by the authorities, they did function as a challenging dimension before that. Since hackers (including the patriotic Honkers who have been ideologically renamed) are fundamentally technological cowboys who believe in some kind of anarchism, and have the potential to act as
dissenters and thus work against the authorities, the Chinese authorities have never publicly accepted this group of netizens. According to Chinese law, hacking is definitely a criminal offence, and has been since 1997. The first publicized hacking trial happened in 1998 and resulted in the execution of one of two men for hacking and stealing from a state-owned bank in Jiangsu province. On 19 May 2009, several “script kiddies” launched a DDoS attack against a free video player, Thunderstorm, disabling the Domain Name Resolution services in over 20 provinces and rendering at least 100 thousand websites inaccessible. This group of hackers were soon arrested and thrown into prison. International commercial hacking activities have happened occasionally, such as the involvement of a group of Mainland Chinese hackers in a scheme to steal money from Taiwanese bank accounts in 2004, and the hijacking of German and American eBay user accounts in 2005 (see Henderson, 2007, pp. 86-87; Y. Ye, 2014). Cases like these have shaped the Chinese authorities’ attitudes to hacker culture – although they have tried covertly to utilize some talented hackers for political purposes, they have never publicly legitimized this culture. It should also be noted that the Chinese authorities have never completely controlled domestic hackers (see the last section of this chapter for more discussion).

**Dissident hackers and their resistance**

Although the Chinese hackers discussed so far place less emphasis on free access to information, freedom of speech, F/OSS or “code as speech” than their Western counterparts, they undoubtedly share the spirit of resistance which has cast a hidden, yet wide, influence on Chinese cybertulture. Precisely speaking, when it comes to dissident hackers, hacker culture may fundamentally show a spirit of resistance. Take the anti-CCP hacker organization
“Fangong Heike” for example.¹³⁴ On 2 June 2014, two days before the politically sensitive anniversary of the Tiananmen Incident, the website of the Information Center for Social Sciences of Renmin University of China was hacked by this organization and the slogan “Chanchu gongfei, zhaoxue liusi” (Wipe out the CCP, rehabilitate June 4) was added to its homepage. This organization targeted not only websites of official institutions such as local governments and universities, but also those of cable TV stations, each time adding anti-CCP campaign messages to their broadcasts. A recent case in which this hacker group may have been involved happened on 1 August 2014, during the evening news time: Wenzhou cable TV was infiltrated and their viewers found anti-CCP messages on their screens.

Hacking as resistance can also be seen in the activities of quasi-religious organization Falun Gong. After being denounced as “cult group” and repressed by the Chinese authorities in July 1999, Falun Gong has since been very active in spreading anti-CCP propaganda. During prime time on 5 March 2002, the eighth-channel Changchun municipal cable television network in Northeast China was hacked by practitioners of Falun Gong; for nearly one hour, Falun Gong propaganda replaced state propaganda on the television screens and two videos were broadcast into more than 300,000 households (Y. Zhao, 2003, p. 209). The targets of Falun Gong’s hacking activities vary, from China’s cable television networks in various cities, to the Sinosat state satellite and disrupted television channels at both national and provincial levels (see People's Daily Online, 2002).

After the GFW tightened its control on the Chinese internet, and information originating from Falun Gong became difficult to reach for Mainland Chinese, Falun Gong started various

¹³⁴ Fangong Heike is physically located outside Mainland China. It not only hosts a website (www.fangongheike.com) and archives its hacking activities in Mainland China on it, but also forms virtual communities on social networking sites such as Twitter (twitter.com/fangongheike).
small internet companies to promote circumvention tools (a theme that will be discussed fully in the coming section) to help some Chinese netizens to access uncensored information.

Various detailed “technical references” are provided on their websites to aid practitioners (or the general public) to breach the Chinese censorship system (Ownby, 2008, pp. 201, 205-206).

Some Falun Gong members possess considerable computer skills, and they have been active in hijacking government websites. They have sometimes also directly involved in challenging the censorship activities of Chinese authorities. For example, in the case of Green Dam Youth Escort mentioned in Chapter One, the programmers of Freegate developed software called Green Tsunami to neutralize the influence of that censorship software. As a vigorous resister to the Chinese regime, Falun Gong never hesitates to show its hostility to the CCP.\(^{135}\) Almost all Mainland cable television programs and/or websites hacked by Falun Gong have been left with hostile messages against the CCP. Similar things happen with its anti-censorship software; in the introduction pages of Ultrasurf (see the coming section for more discussion), it claims that “The tool was originally designed for internet users in Mainland China.”

Moreover, Falun Gong organization has close relationship with some Western media (such as VOA and RFA) which are blocked by the GFW; it also has received U.S. funds for hacking activities (see the coming section for more discussion). These facts have undoubtedly invited the Chinese authorities to place an even stricter control policy over the internet in the name of causes such as internet security or sovereignty – the CCP has been very politically sensitive towards interference in China’s domestic affairs from big powers such as the U.S.

\(^{135}\) Falun Gong has claimed to be resistant to Chinese censorship, but it is ironic that in the first place, when this group received criticism from its opponents, it “urged the Chinese government to use its powers of censorship to muzzle the opponents” (Y. Zhao, 2003, p. 215).
Hacking makes technological resistance in Chinese cyberspace a complicated phenomenon. As discussed in this section, as well as the coming section, technological resistance seems not to have been limited to internet censorship per se; it sometimes originates from a broader socio-political background, particularly in the Falun Gong case.

**Organized Hacking: Circumvention 1.0**

**A brief history of the first generation anti-GFW tools**

Based on the open-source Freenet project, some overseas Chinese hackers started a Freenet China project in 2001, which proved ineffective, because pro-government programmers joined this network as well. Afterwards, one of the project’s creators, Bill Xia, started another project, DynaWeb, under the company name of Dynamic Internet Technology (DIT). DIT was founded in 2001 (with Xia as its president) and was aimed at providing solutions for internet service needs in repressive environments. Emphasizing its early relationship with the U.S. Government on its “About” page, and clients which include the *Epoch Times* (a globally published newspaper of the Falun Gong organization), VOA, RFA and Human Rights in China (HRIC), DIT obviously stands against the Chinese Government. There is no straightforward information about its financial status. But since two of its three products, Freegate and DynaWeb – both are proxy services, are freely provided for users (the third product is a mass mailing service), there is a strong suspicion that it survives mainly on support from its clients. According to the website of Global Internet Freedom Consortium (GIFC), DynaWeb reportedly supports more than 50 million web hits per day on average from Chinese users alone, and Freegate is still active in cyberspace and has gained users in China.
and beyond. Although the GIFC tries to emphasize these successes on its website, signs show that its products (targeted at Chinese netizens) might have decreased in influence.

Table 1. The First Generation Circumvention Tools Used in Mainland China

<table>
<thead>
<tr>
<th>Tool</th>
<th>Active</th>
<th>Company</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>TriangleBoy</td>
<td>2000-2001</td>
<td>SafeWeb</td>
<td>HTTP proxy</td>
</tr>
<tr>
<td>Freenet China</td>
<td>2001-2002</td>
<td>DIT</td>
<td>HTTP proxy</td>
</tr>
<tr>
<td>Garden</td>
<td>2001-2007</td>
<td>Garden Networks</td>
<td>HTTP proxy</td>
</tr>
<tr>
<td>DynaWeb</td>
<td>2002-2006</td>
<td>DIT</td>
<td>HTTP proxy</td>
</tr>
<tr>
<td>Garden G2</td>
<td>2002-2007</td>
<td>Garden Networks</td>
<td>DNS resolution</td>
</tr>
<tr>
<td>UltraSurf</td>
<td>2002-2007</td>
<td>UltraReach</td>
<td>HTTP proxy</td>
</tr>
<tr>
<td>Freegate</td>
<td>c.a. 2004-</td>
<td>DIT</td>
<td>Proxy</td>
</tr>
<tr>
<td>Firephoenix</td>
<td>2006-</td>
<td>UltraReach/WG</td>
<td>VPN</td>
</tr>
<tr>
<td>GPass</td>
<td>2006-2009</td>
<td>DIT/WG</td>
<td>VPN</td>
</tr>
<tr>
<td>Gtunnel</td>
<td>2007-</td>
<td>Garden Networks</td>
<td>VPN</td>
</tr>
</tbody>
</table>

SOURCE: Various sources on websites of these tools, news coverage and beyond.

In 2001 a Canadian-based organization, Garden Network for Freedom of Information was launched, and has since released three tools – Garden, G2 and Gtunnel. After 2007, Gtunnel replaced the previous two tools and has since functioned as the organization’s only product. According to its own words, hundreds of thousands of Chinese people are using Garden Networks tools daily; but again it is hard to confirm the number of its users. This organization is self-defined as not-for-profit, and donation is its main financial source (with a “You can help” donation link on its website http://gardennetworks.org/). Garden, together with two other

---

136 Information comes from the introduction of these products on the website of GIFC. GIFC has a close relationship with some U.S. officials, with help from whom it receives funds from the U.S. government (see MacKinnon, 2012, pp. 188-191). From a technological perspective, Freegate has a significant update which can enable those who share sensitive information through emails by simply attaching it in the email and the email will be encrypted automatically; once the email is successfully sent out, the user just needs to click a button and the trace of usage will be cleaned immediately.

137 For instance, its latest success in mass mailing, which was selectively shown on its website, happened in 2005 (ten years ago)! DIT expressed pride because its mass mailing project was mentioned in a testimony for U.S.-China Economic and Security Review Commission on April 14, 2005 – “We send millions of emails a day, and the response has been overwhelmingly positive to the VOA and RFA language services - news summaries and information on local Chinese and international news.” (DIT, n.d.) DynaWeb has encountered a similar fate: although it was not officially denounced, the fact that its latest updated was done on 15 April 2005 shows that the report that DynaWeb was blocked by Chinese authorities in May 2006 should be somewhat convincing.
tools, DynaWeb and Ultrareach, both of which were launched in 2002, became the main tools in the early days for Chinese users, and gained the title of “The Three Musketeers” in the cyber underground.

Triangle Boy emerged even earlier than these three tools. It was developed by SafeWeb, a U.S.-based software company which was acquired by Symantec on 15 October 2003 and later stopped support for this tool. This company reportedly not only had a financial relationship with International Broadcasting Bureau (IBB, the parent company of VOA) but was also sponsored by a CIA project to provide anti-censorship software for Chinese netizens (Hughes & Wacker, 2003, pp. 72, 154). However, by the end of 2002, the Triangle Boy project was completely blocked in Mainland China. UltraSurf was launched in 2002 by UltraReach Internet Corporation, a Falun Gong internet company (Ng, 2013, p. 40). It enabled users to circumvent internet censorship and firewalls by using a HTTP proxy server, and also employed encryption protocols for privacy, such as the provision of digital certificates for their products to protect their customers from being cheated by fictitious products.

These tools use two main technologies – proxy servers and VPNs. Proxy servers such as Freegate and Ultrasurf can conceal the physical addresses of users and create anonymity for them. Common types of proxy servers include HTTP proxy, CGI proxy, POP3, FTP, and SOCKS, among others. Alternatively, a VPN can create a private and encrypted channel for the user to communicate with internet servers outside the GFW, and it is “faster, fancier and more elegant” (J. Fallows, 2008) than a proxy server. A slight technological shift exists in the first generation circumvention tools, from proxy servers to VPN (see Table 1). This shift is actually a technological response to the update of the GFW.
The political dimension

Chinese hackers with Falun Gong backgrounds have been very active in programming anti-GFW tools. SafeWeb might not have a direct relationship with Falun Gong; however, the other four organizations, especially DIT, UltraReach Internet Corporation, and World’s Gate, may share some common interests (e.g., as parts of Falun Gong) and have a vague relationship with one another. In fact, the companies of Global Information Freedom (GIF), DIT, UltraReach Internet and Garden Networks for Freedom of Information formed a loose alliance in 2006 as the Global Internet Freedom Consortium (GIFC) (GIFC, n.d.). An interesting contradiction on the GIFC website may be good evidence for these companies’ relation with Falun Gong. In a report (GIF, 2007) which announced that it had overcome a temporary setback of increased GFW censorship, GIFC defined the software of FirePhenix and GPass as World’s Gate products; while on its webpage “Our Solutions,” GPass was on the product list of DIT and FirePhoenix of UltraReach Internet Corporation. Although on the websites of these small companies there is no information to publicly confirm that, it invites a reasonable inference that DIT, UltraReach Internet Corporation and World’s Gate either have overlapped personnel or belong to the same parent. This suggestion has been supported by other news coverage (Pomfret, 2010), including the assertion that Bill Xia himself is the president of DIT and at the same time a follower of Falun Gong.

It is interesting that most of these small internet companies aimed at creating a freer Chinese internet are physically based in North America (particularly on the West Coast of the U.S., where a huge number of local hackers gather as well). Hacker culture there is relatively more mature and the idea of a free internet has been widely acknowledged there for a long
time. For the overseas Chinese dissenters (be they religious or political), such a technology-friendly environment provides plenty of moral and technological resources for their development of anti-censorship software. This, however, does not mean that these dissident Chinese hackers have positive interactions with local Western hackers; conversely and interestingly, they seldom interact with each other at the technical level.\textsuperscript{138} The only such interaction publicly available so far has happened in 2012, between Tor and UltraSurf, and it was not a positive interaction but an embarrassing quarrel (see Appelbaum, 2012; Ultrareach Internet Corporation, 2012). Tor checked nine claims by UltraReach and its advocates and found that nine were all “false, incorrect or misleading.” It further pointed out that “it is possible to monitor and block the use of Ultrasurf using commercial off-the-shelf software” and recommended against the use of this tool since “the vulnerabilities presented in this paper are not merely theoretical in nature; they may present life-threatening danger in hostile situations.” UltraReach responded promptly, but insisted that the UltraReach tool was designed according to a different philosophy from that of Tor, and that Tor’s “unsubstantiated attacks” were primarily an attempt to lobby against funding for the UltraReach project.

The quarrel between UltraReach and Tor reveals differing stances between Chinese dissident hackers and their Western counterparts. First, unlike their Western counterparts, Chinese dissident hackers emphasize more on closed-source software rather than F/OSS. Most of the above tools are closed-source, partially due to the tense, fraught relationship between circumvention tools and the GFW. These small companies claim that if these tools were open-source, China could easily update its censorship mechanics accordingly. The price is that these

\textsuperscript{138} Some dissident Chinese hackers such Bill Xia may talk about the GFW and internet censorship in China via media outlets, or publish relevant academic articles. But publicly available data shows that they seldom interact with local Western hackers at the technical level.
tools often receive critiques (as criticized by Tor in UltraReach’s case) about issues relevant to safety, privacy, security and anonymity; for example, the users may risk being monitored further: maybe not by the Chinese authorities, but by the creators of these tools.\footnote{According to the Spy Files leaked by WikiLeaks, 32 companies (including UltraReach Internet Corporation) of the U.S. have been involved (WikiLeaks, n.d.). This invited a wide skepticism among Chinese users that using the tools created by this company could reportedly create the risk of being monitored.} Second, though Western hackers are a pretty diverse bunch, they fundamentally have a “technical orientation” (Coleman, 2011). However, Chinese dissident hackers seem to have utilized hacking activities and circumvention tools purposely as part of their larger religious and/or political agenda. Third, dissident Chinese hackers are bedeviled by ideological contradictions. Although they are against the Chinese authorities, they at the same time try hard to get funds from the U.S. Government and other organizations (Pomfret, 2010).\footnote{To fund U.S. efforts in support of Internet freedom, Congress in the 2008 financial year appropriated $15 million, most of which has been spent or is obligated. Another $5 million was appropriated in the 2009 financial year. Finally, Secretary Clinton’s January 21 speech mentioned an additional $15 million for the 2010 financial year. The U.S. Broadcasting Board of Governors’ IBB also supports counter-censorship technologies and has committed approximately $2 million per year to help enable internet users in repressive regimes to have access to the VOA and other U.S. governmental and non-governmental websites and to receive VOA email newsletters (Figliola, Nakamura, Addis, & Lum, 2010). An ironic fact is that some American technology companies such as Cisco, at the same time, have been busy selling censorship technologies and products to the Chinese authorities (Burkart, 2014; Nobori & Shinjo, 2014).} Since the GFW started to censor widely in about 2001, various news organizations such as VOA and RFA that at least partially targeted Asian countries (China in particular), became unavailable in Mainland China. This is the background to the fact that VOA and RFA have since been very active in funding Chinese dissident programmers to develop anti-GFW tools.

From this point of view, the first generation circumvention tools are products of a much more organized and centralized movement, and they serve – from a technological perspective – a much larger religious and/or political purpose.
The influence of these tools

These tools are targeted at Mainland Chinese users, but some, such as Freegate, also attract users beyond China and have become popular in other authoritarian states such as Iran and Syria. In 2006, about 100 thousand Chinese netizens were estimated to use circumvention tools such as Freegate, UltraReach and Garden Networks to surf online daily, an estimation made by the creator of Freegate (Bill Xia) yet impossible to confirm (Fowler, 2006). Ultrasurf had reportedly gained a population of 80,000 users in Iran, China and Vietnam by the end of April 2011 and in some extreme cases, such as during periods of social unrest in Tunisia and Egypt, the programmers of these tools needed to limit the sharply increased access from these areas to avoid overloading the system (Applebaum, 2011).

However, developers have seldom mentioned the exact number of users of their circumvention products. If they have spoken publicly about this, they have been inclined to either use indirect metaphors or to make announcements in a very vague way. The exaggeration of their products’ challenge to the GFW might be explained as a marketing strategy for funding purposes. The majority of Chinese netizens seem to have little interest (if any) in bypassing the GFW, not only because of the financial and political risk of being caught, but also because most of the time, there seems to be no need to do so – entertainment

141 Such as at the end of Bill Xia’s essay about China’s internet censorship (2008), which implies with the metaphor of “cat and mouse” that “2008 is the year of the Rat in the Chinese lunar calendar, so things are looking pretty good for a little rodent that chews holes in walls; 2010 will be the year of the Tiger. There is no year of the Cat in the Chinese zodiac system” (p.119). On the “About” page of DynaWeb, it says things such as: “DynaWeb was launched in March 2002 and visitors have been increasing ever since then. Access log shows that more than 90% of visitors are from China directly or through proxy.” And UltraSurf describes itself like this: “Originally created to help internet users in China find security and freedom online, Ultrasurf has now become one of the world’s most popular anti-censorship, pro-privacy software, with millions of people using it to bypass internet censorship and protect their online privacy.” Even some ordinary users themselves have realized the bias of Falun Gong’s website such as that “Many news/comments on that website are not objective, only Opposition for the Sake of Opposition” (see Biancheng Suixiang, 2010).
and information within the GFW seem to be enough for their daily needs. Indirect data have explained the low popularity of circumvention tools. For example, a report in 2010 suggested that the tools provided by GIFC were employed by “at most 5 percent of internet users even in places such as China or Iran where the Web is tightly controlled” (Pomfret, 2010). According to a series of four surveys (see Table 2) conducted by the Research Center for Social Development, CASS, the percentage of Chinese netizens who used proxy servers significantly declined over the first decade of this century, particularly between 2003-2007. Anecdotal evidence further suggests that while many Chinese netizens (especially university students) were aware of proxy servers and knew how to use them, the percentage of people using proxy servers daily to access blocked sites was relatively small (Dong, 2012).

Table 2. Proxy Server Users in Mainland China (%)

<table>
<thead>
<tr>
<th></th>
<th>2000 (N/A)</th>
<th>2003(N=1619)</th>
<th>2005(N=1165)</th>
<th>2007(N=1315)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>10.0</td>
<td>13.2</td>
<td>9.0</td>
<td>5.5</td>
</tr>
<tr>
<td>Seldom</td>
<td>25.0</td>
<td>33.2</td>
<td>19.7</td>
<td>21.0</td>
</tr>
<tr>
<td>Never</td>
<td>65.0</td>
<td>53.6</td>
<td>71.2</td>
<td>61.4</td>
</tr>
</tbody>
</table>


Despite the above facts, these tools do have some critical impact for a small group of Chinese netizens (citizen journalists, dissidents, activists and public intellectuals in particular).

---

142 It needs to be noted that, in the original sources, figures for 2005 and 2007 do not add up to 100%. I emailed the corresponding author Guo Liang for some clarifications and he replied that it was because of some “missing data” (since participants might refuse to answer relevant questions, which was quite common in surveys) (L. Guo, 2015). Particularly in 2007, the figure added up only to 87.9%, so the finding that 5.5% netizens “always” use proxy server may not as credible as that in previous surveys. The other issues is that, since the entire population of Chinese netizens has undergone significant increase over the last two decades (22.5 million, 79.5 million, 111 million and 210 million respectively in 2000, 2003, 2005 and 2007) (CNNIC, 1997-2015), the exact population of proxy server may have increased (2.25 million, 10.494 million, 9.99 million and 11.55 million respectively in the above years). We should note that this table does not suggest anything about the user population of the second generation circumvention tools (which issue will be discussed in the coming section of this chapter).
Proxy servers have gained popularity mainly among students and hackers (J. Fallows, 2008). Foreign business, retailers and vendors of technological products, academic institutions, as well as individuals, are the main consumers of VPNs.¹⁴³ Users of these tools might increase significantly in extreme cases such as during periods of social unrest and other emergency events (e.g., SARS in 2003) (Elgin & Einhorn, 2006). The diverse usage of these tools has paved the way for the new generation of circumvention tools.

**Scattered Hacking: Circumvention 2.0**

Hacking resistance functions as a challenge to the Chinese authorities. But similarly to their Western counterparts, Chinese hackers are also far from a monolithic group – they are diverse both in thoughts and in actions. Since about 2007, a new type of hacking has emerged in Chinese cyberspace. The hackers of this type not only engage in releasing new anti-censorship tools which are widely distributed, various, mixed and dynamic (these tools could be defined as the second generation), but also launch scattered, unfocused, low-profile, and quotidian attacks towards the censorship machine (the GFW in particular) as revealed by the theory of the hacking movement the West-Chamber Project (WCP).

These hackers, with anarchistic traits, often self-identify as citizens of “Finnish Country.” Finnish Country is not a real place, but an imaginary place (although it could be a reference to a real state – Finland – where the first open-source operating system, Linux, was created).

¹⁴³ Scholars may apply VPNs to update their databases of recent international research in their fields, particularly since Google Scholar became unavailable within the GFW. As discussed in Chapter One, VPNs are somewhat tolerated by the authorities. This could be understood as part of the strategies of adaptive control discussed in Chapter Two. VPNs are very cheap in China, and cost only about $ 40 per year in 2008 (J. Fallows, 2008). Other resources show that on Taobao.com, various circumvention tools have been sold, some of which are as cheap as ¥ 10 per month (less than $ 2 dollars) (X. Su, 2012). However, Taobao seems to have forbidden the selling of VPNs on its platform, since search keywords of “VPN” on its website elicit the response that “According to the relevant laws, regulations and policies, the results of this search cannot be displayed.”
Since the Chinese phrase “Finnish Country” is “Fenlan Guo” which shares the acronym of “Falun Gong,” this argot was originally used as a euphemism for Falun Gong hackers, but now has been widely used by the Chinese hackers as a euphemism for censorship within the GFW. It can also be used as a verb, which may be seen in some expressions where “Fenlan Guo” should be understood to mean “breach the GFW.” Another case is that these hackers quite often use the phrase “tianchao” (heavenly dynasty) which mocks the present-day CCP regime. Discourses like this mean that a particularly “esoteric and geeky enclave” (Coleman, 2013a, p. 89) has emerged amongst Chinese hackers, similar to their Western counterparts. Hackers often communicate with each other in this sophisticated language. More symbolic means of anti-censorship will be discussed in the following two chapters.

The West-Chamber Project

The WCP, the only anti-GFW hacking project with its main participants physically located in Mainland China so far, started in July 2008 and ended in 2010. The name of this project was provoked by the classic Chinese novel The Story of the Western Wing, within which the hero and heroine are two lovers who climb over the wall and engage in clandestine sexual activity. It metaphorically refers to the software helping some ordinary netizens to reach

144 Such as in this text: “The GFW has its own diaries. What does this mean? It means that, when you Fenlan Guo, all your activities are archived. Not only just you but also all others often Fenlan Guo. However, according to statistic data, 87.53% (316 out of 361) Fenlan Guo without consciousness; from the perspective of statistical theory, the more null information being archived, the harder it will be to make sense of the information.” My translation. For the original text, see GFWREV (2010c).

145 It ended not due to censorship reasons but as planned. The Development Team did not plan to exist for long, and it ended when the tasks had been finished. “For the tek4 team, there is no continual plan to go on with this program, neither is plan to data migration. Any development continued and migrated belongs to all others who are interested in it.” My translation. For the original text, see (GFWREV, 2010b).

146 This book was written by the Chinese writer Shifu Wang (1260-1316). Part of it was first translated as “The Romance of the Western Chamber” by George T. Candlin in 1898; in other English translations it is variously entitled “The Romance of the Western Bower” or “The Story of the Western Wing.” Here I use the translation of “West-Chamber” which was originally used by the hackers of this project.
censored materials. This hacking project planned to provide domestic netizens free information and uncensored websites. The announcement for this project reads like this:

As technologists, we need to do something crazy. If we take no action, we will suffer what the bad guys have done. It would be a shame! The GFW becomes mighty and dreadful only because we have not stood together and against it. Now we should stand out and fight; otherwise, we will be mocked in the future by our children who will say “Hey old men, why haven’t you resisted it in the first place?” [my translation] (Development Team tek4, 2008; as cited in GFWREV, 2010d)

The hackers started a blog, *GFW Jishu Pinglun* [Technical Reviews on the GFW], on an international host server and constantly revealed their hacking activities towards the GFW and their involvement in opposing the Green Dam Youth Escort, and they also covered the history and function of the GFW. The screen names of participating hackers were also published, including tek4, KLZ 毕业 (KLZ Graduate), iGFW, nust-, 店长 (Store manager), r007, r008, t00ls, em777, eviloctal, ZWA, Tor project, i2p, and 会长 (Chairman). This blog posted its first article with an English title, “Hello World,” on 23 October 2009, and up until 21 March 2010 when the project team was disbanded, a total of thirteen articles were published (with seven articles in 2009 and six in 2010). These articles have received limited feedback, with the number of responses shifting from nil to over a hundred (some of which are either advertising...

---

147 Its website seems to change according to the surfer’s physical location. For example, I accessed it on 31 October 2014 in New Zealand, its websites shows with a domain suffix of “co.nz” (www.gfwrev.blogspot.co.nz); while if accessed elsewhere, it might change accordingly to a new one.

148 Screen names reveal something (such as interests, favors, aesthetics or identities) about the hackers. While there is no way to get in touch with these hackers to confirm, we can interpret them as: 1) “tek4” might have something to do with the tools of Ryobi Tek4; 2) the “KLZ” in KLZ Graduate is a common phrase used in the game World of Warcraft; 3) iGFW might refer to a Chinese hacking website (igfw.net), and with “i” meaning “love” in Chinese, iGFW thus ironically means “love GFW;” 4) “nust-” could be understood as the acronym of Nanjing University of Science and Technology (a Chinese university); 5) “eviloctal” refers to a self-claimed grassroots website (forum.eviloctal.com); and 6) “Tor project” and “i2p” are two foreign circumvention tools.
or meaningless information). But these articles were widely re-posted by other overseas Chinese websites, which increased their general influence.

**A new anti-GFW theory**

Based on loopholes in the GFW found by previous research (e.g., 2006), as well as more general research (e.g., 1998), the WCP has developed an interesting resistance theory of “shooting at the GFW.” This means generally that the more attacks on the holes in the wall, the easier it is for users to get around this system; moreover, scattered, dynamic, mixed and distributed means are better. Following this theory, the project team tried hard to mobilize more ordinary netizens to participate in activities challenging the GFW.\(^{149}\) It would be fair to argue that the WCP still might not have been able to mobilize enough netizens, but it seems that they have done much better than dissident hackers. The reason why dissident Chinese hackers have failed in challenging the GFW (and promote closed-source software rather than open-source software) is that, at least partially, they could not mobilize enough talented netizens to become deeply involved in the hacking process.

There are three dimensions of this resistance theory and its practical approaches. First, niche technological resistance has been applied. Compared to those well-organized, centralized and collective attacks against the censorship machine, niche attacks would have less chance of being felt by the Chinese authorities. The censorship machine of course can easily recognize such attacks, but these scattered and small-scale attacks might not be worthy

\(^{149}\) On its blog, suggestions are given to ordinary netizens who encounter problems with internet connection (e.g., internet being entirely cut off, slow surfing speeds which have been technologically manipulated by the censors) as follows: 1) Learn how to use the 56K phone modem and get connected even when the entire internet is cut off; 2) update one’s knowledge of dial-up network from various telnet forums; 3) learn how to connect with satellite internet and update one’s knowledge of this technology; 4) those who are physically located in Shenzhen could think about how to become connected with Hong Kong via technologies of microwave communication and/or atmospheric laser communication – using whatever means possible to set up international communications gateways – and so on (GFWREV, 2010a).
of reporting to higher levels of authorities – the censoring instructions come from higher levels of authority and not from the censorship machine itself, which is just an executive body of instructions from the former. With scattered (such as using technology of P2P), small-scale, various, mixed and dynamic characteristics, the second generation attacks might be tolerated by the system; through tiny and everyday forms of resistance, huge changes may eventually arrive (see GFW Blog, 2009b).

Second, the WCP development team believes that the design philosophy of the GFW is that “better is worse.” In other words, the GFW will not try to fill up every loophole in its system; in the contrast, it survives together with these loopholes. The only criterion is to keep both the number and size of the loopholes at an acceptable scale from the perspective of the GFW (and this might be partially because of the funding issue).\textsuperscript{150} The team acknowledges that resisters against the GFW, and the GFW itself, have formed an ironic relationship, within which both parties try to maintain a dynamic balance. On the one hand, the GFW seems to have potentially left some room for the tech-savvy to breach the wall; on the other hand, in many situations the anti-GFW resisters have appealed to hackers not to push the wall too hard, and thus could avoid enraging the censors, and decrease the possibility of the entire internet being cut off as their last resort.\textsuperscript{151} An ideal dynamic relationship between the GFW and its resisters could be formed if the resisters at the weaker end of the spectrum pretend to be weak and let the GFW become intoxicated with small successes in its blocking activities.

\textsuperscript{150} Refer to the discussion of “goagent”, available at a Github repository issue page (goagent, 2014).

\textsuperscript{151} In 2009 after a riot in Xinjiang Autonomous Region (in Northwest China), the internet there was shut off for almost a year. Only some websites of official news portals and governments could be accessed during this period of time. And in March 2012, when social media carried rumors of an attempted coup in Beijing, the government temporarily shut down some of the internet’s micro-blogging services and detained six people (Epstein, 2013).
A third dimension of this resistance theory is that, although at the current stage the authorities and the GFW are located at the top of this ecosystem and ordinary netizens at the bottom, ordinary netizens still can successfully resist their superiors – successful insofar as they access uncensored information whilst avoiding the risk of being caught – by utilizing low-profile, scattered means of resistance. According to this theory, the only issue resisters must bear in mind is that there is no way to find a perfect, one-off solution with which to circumvent the GFW, since the GFW itself is continually being updated. Resisters have to keep on learning this system and updating their methods of resistance accordingly. The WCP team concluded its program by calling for more netizens to get involved in the process of challenging the GFW in its last article:

These articles are trying to show a learning process and methods of the GFW as well as an interest of reverse engineering the GFW. Readers like you are better off being not only a receiver of these messages but also a positive thinker and actor. If one out of a hundred people start to think about the GFW, one out of a thousand starts to do research about it, and one out of ten thousand starts to make the principals into practice, things might get changed eventually. If all the readers are just passive receivers and engage nothing in challenging this system, the GFW will become even stronger and mightier and that will be a disaster for all of us. [My translation] (GFWREV, 2010b)

The calling for more talented netizens to participate in the resistance towards the GFW has been echoed by other ordinary hackers. For example, a user with the screen name “Laomao” published on his/her blog Wo blog gu wo zai (I blog therefore I am) an article entitled “Guanyu qiang de jishu taolun” (Technical discussions on firewall), which invites “those who
have interests in programming” to engage with shooting at the technical loopholes of the GFW and eventually put an end to it (see Laomao, n.d.).

Precisely speaking, the WCP only tried to point out the loopholes of the GFW and the possibility of taking advantage of these holes; it did not directly produce any new or real circumvention tools. Besides acknowledging the value of existing tools (which are low cost and have shortcomings), it invited more volunteers to focus on technologies of “private SSH and VPN,” since these technologies represent the future of anti-censorship tools. In terms of inviting more netizens to practice the theory of “shooting at the GFW,” the WCP has crucially influenced anti-GFW practices.

**New trends of technological resistance**

Some first generation circumvention tools are still available in Mainland China, but most of them have been blocked completely by the GFW. Various new tools, partially provoked by the WCP, have been created and circulated since, particularly those tools compatible with smart phone systems (e.g., Android) and other existing programs.

Fqrouter is one such free anti-GFW tool for Android mobile (smart phone/tablet) users in China. According to its website (fqrouter.com), several public proxies are built into this tool, which can work on mobiles running Android without needing ROOT permission. But when ROOT permission is given, this tool can additionally function as a “router.”

---

152 This article, together with his/her blog, is not accessible at the time of writing; however it has been reblogged by other hackers’ virtual communities such as the “GFW BLOG.” (see Laomao, n.d.)

153 According to fqrouter’s website, being a “router” means, not only the Android mobile running fqrouter is able to access restricted websites, but also this mobile can “share” the free internet to other devices. There are a number of ways to share free internet to other devices via fqrouter: 1) WiFi in => fqrouter => WiFi out (i.e. WiFi repeater); 2) Pick & Play; 3) 3G in => fqrouter => WiFi out (Android built-in); 4) 3G/WiFi in => fqrouter => usb out (Android built-in); 5) 3G/WiFi in => fqrouter => Bluetooth out (Android built-in); 6) LAN in => fqrouter => WiFi out (some set-top box). Be noted that WiFi repeater is a unique feature, but it requires hardware/driver support; Pick & Play scan the devices in your LAN, and forge the default gateway to redirect their traffic via fqrouter. Another article about this tool is available at Biancheng Suixiang (2014).
“fqrouter” combines the acronym of Chinese phrase “fan qiang” (circumvent the firewall) and “router.” Started in 2013 by a hacker with the screen name Qin Fen, this tool utilizes a technology that can theoretically transform any Android mobile running it into a router. Although it may result in slower surfing speeds and require more frequent battery charges, this tool has functioned stably so far, with its longest streak of downtime only lasting 11 days in December 2013. The creator has made clear that while he or she did welcome donations they would not go to the creator’s own pocket but rather to two public host servers (which help to promote this tool). Users are encouraged to report any problem with this tool, to circulate it as widely as possible and, most importantly, to contribute with their source code (see fqrouter, 2013). A virtual discussion group for this tool has since been set up at Baidu Tieba, a popular BBS service hosted by Baidu. It is interesting that this kind of discussion of anti-censorship measures could be tolerated by the censors. At the time of writing, there have been 18,375 followers and 42,182 individual posts in this group (Baidu Tieba, n.d.-a).

Another tool, fengye xiangjiao (the Maplebanana-proxy), which is also known as the Onion-project or Smartbanana, was developed by an anonymous hacker named “ring-hacker” (see Onion-project: fengye xiangjiao, 2013). This tool simplifies the codes of GoAgent, Wallproxy and Gsnova, and makes these circumvention tools more compatible with the open-source browser Firefox. So too do many others including VPN Gate (designed by Japanese researchers and targeted mainly at Chinese netizens, see Nobori & Shinjo, 2014), GoAgent, Shadowsocks, landeng (Lantern), Gfanqiang (not updated since 2013), and Greatagent (originally named Wwqgtxx-goagent) which have also become available for some ordinary Chinese netizens.
Tools like these reveal some new trends in technological resistance in Chinese cyberspace. Firstly, while organized means and activities of technological resistance may still exist, scattered, low-profile and decentralized means and activities have become relatively more popular. Secondly, the second generation tools are more likely to be open source, and their users may contribute to the source code as well. Thirdly, these new tools are potentially designed for solving the problems of existing third-party programs and are compatible with such programs. Fourthly, these new tools are more likely to be made using cheap and readily accessible technology, and hackers themselves do not seem worried about funding (as was the case with dissident hackers of the first generation). Fifthly, most the second generation tools have been developed by a single hacker rather than a group of hackers (though in some cases volunteer hackers may be involved in the process later on), and they develop these tools “simply and purely” based on their interests. Last but not least, besides using various SNSs, such as Facebook, Twitter, and YouTube, to circulate their products, these hackers may also use other platforms, such as Beauty Garden (Meiboyuan, allinfra.com) and the Project Hosting of Google Code (which aims at “providing a free collaborative development environment for open source projects”), to discuss anti-censorship issues and develop tools. These platforms (most of which are outside the GFW) have become virtual homes for the hackers.

In general, many hackers of the new generation, including the WCP team, tend to believe that technological resistance against the GFW is an ongoing struggle, for while the GFW is very good at attacking resistant tools, the resisters must keep on adapting new methods to get around the firewall. The main problem of this model of imbalanced interaction between resisters and censors lies in the fact that as the GFW becomes mightier and stronger, it will
become technologically and economically harder for netizens to break through the firewall. This worry becomes even more significant in light of two increasingly common viewpoints. One is that “You might think you have successfully broken through the wall, while in fact you are still in the wall” (Yu Zhou, et al., 2010) and the other is that “Our difficulty is not that wall but the decreasing number of users of circumvention tools” (Diao, 2014). Hackers could undoubtedly find ways to adapt themselves to this system, but it is part of a much larger problem that technological methods alone – circumvention tools included – cannot fix.

Technological resistance in Chinese cyberspace does function as a challenge to the GFW control system, and enables users of circumvention tools to access and share freer information. However, we should not overstate the influence of such resistance. There is no sign of the GFW becoming less powerful; by contrast, it seems to be more powerful than before. The second generation hackers strategically launch scattered, low-profile and quotidian attacks and tools to challenge the GFW system – which is impossible, to date, for the GFW to block completely. At the same time, however, they try to avoid enraging the censors and emphasize their co-existence with this control system, which determines that such small-scale, scattered resistance may not be able to fundamentally challenge this system. From this point of view, this new kind of resistance seems to have become a part – albeit an unharmonious part – of the authoritarian control system.

---

154 The second sentence was said by a user with the screen name Diao Jinping (刁近平) on his Google+ page. According to his activities there, he is a student who is pro-Kuomintang and against the CCP, and has posted various trolling content. His screen name is a satirical substitute for the current Chinese president “Xi Jinping (习近平)” and “diao (刁)” in Chinese means “bloody, unruly.”
Though many ordinary netizens may also be involved in technological resistance (through means such as becoming consumers of circumvention tools), this kind of resistance is mainly conducted by a small group of tech-savvy netizens. Non tech-savvy netizens are more likely to utilize symbolic means (such as euphemistic words, esoteric way of writing, and satirical images) and rhetorical means (such as parody) to bypass and challenge the GFW system, a theme that will be fully investigated in the coming two chapters.
CHAPTER IV. THE POWER OF DISCOURSE

The discussion of technological resistance never represents the whole story of internet resistance in Chinese cyberspace. Symbolic resistance, another very important form of resistance, deserves equal (if not greater) emphasis. So far, symbolic responses to internet censorship have seldom been investigated by scholars, if not entirely overlooked. Take Gary King et al.’s research (2013, 2014) as an example. When designing their research methods, the authors use a list of sensitive words (based on a dictionary, Chinese-language online Wikipedia, and other relevant databases) and seldom realize that many Chinese netizens may not use such words (which are blocked or deemed sensitive by the censorship system) in their online expression. In reality, in the Chinese context, as Fu, Chan, and Chau (2013) find, puns, homophones, or special combinations of written Chinese characters that don’t appear in dictionaries are commonly substituted for sensitive topics or names. In other words, studies that “impose a predetermined list of Chinese terms might fail to correctly identify the user-generated terms and thus limit the scope of their findings” (p. 49).

This chapter and the following one focus directly on the various symbolic strategies utilized by many Chinese netizens to circumvent top-down censorship in their everyday lives online. Although symbols may play important roles in real-world resistance, they are even more crucial in symbolic resistance in cyberspace. Symbolic resistance in cyberspace is involved densely in discourses (cyber slang and esoteric writing) and rhetoric (e.g., humor, satire, and parody); and, within the context of media forms, resisters of this kind may apply various kinds of texts, images, audio materials and videos to express and practice their resistance. While Chapter Five will investigate images, audio materials and videos as forms of
symbolic resistance and resistant rhetoric, this chapter deals with the theme of discourse as symbolic resistance.

**Multiple Themes of Discursive Strategies**

Keyword filtering is one of the main methods utilized by the Chinese internet censorship system, which, as discussed in Chapter One, has greatly limited ordinary netizens’ free speech in Chinese cyberspace – many Chinese netizens have a sense of the forbidden words and topics, and quite often self-check before they cross the line. It is arguable whether this mechanism can entirely prevent netizens from expressing sensitive information (Neumann, 2001). In fact, netizens have used various discursive strategies to breach the keyword censorship mechanism. This discursive dimension of Chinese cyberculture has attracted some academic attention, such as the publication of some dictionaries that have included internet discourse.155 A few scholars outside China have paid some attention to discourses relevant to censorship. For instance, the U.S.-based research organization *China Digital Times* (chinadigitaltimes.net) has long focused on censored words in Chinese cyberspace; and some scholars (e.g., Bamman, et al., 2012; Ng, 2013) also have tried to make a list of such words. Having acknowledged the existing research, this coming section investigates the main types of discursive strategies used for circumvention purposes. These discursive strategies enable some

---

155 In the early days of the new millennium, some domestic scholars turned their attention to cyber discourses and even edited some dictionaries on the subject, for example, *Zhonguo wangluo yuyan cidian* [The dictionary of China’s internet language] (G. Yu, 2001b) and *Wangluo shishang cidian* [The dictionary of internet fashion] (W. Yi, 2000). Most terminology collected in these dictionaries is mainly about the new information technologies (both hardware and software). Dictionaries published much more recently include *Wangluo naxier* [Those words used in Chinese cyberspace] (2014), *Xinhua wangluo yuyan cidian* [New China’s internet language dictionary] (2012), and *Wangluo xinxin cidian* [Internet dictionary for generation X] (2012). Though in these recent dictionaries, much slang that reveals socio-political and cultural issues has been included, discourses relevant to censorship and resistance are rarely included, albeit that these are, undoubtedly, becoming more and more important in this realm.
Chinese netizens to discuss sensitive topics or even criticize the Chinese authorities, which is otherwise impossible. My typology of discursive strategies here has been greatly inspired by Rauchfleisch and Schäfe’s (2015) research on the multiple public spheres of Sina Weibo, though my focus is not on public spheres but on discursive strategies. According to their contents, I will propose five ideal-types of discursive strategies: the hard-political type, the livelihood-related type, the non-domestic type, the sub-cultural type, and the meta type. Each of these types can be substantiated by numerous examples, but in the interest of brevity, I only give a limited number here, for the purpose of clarification (see Appendix C for more examples). This typology aims to provide a complex and dynamic picture of cyber slang in Chinese cyberspace and a better understanding of this phenomenon, although the merits of my selection may be debatable.156

The hard-political type

The hard-political type of discursive strategy is mainly concerned with hard-political issues which have been officially acknowledged as political taboos, such as the anniversaries of the Tiananmen Incident. Since discussion of June 4 (the date when the Tiananmen Square massacre happened in 1989) has long been blocked in Chinese cyberspace, netizens speak in alternative ways, such as “May 35,” “liusi” (willows, a homophone with “June 4” in Chinese), or “82” (eight squared equals 64, which can refer to June 4), among many others (see Appendix C for more examples). Sometimes, it is striking that netizens can develop ironic and esoteric references to discuss and make criticisms of the ruling party and the regime, the top

---

156 This typology, of course, does not mean that no other types exist – other types may exist, but these types are the main types here and may cover issues relevant to other types. But, these types are not entirely mutually exclusive and may sometimes overlap with one another. For example, the livelihood-related type may also be involved in hard-political issues.
leaders, corruption among political elite, and party-controlled media. For example, “wodang” (my party), “nidang” (your party) (Nordin & Richaud, 2014), or even “tugong” (indigenous communists) have been used to poke fun at the CCP. When it comes to the state, the phrase “天朝” (Tianchao, Celestial Empire), originally referring to the traditional Empire of China, now is satirically used to mean China under the control of the CCP. Other ironic euphemisms include “天朝” (Wangba Chao, Tortoise Empire), as “天” (Wangba, Tortoise) looks pictographically like “天” (Tian, Celestial) and “tortoise” is a swearword in Chinese. “Xi Chaoxian” (West Korea) also is used for satirical expression, since China is located west of Korea. Sometimes, “guiguo” (your honorable country) can ironically be used to refer to China as well, though the speakers themselves are Chinese people.157 Similar strategies have enabled some netizens to vent even harsher criticism. Although “独裁” (ducai, dictatorship) is a sensitive word (often used by Western media to describe the regime under the CCP), it is quite common for netizens to use hidden yet ironic phrases such as “毒豺” (vicious jackal) or “毒菜” (poisoned vegetable) to avoid being censored, as both terms share the pronunciation of “ducai” with 独裁 and are thus used as ironic alternatives to refer to dictatorship.

Although internet censors keep on working hard to delete negative information about top leaders, some ironic and cynical words and phrases do circulate virally in Chinese cyberspace. For example, “chujun” (crown prince, heir apparent) referred to Xi Jinping, and was used for some time before he officially became China’s new leader (K.-W. Fu, et al., 2013); with other names mocking Xi such as “Weinixiong” (Winnie the Pooh) and “Qingfeng Baozi” (the

157 In the cases of “your party” and “your country,” the rhetoric is very interesting, since although the speakers themselves may rightfully be members of the CCP or Chinese citizens, they still use “your” to distance themselves from the party and the country. Users communicate a kind of satire when using these words.
steamed bun from the Qingfeng restaurant). During the processes of some politically
sensitive events, a list of words may be temporarily forbidden in Chinese cyberspace; and,
accordingly, a list of anti-censorship words will be created. Take the Bo Xilai event in 2012 as
an example. During this event, the authorities tried to control the information flow about
this event by banning the names of relevant people and places. Meanwhile, netizens created
alternative words to talk about this case. *Pingxi Wang*, literally the “King who pacifies the
west [Chongqing],” is encoded as a reference to Bo Xilai. And “*hushizhang*” (head nurse, a
near homophone with “deputy mayor” in Chinese) meant Wang Lijun, a key figure in the Bo
scandal; while “*xihongshi*” (tomato, a homophone with “western red city” in Chinese) referred
to Chongqing. The censors may well understand these tactics after the fact, but it is impossible
for the censorship system to forbid all kinds of strategic expression since variations may keep
on appearing.

The discursive strategies enable netizens to criticize party-owned media as well. As shown
in Appendix C, “*houshe*” (monkey and snake) is used as a homonym of “mouthpiece” and
“*meiti*” (pleasing body) refers ironically to party-owned media in general. In particular,
various ironic names for CCTV (*China Central Television*) have been created, CCAV (*China

---

158 On 28 December 2013, Xi Jinping was photographed lunching at a Beijing steamed bun restaurant
named Qingfeng, which was read as an attempt to show he was in touch with the lives of ordinary people. Some
protestors soon adopted the bun as a symbol of their protests. The steamed bun from the Qingfeng restaurant
became a satirical argot used by some netizens. The title of Winnie the Pooh is used to mock Xi’s podgy
appearance. See Appendix C for more euphemistic terms for Xi Jinping.

159 Bo Xilai, then the party chief of Chongqing (a western municipality in China), was removed from his
position because of a series of incidents. Earlier, Wang Lijun, Bo’s top lieutenant and then the deputy mayor of
Chongqing, sought asylum at the U.S. consulate in Chengdu (the capital city of Sichuan Province, west of
Chongqing), and Bo’s wife was involved in the murder of a British businessman. Bo himself, as one of the
“princelings” of the CCP and the initiator of the Chongqing Model, tried hard to build a charismatic personal
image and was active in public media, which was very different from the normally staid nature of Chinese
politics. Some commentators believe that the fall of Bo was mainly due to political struggles between different
factions within the CCP.

160 For example, Bo Xilai can also be referred to by other phrases such as “*buhou*” (not thick), another way
of alluding to “*bo*” (thin) in Chinese, and “*Bo Du*” (Bo the Governor).
Centra Adult Video) and “yangshi” (calamity TV), to name a couple. And one of the party-owned daily newspapers – Renmin Ribao (People’s Daily) – is mocked as “People’s Daily Explosion” (“explosion” shares the syllable “bao” with “newspaper”). Its affiliated newspaper,环球时报 (Huanqiu Shibao, Global Times), is named “环球屎报” (Huanqiu Shibao, Global Shit Times), “环球时报” (Huaiqiu Shibao, Bad Global Times), or “混球屎报” (Hunqiu Shibao, Muddled Shit Times). The chief editor Hu Xijin is mocked as a watchdog for the Party, with the ironic names of “Hubian” (Hu the Fabricator), and “Hudiao” (Hu Bite, literally “to hold something in the mouth like a dog”).

The livelihood-related type

This type mainly addresses issues relevant to people’s livelihood and quality of life, including environmental pollution, food safety, human rights and grassroots protests. In environmental protests, such as the Xiamen anti-PX protest in 2007 (among many other cases in the following years), since the phrase “shangjie youxing” (street protest) is blocked in cyberspace, protestors strategically use “sanbu” (leisure walk) as a euphemism in their everyday communication via internet or mobile networks. “Lianghui” is a term which commonly refers to two meetings, the National People’s Congress, and the Chinese People’s Political Consultative Conference, held every March by China’s political leadership. Many protesters and petitioners organize relevant activities during this period, in the hope that their demands might be more likely to be met. Meanwhile, the entire censorship system works harder than in other periods of time to monitor and filter the protesting activities online. Organizers strategically disguise their protesting events as “lianghui,” and this cleverly selected terminology generally indicates attempts by protest organizers to circumvent
censorship on various platforms in the lead-up to these two meetings (see Kent, 2011). Social unrest also sparks neologisms. In 2011, a mass protest broke out in Wukan (a village in southern China with a population of around 13,000). Thousands of villagers gathered outside a local government building to protest the corrupt local officials’ selling of land to developers without properly compensating the villagers. This topic became blocked in many cyber communities, and relevant searches were blocked by internet censors (BBC, 2011). Strategies were developed by netizens. For example, the Chinese characters 鸟坎 (niaokan, bird ridge) which were pictorially similar to 乌坎 (wukan, black ridge) were used to refer to this village. And “WK,” short for Wukan, was often used as a reference to the protest as well. A further euphemistic expression is 乌鸦 坎坷 (wuya kanke, crow bumpy), with the first character in each word together reading wukan.

Similar tactics can also be seen in events about human rights. In 2010, Chen Guangcheng, a blind human-rights activist who always wears sunglasses, escaped from house arrest to the U.S. Embassy in Beijing. Although directly searching for relevant news was blocked from the Chinese websites, “CGC” (the initials of his name) or “mangren” (blind man) were strategically used to talk about this case, terms which were finally filtered as well. “Sunglasses” became an ironic, yet factual internet meme for a while, both online and offline (Branigan, 2012). When netizens get into trouble with the police because they have published something that has crossed the line, they use “qing hecha” (be invited for tea).161 Similarly,

161 For example, “Since 360 (a freely available anti-virus software which is believed to monitor its users on requests from the Chinese authorities) monitors every detail of your activities and sends the monitoring file to cyber police, you should be care of your activities [and do not cross the line] to avoid being qing hecha” [my translation]. (Original text refers to wwqgtxx, 2014)
“cha shuibiao” (check the water meter) refers to an excuse, said to be used quite often by the police when they come to detain those who cross the line.

The non-domestic type

This type is mainly about issues (particularly democracy-related issues) that have happened outside Mainland China, yet attracted huge attention from the domestic public, such as the Arab Spring, the Occupy Movement, and Hong Kong pro-democracy protests in 2014. Though discussions of such issues may not be sensitive in the beginning, they can easily become sensitive when they are referenced back to China; censorship as well as resistance thus often happens. For example, since information about the Hong Kong pro-democracy protest has been blocked in Chinese cyberspace, netizens develop many alternative terms such as “yushan geming” (umbrella revolution), “yuzhe geming” (awning revolution), “sanhua geming” (umbrella flower revolution), “zhanzhong” (stand central) and “Occupy Central”. The censorship system responds promptly and has blocked many of these terms, but it seems unrealistic to completely wipe out discussions about this topic in Chinese cyberspace.

The sub-cultural type

The sub-cultural type involves issues such as feminist resistance, erotic activism and hacker resistance. Some women’s rights websites (e.g., www.ifeminists.com and www.womenofarabia.com) are currently blocked by the GFW, as are LGBT websites and mobile apps. An example of a blocked LGBT website is Jack’d, a gay dating and hook-up app created in Belgium and often referred to by its Chinese name jiekedi (literally referring to the activity of a sex worker finding his or her customers), which became popular in recent years in larger Chinese cities such as Shanghai (see Sun, 2014). However, alternative websites do exist
which are available for Chinese feminists and LGBT (Ho, 2007), and they develop
euphemistic terms for everyday communication such as “duanbei” (broke back, a term from
Ang Lee’s movie “Brokeback Mountain”) (Ho, 2008). In another case, discussed by Jacobs
(2012), when an actress’s name was temporarily banned in Chinese cyberspace because of her
naked appearance in a movie, netizens “allocated new names for her so that they could keep
circulating the infamous sex scenes and other information about the actress” (p. 30).
Discursive tactics have also been used in hacker groups, such as “Fenlan Guo” discussed in
Chapter Three. Another case is “tao” (Tor, literally referring to condom; as the pronunciation
of Tor is similar to “tao” in Chinese). When hackers or users of circumvention tools say
“daitao,” they often mean “using Tor.” More discursive strategies for cheating the censorship
system can be found in the anti-GFW community. For instance, before Google withdrew its
search engine service from the Mainland China, netizens often searched it by “elgoog”
(Google spelled backward) and it led them to the site which allowed free searches. And an
email that contains “VOA” might be monitored, but one with a zero substituted for the “O”
could get through (Elgin & Einhorn, 2006).

*The meta type*

This type addresses discussions and criticisms of issues relevant to censorship itself. The
“Grass Mud Horse lexicon” is a good example, which has been defined as revealing a kind of
“resistance discourse” (Mina, 2014; Xiao, 2013). Both “Cao Ni Ma” (Grass Mud Horse,
meaning “fuck your mom”) and “Mala Gebi” (the Mahler Gobi, meaning “your mom’s cunt”) are dirty words, which originally show some ordinary netizens’ anger towards the censors and censorship itself. “Mala gebi” begins a collective narrative trend, and a lot of other “shenshou”
The majority narratives have been focusing on the fight between these mysterious animals and “He Xie” (River Crab), which reveals an imaginary battle between censors and those being censored. All these dirty words used against River Crab are dressed up as “pure” homophones to be able to pass through the monitored gateways. The censors have responded to such encoded yet overt offence by limiting the circulation of such homophones; relevant search on Baidu seems to have been “purified” by removing plain discussion about the political meaning of these homophones. Encoded yet satirical expressions have also been made towards censorship departments themselves as well, such as replacing the Publicity Department with the Ministry of Truth (Ng, 2013, p. 46), whose voice is by all means  
\[\text{weiguangzheng} - \text{weida} \text{ (great)}, \text{guangrong} \text{ (glorious), and zhengque} \text{ (correct), and mocking the SAPPRFT as guangdianju} \]
(state administration in the nude) or  
\[\text{guangdian zongji} \text{ (State of Anxiety on Film, Radio, and Television).} \]

As discussed above, despite the controlled atmosphere, many Chinese netizens have developed multiple themes of discursive strategies. Through this type of discursive guerrilla

---

162 In 2009, Baidu Baike listed ten mythical creatures on the Chinese internet. Besides Cao Ni Ma, there are  
\[\text{Fa Ke You} \text{ (literally meaning “French-Croatian Squid” but actually referring to the English phrase “fuck you”)}, \text{Ji Ba Mao} \text{ (literally meaning “Lucky Journey Cat” but a homophone with “pubic hair”), Wei Shen Jing} \text{ (literally meaning “Stretch-Tailed Whale” but actually referring to “menstrual pads”), Yin Dao Yan} \text{ (literally meaning “Singing Field Goose” but actually referring to “vaginal infection”), and other creatures.} \text{ On the translation of these mythical creatures, refer to H. Li (2011, p. 79).} \]

163 River Crab is a similar homophone of “harmony” in Chinese, a mockery of the ideological slogan “building the harmonious society” which was promoted by the former Chinese president Hu Jintao. It has been used as an ironic reference to the censors. Each session of Chinese Government in recent years has launched a certain kind of ideological idea. In the times of Jiang Zemin, he proposed the idea of the “Three Represents [sic]” which means that the CCP “represents the development trend of China’s advanced productive forces, represents the orientation of China’s advanced culture, and represents the fundamental interests of the overwhelming majority of the Chinese people.” Jiang’s idea has been mocked by netizens as “dai sankuai biao” (wearing three watches), with “represent” and the euphemistic phrase “wear watch” sharing the pronunciation of “dai biao” in Chinese.
war, the users create a limited yet uncommon discursive space, within which discussion or even criticism of sensitive issues becomes possible. The making of satirical discourses nowadays has become collective and carnivalesque in Chinese cyberspace. Many Chinese netizens utilize a rich and playful language which is not immediately comprehensible to average Chinese speakers, but is understandable for those who are familiar with this encoded language (Rauchfleisch & Schäfer, 2015).¹⁶⁴ This cyber slang, having provided the users with an alternative way to communicate sensitive issues, functions basically as a challenge (and sometimes resistance) to the control policy and official discourses. Although in some situations the censorship system has responded to user-generated esoteric words very promptly – for example adding some euphemistic phrases to the blacklist of sensitive words, it is impossible to completely block the creating mechanism (Faris, Wang, & Palfrey, 2008). For if one phrase has been blocked, another one will soon appear. At least many Chinese netizens are never passive targets of censorship; they continue engaging actively and creatively in the battle between River Crab and Grass Mud Horse.

The Mechanism of Discursive Resistance

While the previous section focuses on different types and themes of discursive strategy and resistance, this section discusses two issues: the technical means which makes discursive resistance possible, and the historical development of such technical means in Chinese cyberspace.

¹⁶⁴ It should be pointed out here that “encoded language” does not refer to a fixed discursive phenomenon (i.e., every disguised discourse is always “encoded”). In fact, the situation of “encoded” is not fixable; encoded terms will become less encoded and even not-encoded, after they have been known to the wider public including the censors.
Technical means

In general, there are five kinds of technical means that enable some Chinese netizens to practice discursive resistance: English equivalents, Pinyin, pictography, homophones, and remixing.

*English equivalents*

Since the keyword censorship used by the GFW is mainly focused on Chinese characters (rather than other language systems), netizens have greatly utilized English words – both whole words and initials, such as kmt (Kuomintang), CNN, VOA, CCAV, June 4 and umbrella revolution – to express sensitive content, via which method sometimes they are able to breach the censorship system. Most of the time, Chinese netizens use these English words and initials in the same way their foreign counterparts do. But, sometimes, they may use some English words in the Chinese way. “Chinglish” usage may not follow English grammar and is sometimes barely understandable for English native speakers. The discursive resistance disguised in English words become part of the language used by many Chinese netizens nowadays, and reveal an important feature of Chinese cyberculture. It, however, does not mean that the censorship system is oblivious to this grassroots strategy. In contrast, it keeps on...

165 Why do Chinese netizens use English words, rather than words from other languages, to express sensitive information? The historical reason is worth mentioning here. Two language learning trends have happened since 1949 in China. One was the enthusiasm for learning Russian in the 1950s, when China and the Soviet Union were in their honeymoon phase. Almost all intellectuals were proud of being able to speak some Russian words. This enthusiasm declined when the relationship between China and the Soviet Union hardened. Another trend has been the enthusiasm for English since the 1980s. The reform and open door policy showed China’s friendly attitudes towards the English-speaking world. For both the authorities and ordinary people, English seemed to symbolize a distinctively different culture – a capitalist culture and thus a civilization of modernization (Y. Chen, 1991, p. 1). This trend for English lasts to this day, in the internet era, and has determined the bilingual or multilingual phenomenon in Chinese cyberspace. Two other factors have also helped to form a hidden resistant culture by using English words: that English is the dominant language on websites (85% of websites are reportedly in English), so Chinese users have had to get used to this cultural context (particularly in the early days), and that consuming foreign culture and using English discourses have become a symbol of fashion and modernization for many Chinese netizens. This can be explained by the crucial phenomenon that a huge population of Chinese netizens are consumers of English-language entertainment industry products (pop music, movies, and TV dramas, etc.).
adapting itself to update its blacklist of sensitive words (e.g., posts with English words such as June 4, Umbrella Revolution and Jasmine Revolution are more likely to be blocked). Although nowadays a huge number of Chinese netizens can understand some English words – or if they do not, online English-Chinese dictionaries make deciphering English words fairly easy – most Chinese netizens are monolingual. Sensitive information disguised by English words may thus have limited political influence.

Pinyin, pictography and homophone

Since the keyword censorship system initially targeted Chinese characters, a huge number of Pinyin words, or initials of Pinyin words are used to circumvent this censorship mechanism as well. Some examples discussed in the previous section actually have been disguised in Pinyin words, such as “tugong,” “liusi,” “WK,” “zhanzhong” and “CGC.” The censorship system sometimes does add Pinyin words onto its blacklist of sensitive words. For example, searching “xijinping” (a reference of the name of the current president Xi Jinping) on Weibo will result in nothing but a notice that “According to the relevant laws, regulations and policies, the results of this search cannot be displayed.” However, some Pinyin words such as “tugong” (a satirical reference to the CCP) can still be used in Weibo posts.

The pictography of Chinese characters has also been widely used for anti-GFW purpose in Chinese cyberspace, which can be shown in the aforementioned examples of alternative references to China (e.g., Celestial Empire and Tortoise Empire), the Global Times, and the Wukan case. Based on the pictographic similarity, politically sensitive terms can be encoded. For example, since “自由” (ziyou, freedom) is sometime a sensitive topic (as shown in the discussion about online game censorship in Chapter Six), netizens develop various disguised
expressions, such as “目田” (*mutian*, literally meaning eye-field) and “自曲” (*ziqu*, self-twist).

It is also common to use character variations (e.g., break up a Chinese character into several parts) to escape censorship. The Chinese phrases “李月月鸟” is a break-up of the name of previous Chinese prime minister “李鹏” (Li Peng), who was deeply involved in putting down the Tiananmen Incident. In another example “火乍和弓单” (fire suddenly and bow single) actually means “炸弹” (bomb). The pictographic technique can even be used in a very creative way. For example, in discussions of the Tiananmen Incident, netizens use “占占人” (*zhan zhan ren*) to mean “a man in front of two tanks,” and thus to indicate the hero “tank man” in the Tiananmen Incident.\(^{166}\) Similarly, “占占点” (*zhan zhan dian*) or “占点占” (*zhan dian zhan*) means “tanks crush people to death.” These Chinese phrases have little chance of being recognized by auto-censors as sensitive materials, thus gain the possibility of circulation in Chinese cyberspace.

Use of homophones is a further technique that enables some Chinese netizens to escape the censorship machine. This can be shown in the aforementioned examples of alternative references to dictatorship, and in many other cases. For instance, when talking about human rights, netizens sometimes use “人犬” (*renquan*, human dog) – since “犬” (dog) and “权” (right) share the sound of “quan” in Chinese, “人犬” becomes an encoded reference to “人权” (*renquan*, human right).

*Remixing*

In Chinese cyberspace, hybrid characters and initials of Pinyin (or English words) successfully help the users to cheat this system on occasions, and get sensitive messages

\(^{166}\) This is because the character of 占 (*zhan*) pictorially looks like a tank, and 人 (*ren*) means “man.” See Appendix C for more detail.
published. For instances, phrases directly referring to the CCP may not be allowed to published in some situations, but remixed phrases such as “共 chan 党” or “GC 党” can sometimes escape the keywords censorship system. This technique can also be seen in the aforementioned case of Hong Kong pro-democracy protest. Since the Chinese words “占中” (zhanzhong, occupy central) were once blocked on Sina Weibo, users strategically used “z 中” or “站中” (zhanzhong, stand central) to refer to what has happened in Hong Kong. (See Appendix C for more cases.)

**Historicizing discursive techniques**

Although internet censorship has played a significant role in shaping and determining these above discursive techniques, other factors do influence them as well. It is worthwhile to briefly discuss the development of these techniques in the Chinese cyber context.

In the early days of internet development, Chinese netizens had more freedom in their online practice; some of these techniques already existed, for example, initials, pictography and homophones. Since surfing speeds were relatively slow and costs were relatively high, in order to conduct online chat more quickly and smoothly, users creatively brought in initials, homonyms and transliterations, which could help them save time and money. These methods were gradually normalized. Due to increasing political censorship on cyber expression, they have more recently become popular techniques to evade the gaze of the authorities.

The development of internet technologies has deeply shaped these techniques, as has the development of Chinese character input-technologies. Unlike the convenience of the English input process, Chinese character input is not a matter of simple permutations and combinations of 26 Roman alphabet letters. Keyboard inputting of Chinese characters requires a special
software program which is based on either the shape or the pronunciation of the character (Danet & Herring, 2007, pp. 70-72). This made it a real challenge for early users to input a Chinese sentence. Chinese character input-technologies since the 1990s can be divided into two types: those with a pronunciation-based input method (yinma) and those with a form-based input method (xingma). The former becomes more popular (see L. Gao, 2005, pp. 113-118). It is much easier to get used to the pronunciation-based input method, because, compared to the form-based input method, the pronunciation-based input method requires much less systematic training, and only requires familiarity with Roman alphabet letters in order to recognize a character.

Many Chinese characters have the same pronunciation as other characters but different shapes. This implies that the pronunciation-only method is not enough. Sometimes this method causes problems. Particularly in the early days, this method was not sufficiently intelligent. When the users typed some letters of a pronunciation into the computer, the computer might not easily have recognized relevant Chinese characters. In order to save input time, many users often skipped the phase of choosing the correct Chinese characters and kept the computer’s first suggestion, despite the fact that the computer sometimes made hilarious mistakes. A small number of homonym mistakes did not block the normal communication process among users. Quite conversely, some mistakes have been gradually accepted by users and treated as a personalized feature of online communication. Though the pronunciation input method has become much more precise, some users even purposefully create some wording mistakes in order to make the content more vivid and interesting. This technique has become a

167 In China at that time the internet service was still relatively expensive and the customers were usually charged based on the amount of time they spent online. Refer to Liwei Gao (2005, p. 62).
significant satirical method and been greatly used in later expressions of politically sensitive issues. Many newly created anti-censorship words (particularly the Pinyin homophones and character variations) are actually affected by these input methods.168

Some of the techniques are not brand new; they have much to do with previous cultural practice. Many linguistic means can be dated back to the 1980s; as a Chinese sociolinguist recorded, ironic transliteration of English phrases already existed then.169 Breaking up and/or remixing Chinese characters is not a wholly new phenomenon either. This has actually long been practiced by Chinese men of letters in pre-internet times. Party-owned media often publish their editorials along the party line (as publicity organs should do); while at the same time, disguise their voice and stances by using “unofficial” pen names. For example, the pen name of “郑志学” (Zheng Zhixue) shares the pronunciation of “政治学” (zhengzhixue, politics science);170 “任仲平” (Ren Zhongping) is short for, and a homophone with, “人民日报重要评论” (Renmin Ribao zhongyao pinglun, important comments from the People’s Daily). Another case is “单仁平” (Shan Renping), an important pen name seen quite often in the Global Times. “Shan Renping” is believed to be a homophone of “San Ren Ping” (三人评, comments from three people including the chief editor Hu Xijin). (For more cases, please see Fangjiahutong, 2012). This political climate cultivates a culture within which political struggle
can take place via wordplay and at the discursive level. Both the development and the tightening control of the internet have made these discursive techniques popular again – though this time as part of a more bottom-up process.

**Esoteric Writing: Modes of Expression**

In Chinese cyberspace, discursive struggles happen not only at the level of words and phrases, but also at the textual level. By textual level, I mean that netizens also apply various modes of expression to circumvent censorship. In general, based on present technologies, the GFW can only monitor and automatically filter sensitive keywords; when it comes to texts, which involve cyber slang, emotions, narratives, rhetoric, the censorship system depends more heavily on human censors. It is impossible to monitor and filter every piece of texts online. In order to circumvent auto-censorship or even human censors, some Chinese netizens have developed various modes of expression, such as chrysanthemum writing, Martian scripts, and encoded writing. Based on these modes, the users are able to communicate sensitive messages and make criticisms of the regime, social problems, and censorship itself. Although this section discusses several main modes netizens utilize in their everyday resistance, this is not to say that other more marginal modes are not important. Every mode is important in its own context; and furthermore, new modes keep on emerging to become indispensable parts of a resistant cyberculture.

Chrysanthemum writing was initially created by some young Chinese netizens mainly for fun, but this writing was soon used widely for censorship circumvention by dissident netizens. When users want to publish an article or a post with sensitive words, they just have to run this text through an online conversion tool, or simply use some input methods which are
compatible with chrysanthemum writing, and a new text, with every character encircled by a chrysanthemum flower, will be immediately created. Based on this textual trick, the new text can seldom be detected by automatic censorship machine, while other in-group users are able to decipher it fairly easily (Ng, 2013, p. 42). For example, the below text simply reads “人权, renquan, human right,” which is written in chrysanthemum writing. With each character and letters encircled by the interference of a chrysanthemum flower, the phrase is unrecognizable for auto-censors, but it is still readable if readers ignore the chrysanthemum flowers.

人权 renquan human right

Along the line of chrysanthemum writing, users also quite often apply brackets, boxes or circles to break up sensitive characters and thus avoid recognition by the automatic censorship machine. It is quite normal for a speaker to use characters to say one meaning while at the same time to use brackets with Pinyin words inside, to say another meaning (often an opposite meaning). For example, in the case of “民主 (du)主 (cai),” if readers only focus on pictograms, it says “民主” (minzhu, democracy); but if readers focus instead on what is inside the brackets, it says the opposite, “dictatorship). Expressions like this can not only escape auto-censors, as sensitive keywords such as “民主” (democracy) have been broken up by brackets, but also can produce an ironic meaning, since this expression combines two conflicting meanings in a single saying.

Martian script, popular with the younger generation of Chinese netizens, can also be utilized for anti-censorship purposes. The main characteristic of this writing is the breaking up of sensitive characters into pieces and/or combining several characters to mask sensitive words. Character variations (e.g., breaking-up characters), as discussed in the previous section,
have been used a lot in Martian script. Words from other languages (such as Japanese words and English words), emoticons, and Arabic numbers (as homophones of Chinese characters) are also quite often used in a single article. Also, articles of this kind have no fixed narrative rules or grammar. For example, the title of a Weibo post, “人木又与 MZ 报告” (Renmuyou yu MZ Baogao, Report on Human wood-again and MZ), seems to be meaningless. But if readers understand that “木又” (muyou, wood-again) is a broken up version of the Chinese character “权” (quan, right), they can easily read “人木又” (renmuyou, human wood-again) as “人权” (renquan, human right). Together with “MZ,” short for the Pinyin “minzhu” (民主, democracy), this title means “report on human rights and democracy.” Posts written like this can thus easily escape being filtered by auto-censors. Although sensitive material hidden in these writings cannot be well-monitored by the automatic censorship machine, they can, however, easily be recognized by human censors. But, again, they sometimes do enable some Chinese netizens to breach the keyword censorship system and communicate sensitive information with one another.

A further kind of writing is popular in Chinese cyberspace, which I define as encoded writing – often combining parabolic expression and parody in a single text. For example, the following is a Sina Weibo post on 3 January 2015 by verified official account Xining Yesheng Dongwuyuan (Xining Safari Park):

171 Similar cases have happened on English websites as well, though their purposes may not be anti-censorship ones. For example, on 5 May 2014, a post on @NSACareers Twitter account reads “tpfcdlfdfdtte pccaplicrdt dklpcfrp?qeiq ihqolipgeodf gpwafopwprti ixndkqkpki krippacmpc dxkdcigcafmd vkipcadf. #MissionMonday #NSA #news” (NSACareers, 2014). This encoded piece of writing was decoded later as a recruit advertising “Want to know what it takes to work at NSA? Check back each Monday in May as we explore careers essential to protecting our nation.”
#Animal Science # Ancient dove – a kind of searching latent-bird headed into extinction within the borders of China. It originated in North America and was once active all over the word (particularly during the late 20th century and early 21st century). However, from 23 March 2010 onward, the ancient dove in China began to migrate on a large scale to a harbor in Southern China, and it soon disappeared entirely from Mainland China. This is a mysterious problem for biologists. [My translation] (Xining Yesheng Dongwuyuan, 2015a)¹⁷²

In order to understand this text, the meanings of several keywords should first be made clear. Since the Chinese Pinyin for ancient dove is “guge” which shares the pronunciation of “Google,” it thus functions as a covert reference to Google. Similarly, “searching latent-bird” (sousuo yinqin, search engine) again refers to Google. Google declared the withdrawal of its search engine service from Mainland China on 23 March 2010 and moved it to Hong Kong (referred to as the “harbor in southern China” in this post). This is a verified official account (by contrast to private ones, which are believed to be much freer to publish light jokes, unverified and unserious information) for Xining Safari Park, which is located in Qinghai Province in Northwest China. This account regularly posts information about animals all over the world with the hashtag “#Dongwu Kepu#” (Animal Science).¹⁷³ This jocular post began with this hashtag as well, and disguised its metaphorical criticism of the authorities’ banning

¹⁷² After being posted, this post was forwarded over 2,000 times in the first two hours. However, the original text has been deleted by this account due to the reason: “Planned to amuse everyone for a happy new year, never thought that it would spark quarrels! Just delete it. Sorry for any negative influence on you guys!” (Xining Yesheng Dongwuyuan, 2015b)

¹⁷³ Sina Weibo has copied the hashtag function from Twitter, but two symbols of “#” (rather than only one “#” as in Twitter) are used.
of Google. The whole post thus actually talked about Google and censorship, rather than “animal science” as declared.

Speakers often apply encoded writing to talk about sensitive issues such as political regime, human rights, and censorship itself. An esoteric Weibo posted on 11 September 2011 was forwarded over 100 times within the first 48 minutes. It mocked China’s human rights status quo. And this mockery was disguised by criticizing an imaginary fact that the U.S. Government detained, ill-treated and put into prison its actor Jim Carrey just because the actor tried to point out the number of victims, and their names, in the 9/11 Event. The Chinese prototype of this story is that artist Ai Weiwei was suppressed when he tried to account for the deaths of students and their names after the Sichuan earthquake in 2008. Another case is about the GFW. The Economist reported that in 2009 a science-fiction post circulated virally in Chinese cyberspace. This short piece of writing mocks the GFW project, suggesting a new project, GFW Turbo, which has become self-aware and runs out of control, banning almost the entire Chinese language. This parody imagines that in 2020 a National Anti-GFW Ministry will appear and this organization will add 2,000 more Chinese characters to meet the people’s ever increasing needs for means of production, only to find them censored within two seconds.

174 The deputy leader of Xining Safari Park later denied that this post was planned to make such criticism, but its meaning was obvious for readers (and because of critical comments following the original post, the account decided to delete it). In fact, this was not the first time that posts with similar content have existed on Sina Weibo – similar posts emerged as early as in August 2011. And Hudong Baike (Baike.com), China’s largest wiki site, even had a detailed explanation of “guge” (ancient dove) (refer to Hudong Baike, n.d.).

175 This case also reveals that nowadays not all official background media outlets (including their social media accounts) are standing fast along the party line.

176 For the original text, refer to the twitter post (pufei, 2011). My translation is as follows: “Today it’s the tenth commemoration day of the “9/11” event. Within the past ten years, American actor Jim Carrey was beaten by New York police several times and forbidden to leave the borders and got lost for 81 days because of his investigation of the names of victims, famous writer Stephen King was sentenced to prison for five years for his investigation into the numbers of victims.”

177 See The Economist’s article (Epstein, 2013). The post is titled “GFW de lishi” [The history of the GFW]. Most forwarded posts cite the website of the original post, (http://yizhituzei.blogbus.com/logs/41486880.html), but it is not available at the time of writing. See the GFW Blog for a re-posted copy (GFW Blog, 2009a).
It will hopelessly realize that in 2025 only one phrase will be left in the Chinese language, and that’s “minganci” (sensitive word).

The above modes of expression in Chinese cyberspace constitute a cyber genre of esoteric writing. Esoteric writing, a concept from Leo Strauss (1988), involves various parables and enigmas, as well as symbolic techniques (such as chrysanthemum flowers, brackets, boxes, circles and discursive techniques used in cyber slang). Under controlled circumstances, speaking out about sensitive issues in a straightforward and direct way may bring higher risk of being punished; esoteric writing enables Chinese speakers to encode their discussions and criticisms of sensitive issues and reduce such risks. This, of course, does not mean that esoteric writing cannot be understood by the censorship system: in fact, the censorship system is becoming smarter (with more human-censors getting involved in it) and is sometimes able to block esoteric texts. For example, the aforementioned case of a science-fiction post about the history of the GFW has been blocked in Mainland China. But esoteric writing can at least empower the speakers to escape the gaze of the censorship system for a certain period of time (until it is recognized by the censors), and helps to create an in-group culture within which resistance to censorship becomes possible. However, the relatively dark side of esoteric writing should also be noted. Writing in an encoded way can sometimes avoid censorship while, at the same time, it can also hinder an accurate meaning being communicated. This kind

---

178 On 3 June 2014, one day before the 25th anniversary of the 1989 Tiananmen Incident, a Sina Weibo user wrote that “These days, I want to read Leo Strauss very much and to learn his esoteric writing.” [My translation] The user, named Zhou Baosong (also known as Chow Po Chung), is a political scholar who is physically located in Hong Kong, and often writes posts about liberalism, neo-liberalism and social justice, some of which touch on the politically sensitive issues (such as June 4, Occupy Central Movement in 2014). It is quite interesting that Sina Weibo (and the Chinese authorities) puts up with him and has allow his account to remain active for a long time (with about 149,000 followers at the time of writing). The original text of this Weibo post is in traditional Chinese and is available at (B. Zhou, 2014).
of resistant discourses is more like an encoded discourse rather than a new kind of civic discourse. As will be discussed in Chapter Six, an esoteric interpretation (rather than an adequate interpretation) of a suspicious text is invited more often in online communication, which helps the popularity of conspiracy theories in Chinese cyberspace. However, this discourse does reveal subtle changes in broader social, cultural and political realms in China: in such a repressive environment, to challenge certain things that cannot be said is to challenge certain forms of power that are not supposed to be challenged. For users, interpreting a phrase differently from the authorities, using discursive guerrilla war to challenge keywords censorship, and feeling where the red line is after many attempts – all these form a meaningful and encouraging process.

**Discursive Weapons of the Weak**

The amount of research into Chinese internet discourses has gradually increased over recent years.\(^{179}\) While some scholars define internet discourses in terms of playfulness (e.g., Herold & Marolt, 2011, pp. 11-15; B. Meng, 2011), some others emphasize its political potential as an alternative way to “challenge the hegemony of official discourses” (Gleiss, 2015) or “encoded public spheres” (Rauchfleisch & Schäfer, 2015) or “a sphere for instances of repoliticization” (Nordin & Richaud, 2014). A further approach comes from an authoritarian framework and defines internet discourses as part of authoritarian deliberation (M. Jiang, 2010). Having acknowledged these empirical studies and theoretical assumptions,

---

\(^{179}\) According to Nan (2000, p. 37), “the flourishing of discourse of internet implies the beginning of internet history,” since discourse is the other soft but vital part of internet – compared with the physical or technical part (software, hardware, etc.). December (1993) posits this cultural phenomenon as a discourse culture that is based in computer-mediated communication (CMC) systems. As he supposes, this discourse “exhibits many characteristics of an oral culture.”
this section focuses on the dimension of control and resistance in Chinese internet discourses, and investigates the political influence of discursive weapons and discursive resistance from this dimension. It is widely acknowledged that the keyword filtering system has been kept on upgrading (Jedidiah R Crandall et al., 2013; MacKinnon, 2009a), with words going on and off the blacklist – some words may only be temporarily sensitive, while others may be durably sensitive. This dynamic means that discursive resistance to censorship is an on-going process as well. The political influence of discursive weapons and discursive resistance should be understood within this context.

Discursive strategies in Chinese cyberspace are much like what Scott has defined as “hidden transcripts” (1990) or “weapons of the weak” (1985). While public transcripts describe the open interaction between subordinates and the dominant, hidden transcripts refer to discourses and practices that are behind the back of the dominant and can often be termed as offstage, disguised, low-profile and surreptitious (Scott, 1990, pp. 2-5). According to Scott, no fixed frontier exits between public and hidden transcripts; in other words, because of the constant struggle between dominant and subordinate, some initially hidden transcripts may later become public. Hidden transcripts provide subordinate groups with a social space in which offstage dissent toward official transcripts may be voiced, and disguised and low-profile resistance may be possible. Scott emphasize the importance of hidden transcripts and bottom-up everyday resistance by proposing the concept of infrapolitics, which is seemingly far away from real politics but actually minimizes the risks its practitioners run and remain as a defense for the powerless (1990, pp. 200-201). Although Scott’s discussion of domination and resistance mainly concerns peasants in an agrarian (and pre-modern) context, this does not
prevent his findings being provocative and useful for discussions about control and resistance in a modern cyber context. In fact, some internet scholars have applied Scott’s theories to internet studies by defining hacking as “the weapon of the geek” (Coleman, 2013b) and emphasizing the importance of discursive strategies for digital activists in repressive contexts (Gleiss, 2015).

Along similar lines, encoded language and esoteric writing in Chinese cyberspace have increasingly become “discursive weapons of the weak,” which enable netizens to press, test, and probe the boundaries of the permissible, or, more generally, to resist and challenge the powerful censors and dominant discourses. Discursive strategies to bypass the censorship system may not be able to push for major changes in cyberspace, but they do help to create minor fissures in internet governance. The mockery and satirical criticism disguised in discursive resistance are usually at odds with official transcripts and dominant culture, and locate official discourses in a ridiculous position – tacitly mocking the official transcripts and counter-interpreting their potential meanings. As explained by Bakhtin (1984):

The author speaks through another person’s word…he [sic] introduces a semantic direction into that word which is diametrically opposed to its original direction. The second voice, which has made its home in the other person’s word, collides in a hostile fashion

---

180 However, I bear in mind the social, cultural and political differences of the contexts between then and now. For example, though Chinese authorities have tried hard to build an intranet and place close control on information flow crossing the border, it is impossible to keep every Chinese netizen under control. Various alternative choices are always available (as discussed in Chapter Two) for some Chinese netizens, which means that their resistant forms may differ from that of Malay peasants whose alternative choices were often very limited. (For instance, some Chinese dissidents may apply overt and direct resistant forms, which was often not the case for Malay peasants at that time). Another difference is the power holders (though Scott has not paid much attention to this end of the power spectrum): the power holders in current China are very adaptive in internet governance, which undoubtedly has a crucial influence in shaping the power relation between censors and netizens. For example, some resistant forms and activities (providing that they do not fundamentally challenge the system) may be potentially have a blind eye turned to them, and be used strategically as a covert form of social control.
with the original owner and forces him [sic] to serve purposes diametrically opposed to his
[sic] own. The word becomes the arena of conflict between two voices. (as cited in Talbot,
2007, p. 64)

The satirical interpretation of official discourses here can also be defined as pollution of
official transcripts. Inspired by Douglas’s (1984) analysis of purity, pollution and taboo,
polluting official transcripts and, as a result, polluted words (e.g., cyber slang), the idea of
“pollution” refers to a dissatisfaction with what the authorities try to push onto the people.181
Furthermore, with the constant struggles between authorities and netizens, censorship and
discursive resistance to such censorship (that is, pollution of the official discourses and
creation of new encoded hidden discourses) reveals a discursive guerrilla war in Chinese
cyberspace,182 surbverting the ideological order propogated by the authoirities.

It should be noted that the practice of polluting the official discourses may not directly
function as resistance to internet censorship, but it does empower some ordinary netizens with
a useful means, a weapon (of the weak), to challenge, at least symbolically, the authorities
(e.g., the publicity departments and departments responsible for internet censorship) and their
linguistic standardization attempts. The parody or satire behind these satirical words is
undoubtedly an embarrassing activity for the authorities. Counter-strategies from the
authorities do exist, which include not only upgrading the internet censorship system and
placing harsher control on internet expression but also placing closer control on the circulation

181 In this book, Douglas has made a fantastic interpretation of the rules of purity and pollution, and
examines what is considered as unclean in a culture, and what that culture strives to establish. This
interpretation seems still applicable in the internet context.

182 It is not sufficiently accurate to treat such a battle as “flame wars” in Dery’s sense (1994), since the
polluting activity here mainly targets official discourses and traditional culture ethos, and functions as a special
type of interaction between the powerful and the powerless.
of cyber slang and esoteric writing in other cultural spaces. A very recent case happened in November 2014 when the authorities of the SAPPRFT issued a regulation to forbid the usage of cyber slang in radio, television and advertising products, and urged relevant providers to place stricter censorship over their products. Moreover, cyber slang and esoteric writing have been defined by the authorities as a kind of irregular cultural phenomenon and these new discourses are viewed as endangering the purity of the system of Chinese characters and undermining the foundations of traditional Chinese culture (Y. Chen, 2014). Many schools in Mainland China are mobilized to launch “purifying” movements, forbidding pupils to use cyber slang in their assignments. Under such circumstances, using cyber slang itself reveals a resistant attitude to the ideologically-charged linguistic standardization.

To better understand the discursive battle and the discursive weapons of the weak regarding propaganda and internet censorship, a more general discussion about the ideological dimension of censorship in Chinese cyberspace is worthwhile. The Chinese authorities have long practiced their domination in the cultural and ideological field by censoring information that has crossed the line, and encouraging following the line. This, however, does not mean that the authorities are monolithic; factions always exist within this dominant system (as discussed in Chapter One). Taking internet governance as an example, some authorities have strong faith in censorship while others do not, and different levels of the censorship system may respond differently to a given situation. For example, censors at the front line (such as monitoring staff in internet companies) may suspect and know that a good portion of discursive resistance takes place behind their backs. But since these low-level censors are only responsible for censorship orders from higher-levels, they may choose to “turn a blind eye” to
some discursive strategies and some forms of discursive resistance if the latter do not obviously contravene their orders. Another reason is that too much cyber slang has been developed, which is highly scattered and low profile and thus impossible to censor. Increasing numbers of Chinese netizens take advantages of this bureaucratic problem in the censorship system and become even more creative in this discursive guerrilla war.

Although netizens perhaps well know that resistance from polluting and negating may result in more counter-strategies or even being forbidden, through scattered, disguised, low-profile and quotidian discursive means, netizens enact their vengeance on the censorship system, their resistance towards ideological control, and also their struggle to construct their identities in Chinese cyberspace, or in other words, “win small victories from larger, more powerful and ultimately determining systems” (Turner, 2003, p. 182). These discursive struggles, along with the technological struggles discussed in Chapter Three, reconstruct the power relation and power structure in Chinese cyberspace.
CHAPTER V. EXTENDING THE SYMBOLIC POWER

Encoded discourses represent not the whole picture but an indispensable part of symbolic weapons, which often involve other media forms such as images, audio materials and videos. This, however, does not mean that these images, audio materials and videos always apply brand new elements that have never been seen in encoded discourses; by contrast, much cyber slang, as well as the rhetorical elements it uses, has been greatly incorporated in resistant images, audio materials and videos. A few empirical studies have touched on the issue of ironic images (Mina, 2014) and spoof videos (Lugg, 2013; Voci, 2010) in Chinese cyberspace, using mainly case studies and situating them in contexts such as digital activism, internet memes, infotainment and “politics of visibility” (F. Yang, 2014). For these scholars, the prevalence of ironic images and spoof videos has been shaped by internet censorship, but little academic attention has been paid to how and why such forms may function politically as forms of resistance to internet censorship. Also, some scholars have tried to situate these forms within a broader theoretical framework, i.e. that of “symbolic power” (e.g., Tang & Yang, 2011), which is undoubtedly a good starting point, but since they often focus on a single media form or a single case, it may not be enough to suggest symbolic power whilst overlooking other forms and the interactions between these forms. Furthermore, rhetoric has been believed to play a significant role in internet resistance (Tang & Bhattacharya, 2011; G. Yang & Jiang, 2015); however, the specific role of rhetoric in the circulation of internet cynicism and the reproduction of powerlessness has rarely been discussed by existing scholars.
Based on case analyses, this chapter tries to provide a complex and nuanced understanding of symbolic resistance in Chinese cyberspace. Apart from discursive weapons discussed in the previous chapter, symbolic resistance has also been empowered by other weapons such as iconic weapons, audio and visual weapons and rhetorical weapons. Some Chinese netizens often apply multiple weapons simultaneously – rather than one single weapon – during their practice of symbolic resistance, but for the sake of convenience I discuss these weapons one after another. Five sections are included here. The first two sections focus respectively on iconic, audio and visual weapons of symbolic resistance, before discussing rhetorical weapons in the following two sections (one section deals with general online rhetoric such as parody, and the other deals with political silence as a rhetorical strategy). I conclude in the fifth section by discussing the power and limitations of symbolic resistance in Chinese cyberspace: on the one hand, such resistance may not be able to challenge the political status quo in a fundamental way; on the other, it does create fissures in the internet governance and help to form a cultural political space in which netizens can voice non-compliance and practice quotidian identity politics.

**Politicizing Images**

Dissemination of images in Chinese cyberspace has received gradually closer control since about the beginning of the new millennium (when new technological developments enabled images to be shared and spread more easily and quickly). The first relevant regulation was issued in June 2004 (titled “Self-Discipline Pact on Prohibiting the Dissemination of Pornography and Other Unhealthy Information on the Websites”), one clause of which called for rejection of pornographic and violent images in Chinese cyberspace. Periodic censorship
events have since been created by the authorities to purify the internet and fight against vulgar culture; for instance, in 2009 alone, two such censorship events happened: the launch of an “Anti-Vulgarity Campaign” to wipe out unhealthy information (including that carried on images) in cyberspace, and the attempt to promote Green Dam Youth Escort to guarantee a “greener” cyberspace (Faris, et al., 2009). Such actions may have some influence in disciplining Chinese netizens, but seen from the perspective of censorship of images, their influences are very limited, because compared with words and texts, images are not easily auto-censored and censorship work is heavily reliant on human-censors. While pornographic images are often relatively easily detected programmatically (though sometimes mistakes exist), politically sensitive images are harder to monitor by auto-censors. This provides some room for iconic resistance in Chinese cyberspace.

Two dimensions of iconic resistance

According to internet regulations, sensitive images in Chinese cyberspace mainly include two types – pornographic images and politically sensitive images. The resistant implication of online images thus, accordingly, can be understood from two dimensions – challenging the censorship of pornographic images and of politically sensitive images.

---

183 In the case of Green Dam Youth Escort, a research institute of the MPS engaged in developing image-recognition technology, but they seem to have failed to do so, at least so far (MacKinnon, 2009b). Many “healthy” images are treated by automatic censors as “pornographic” (B. Hu & Guo, 2009). Another phenomenon is the popularity of textual images in SNSs. Take Sina Weibo for example. Like its Western counterpart Twitter, Weibo has a word limitation for each post (strictly 140 Chinese characters). But Sina utilizes a technology of long micro-blogging (chang weibo), which enables users to publish a long article in the form of an image and overcome Weibo’s 140-character limit. Designers of this technology may not have realized that it could later be strategically used as a means of circumvention. By long micro-blogging, users are able to put politically sensitive information into a readable image which, however, is difficult for machine filtering crawlers to recognize. Although such sensitive images can be distinguished by human censors, the huge intensity of labor needed does not guarantee that every instance of these images will be monitored and filtered, and politically sensitive content can be spread to some degree.

184 The technological difficulty of image censorship is a worldwide issue. For example, Facebook was reported to ban breastfeeding photos from online profiles and received protest from irate mothers (Sweney, 2008).
Challenging the censorship of pornographic images

Though Chinese authorities have placed very strict censorship policies on online pornography, pornographic materials (e.g., sex images and videos) do find their way to circulate in cyberspace – via blogs, BBSs, Instant Messengers, SNSs, and P2P downloading sites (e.g., Bittorrent and Emule). ICPs and ISPs are also sometimes involved, in varying degrees, in circulating pornographic images, audio materials and videos, to gain web traffic. In fact, some adult websites (chengren wangzhan or huangwang) survive mainly on pornographic products.\textsuperscript{185} The rise of amateur pornography (Paasonen, 2010) means that many erotic user-generated images also appear and skirt the bottom line. Since Chinese authorities often begin censoring dissident ideas and other more widely political sensitive materials in the name of censoring pornography and violent information, the resistance against censorship of pornography is also sometimes politically significant. This resistance has been termed “erotic activism” or “sexual rebellion” (Jacobs, 2012, p. 16).

The wide online protest against the “Anti-Vulgarity Campaign” in 2009 is a good example of this. The authorities claimed that this action mainly targeted pornographic and violent information online, but in reality they extended the censorship to much less pornographic and violent information as well. In fact, many classic oil paintings of the Renaissance on Douban.com were treated by the censorship machine as vulgar and pornographic material.\textsuperscript{186}

\textsuperscript{185} An early example is the 99BBS case. 99BBS (jiuju qingse luntan), reportedly once the top pornographic website in Mainland China, was started in 2002 by a 19-year-old Chinese who lived in the U.S., with a host server located in the U.S. as well. At the peak time of this website, there were over 300,000 registered members, 6,000 vulgar and pornographic videos, over 100,000 pornographic images, and 20,000 vulgar posts. This website was raided by police during the special operation of “anti-vulgar and pornographic websites” in 2004, 11 members of the management team being put on trial a year later. (Guan & Li, 2005; Jacobs, 2010; Xing & Chen, 2005). Currently, the majority of Chinese pornographic websites (such as Caoliu Shequ, http://t66y.com), hosted overseas and targeted at Chinese users, have been blocked by the GFW.

\textsuperscript{186} According to its "About me" page, Douban is a Chinese website providing an exchange platform for reviews and recommendations on movies, books and music. Similar to Twitter and Digg, it is a "follower
Figure 3. Some Images from the Campaign of “Putting Clothing on Famous Paintings”

Clockwise from the top-left: The Source; Bouguereau’s The Birth of Venus; David; Liberty Leading the People. Source: Online open source

This campaign triggered a humorous bottom-up campaign called “anti-vulgarity, let’s put clothing on famous paintings” (H. Li, 2011, p. 79). The nude in Jean-Auguste-Dominique Ingres’s oil painting The Source, Michelangelo’s David and the woman in Eugène Delacroix’s Liberty Leading the People among many similar others (see Figure 3) have become “internet memes” (Bauckhage, 2011) and all were dressed by anonymous netizens. Shortly after this, a network” in which users can broadcast short messages to their followers (refer to J. Zhao, Lui, Towsley, Guan, & Zhou, 2011). With much UGC, it proves to be a popular and successful Web 2.0 website, particularly for some young people. Some topics in its discussion groups may approach the bottom line of the information control policy.
new virtual protest on Douban started and users there were called to “participate without making any statement and communicate with each other merely through eye contact.” 187

Another good example happened in May 2009 when the Chinese authorities made it mandatory for every new computer sold after 1 July in Mainland China to pre-install the Internet filtering software Green Dam Youth Escort or the setup files on an accompanying compact disc (see the notice on official website of the MIIT 2009). This software was believed to have cost the government at least ¥ 400 million (H. Li, 2011). Nominally, this filtering software aims to provide protection for young Chinese netizens and therefore keeps them away from violent, pornographic information. This “favor” provided by the authorities, however, has received huge criticism. Many people believed that this software would make monitoring every computer in Mainland China more convenient for the authorities. According to an article (B. Hu & Guo, 2009) from Southern Weekend, a high-profile market-oriented Chinese newspaper, this software seemed to be far from perfect, since it mistook images with large yellow marks for pornographic images; similar vulnerabilities have also been found in academic research (Wolchok, Yao, & Halderman, 2009). As resistance, Green Tsunami, counter-software developed to neutralize the Green Dam Youth Escort by an American-based company GIFC (as mentioned in Chapter Three), became freely available for those located inside the GFW. A female cartoon figure named “Lvbianiang” (Green Dam Girl) was created in an online animations, comics and games (ACG) fan community and then widely circulated in other online communities. With a “River Crab” logo on her cap and a red badge indicating ethical and moral discipline, this figure reflected strong yet disguised irony and skepticism.

187 “Communicating only with eye contact” refers to an ancient story in China. It means that in a closely controlled society the people dared not even to say hello to each other when they met each other, only communicating through eye contact.
Adult comics, cosplay shows, games and songs which took this figure as the main character, emerged afterwards. These cultural products, whether disguised or not, were once blocked from relevant search results by the top Chinese search engine Baidu.com. This mandatory act was ultimately unsuccessful (R. Deibert, et al., 2010, p. 278).

Bottom-up movements against the censorship actions in 2009 have helped two mythical creatures – Grass Mud Horse and River Crab (as mentioned in Chapter Four) – become basic elements of many iconic memes in Chinese cyberspace.188 Such iconic memes often target the censorship system. For example, on one image, the Green Dam Girl drags a Grass Mud Horse with a string tied on the latter’s neck, a metaphor of censorship and resistance. They also extend criticism to broader socio-political issues, as shown in another image that depicts a crab with three watches, a mockery of the ideological slogans “building harmonious society” (“harmonious” shares syllables with “river crab” in Chinese) and “Three Represents [sic]” (“three watches” is a euphemistic yet ironic alternative term for it). Another example is a photo of Chinese activist Ai Weiwei who is naked and with a Grass Mud Horse toy covering the central part of his crotch. In Chinese, the phrase of “the central part of one’s crotch” shares the same pronunciation with “Party Central Committee.” Performed together with the Grass Mud Horse toy, this performance thus means “Fuck your mom, Party Central Committee.” The above cases reveal that, erotic activism, challenging censorship of pornography at the outset, may achieve something different than pornography at the end.

---

188 There is no direct evidence to show that the authorities do not understand the satirical metaphor behind these memes and relevant cultural products, but they choose to let them circulate freely in Chinese cyberspace – a probable reason may be that such challenge does not erode the stability of the system in fundamental way and thus seems to be more tolerable. This is another case that may reflect the authorities’ adaptive control strategy (as discussed in Chapter Two).
However, we should not overstate the political influence of erotic activism. The Grass Mud Horse, for example, was later commercialized, using an alpaca as a prototype for this mythical creature (S. S. Wang, 2012). A search for “Cao Ni Ma” on Taobao.com reveals thousands of Grass Mud Horse toys for sale. This indicates that in Chinese cyberspace the political implication of a given case may be diluted by other factors that are involved afterwards; also, we should not assume that something politically significant in cyberspace will still be taken seriously by netizens in their offline lives (Nordin & Richaud, 2014).

**Challenging the censorship of politically sensitive images**

The political implication of an image in Chinese cyberspace can be fully revealed when it is used to carry politically sensitive information. Take a user-generated image of Jiang Zemin in 2011, for example. In that year, Jiang, previous president of PRC (in leadership 1993-2003), was rumored to be dead in Beijing 301 Hospital because of bladder cancer. Both bladder cancer and Hospital 301 soon became sensitive words in Chinese cyberspace, so did many other terms such as “jiang” (meaning “river” in Chinese). Netizens applied not only discursive means (as discussed in Chapter Four) to discuss this sensitive topic online, but also iconic means. A very popular image depicting a uniform hanging on a line quickly became viral. The

---

189 Jiang was in office when the Tiananmen Incident occurred, and many overseas dissidents believed that Jiang should be held responsible for it. This is partially the reason why he received huge attention from overseas dissidents and became a subject of heated discussion on both domestic and international SNSs. Since discussions about the private issues of top political leaders are sensitive in Mainland China, various euphemistic words have been created to refer to Jiang (as shown in Appendix C). As a retired leader who is now in his eighties, Jiang has been guessed to be in frail health by outside media. Periodical rumors exist and circulate in cyberspace.

190 Hospital 301, or PLA General Hospital, is reportedly the hospital taking care of both current and retired Chinese leaders. Thus much information about deaths or illness of leaders involves this hospital.

191 The euphemistic terms for discussing Jiang’s case include “xianhuang” (or xandi, deceased emperor), “naosiwang” (brain death, since Jiang was regarded as the head and brain of the party), “jiaobeng” (death of the emperor), “jiahe” (ride crane, meaning to pass away), “xiqu” (go west, to pass away), “shangchuan” (aboard a ship, meaning to pass away), “yongchuibuxiu” (live forever, another euphemism for dying), or “guaile” (hanged, died).
uniform is an ironic metaphor for Jiang, since he often dressed himself up with a high belt, while “hanging” in Chinese has the meaning of “die” (gua). So this image is a kind of indirect expression of “Jiang has died” (also see Branigan, 2011). Another popular image is a toad-like person lying down with a bound up bladder, which indicates death due to bladder problems (see Figure 4). These two images were soon blocked by the GFW, but other similar images kept on appearing and circulating. This strategy enables netizens to speak out in repressive situations, since oblique messages with images can survive longer than those in text, as some scholars have found (e.g., Zuckerman, 2014).

Figure 4. Esoteric Images Containing Ironic Meanings

![Figure 4. Esoteric Images Containing Ironic Meanings](image)

Left to right: A uniform hanging on a line; a toad-like person lying down with a bound up bladder; an amended version of Munch’s The Scream. Source: Online open source

The use of metaphorical images to resist internet censorship is widely seen in other politically sensitive situations. For example, in order to show his or her concern about the 24th anniversary of the Tiananmen Incident, a netizen shared the Norwegian painter Edvard Munch’s well-known work The Scream (1893) with an amendment of two pieces of red tape crossed over the agonized figure’s mouth (refer to Pingaotulou, 2014) (see Figure 4). It is a euphemistic strategy for speaking the unspeakable. Similar iconic strategies can also be seen in a euphemism for “tank man” – netizens creatively replace the tanks with big yellow ducks.
or other popular images to camouflage the original picture (Rauchfleisch & Schäfer, 2015). Under such circumstances, images become a symbolic weapon to challenge the authorities. Mainly because of this reason, many international image and video hosting websites have received blockade by the GFW. For example, Flickr has been periodically blocked since June 2007 – a tricky timing implying the anniversary of the Tiananmen Incident – and has been completely blocked in Mainland China since July 2014.

**Political cartoons in Chinese cyberspace**

Chinese netizens participate in iconic resistance not only by accessing and sharing sensitive images but also by creating and recreating images which sometimes cross the line set by the authorities. The technological developments (e.g., cheap digital camera, easy-to-use image processing software and various photo-sharing websites) and do it yourself (DIY) culture help this to happen. Plenty of DIY political images are circulating in Chinese cyberspace. Political cartoons are a significant subset that is worthwhile of detailed analysis. Many political cartoonists are (or were) active in the GFW; a complete research of these cartoonists and differences between them is beyond the scope of this research. Here I take a typical cartoonist, Rebel Pepper (*Biantai Lajiao*), as an example and do some analysis of his works for clarification.

Rebel Pepper is the screen name for Wang Liming, a Chinese political cartoonist who began his satirical drawings on burning socio-political affairs in 2006. His drawings, often full of irony and black humor, have gained him a high profile on domestic SNSs such as Tencent

---

192 Some political cartoonists such as Crazy Crab (Fengxie), like Rebel Pepper, focus mainly on sensitive issues and are banned within the GFW. While many others touch on issues less sensitive and survive in the GFW, such as Niguang Feixing (fly against the light), Li Xiaoguai, and Wu Junyong.
Weibo and Sina Weibo. His accounts on the latter sites had, respectively, 550,000 and 340,000 followers before they were blocked by the authorities. In August 2014 when he was paying a visit in Japan, his Chinese social networking accounts became inaccessible, including relevant search results about him on Baidu.com and even his e-shop at Taobao.com. He declared his being blocked by the Chinese authorities on his Twitter account (see remonwangxt, 2014).

Later, Strong China Forum published an article to fustigate Rebel Pepper and fiercely criticize his attachment to Japan and Japanese culture, describing him as a traitor (Zhangyan, 2014). He decided to live in exile in Japan after this.

Figure 5. Three Cartoons by Rebel Pepper

Anti-clockwise from top-left: Mockery of the CCP; Hong Kong pro-democracy protest in 2014; Mockery of internet censorship. Source: Rebel Pepper's Google+ page

---

193 Using party organs to bring shame on dissidents is a very common strategy for the CCP’s social control. Similar cases include the Li Chengpeng case in 2014 (see Chapter One for more detail).
Rebel Pepper has long practiced political satire in his cartoons. This can be seen in a cartoon he drew in 2011 to mock the Chinese government’s bus donation to Macedonia. This picture, with a pupil in front of a line of three yellow buses, may remind readers of the tank man in front of a line of moving tanks in the Tiananmen Incident in 1989. According to the posts at his personal webpage on Google+ where most of his political sensitive comics can be found, he seemed to have tried many times to publish sensitive images on Sina Weibo but failed (see Rebel Pepper, 2011). International SNSs such as Google+ and Twitter have, since 2011, become his alternative platforms on which to publish politically sensitive cartoons, the themes of which include human rights, freedom of expression, internet censorship, democracy, one-party regime, corruption and the Tiananmen Incident, among others (China Digital Times, n.d.-a). Blockade and exile may have had some influence on his style of drawing. After this, he was reportedly to decide that he would throw away the esoteric way of drawing since it could not avoid being blacklisted (Gelan, 2014). Further evidence of the recent change in his style of drawing is the fact that many of his recent cartoons directly mock the current Chinese president Xi Jinping and China under his control (see Rebel Pepper, n.d.), which was unusual before. Moreover, on Twitter, he has since published every original post in traditional Chinese (which is still in use particularly in Taiwan and Hong Kong). Taking into consideration his Mainland Chinese background (where simplified Chinese is used), rejecting the use of the official language of Mainland China is no doubt a political choice, showing his antagonistic yet ridiculing attitude towards the CCP. He builds a connection with other dissidents, not only by tweeting and re-tweeting content from other dissidents who also use Twitter, but also by drawing relevant cartoons to give symbolic support to those who have needed it. Examples of
the latter include supportive cartoons of Chen Guangcheng (the blind human rights lawyer discussed in Chapter Four), Liu Xiaobo (the 2010 Nobel Peace Prize winner) and artist Ai Weiwei, among others. Such activities, having crossed the line set by the Chinese authorities too often, resulted in his being entirely blocked within the GFW.

The case of Rebel Pepper reveals the depth and reach of iconic resistance in Chinese cyberspace. Though his cartoons are now publicly unavailable in Mainland China, for some Chinese netizens who are physically located overseas as well as those located in the GFW with the ability to bypass the firewall, his works are still accessible. He still draws political cartoons to criticize Chinese issues and publishes them on his overseas SNS accounts. At the time of writing, his Google+ account has gained over 50,000 followers and over 15 million views; his Twitter account has attracted 114,000 followers.

**The political potential of images**

Images and words make sense through different systems; as discussed above, images sometimes help users to bypass the censorship system where words fail, or at least, are an important supplement to discursive expression. Iconic weapons have – at least sometimes – enabled some Chinese netizens to circumvent censorship of pornographic materials and politically sensitive expression. The political potential of images, as revealed in both the Grass Mud Horse and the Rebel Pepper cases, is often cast beyond internet censorship issues and on to broad socio-political issues. Despite the increasingly strict control over iconic expression, resistant images find their way, circulating either underground or in overseas media outlets, as political memes, which helps to downplay “the importance of what the government considers significant and reveal the stupidity and hypocrisy of official culture” (H. Li, 2011, p. 81).
An emergent dialogue centered on image may prove to be a “rewarding public sphere,” as Zuckerman finds (2014), but with censorship and resistance often becoming involved, it is likely to be a very different space for expression than those in the Western sense. The political power of images can be seen particularly in online activism (Mina, 2014), such as environmentalist activities, grassroots protests, pro-democracy movements, feminist activities and erotic activism. From this point of view, besides discourses and texts (as discussed in Chapter Four), images also help to add an important dimension to the political power of symbolic resistance in Chinese cyberspace. However, it should also be noted that most of the time, iconic resistance, similar to other forms of resistance in Chinese cyberspace, may not always be collective and overt, but scattered and low-profile. This feature has decided that, on the one hand, iconic resistance may not be able to really erode the efficacy of the censorship system since the system also learns and adjusts; on the other hand, it helps erode the legitimacy of censorship system and makes complete censorship impossible. When one image is censored, new images appear, and the “cat and mouse” game continues. We should always bear this in mind when considering the political potential of images in Chinese cyberspace.

**Historicizing Audio and Video Weapons**

Audio and video forms can be used for resistant purposes as well. As with resistant images, the resistant meaning behind audio and video materials is difficult for auto-censors to recognize. If the censorship system wants to block a piece of sensitive audio or video

---

194 A recent case happened in Hong Kong in 2014. Since during the movement, umbrellas were used as self-defense tools against pepper sprays which had echoed the feature of this movement — “Occupy Central with Love and Peace,” umbrellas became one of two symbols of this movement (with yellow ribbons the other symbol). Umbrellas showed the protesters’ non-compliance with the Beijing authorities; moreover, they functioned as an emotional bond between participants and may have helped to mobilize more people to participate in the pro-democracy movement.
materials, they will have to form an even bigger army of human censors, which makes “building an ideologically clean cyberspace” unrealistic, at least currently. Most of these resistant audio and video items use cyber slang, and esoteric writing, discussed in Chapter Four, to generate resistant meanings. Their creators are often non-professional (that is, not traditional media professionals), with most creators anonymous – or disguised under screen names – and nondescript, and only a few becoming famous in cyberspace. This section approaches the audio and video weapons of symbolic resistance from a historical perspective. It tries to make clear how technological developments and DIY culture shape some Chinese netizens’ ways of using audio and video forms for resistance purposes, and how creators of audio and video products tactically cover their resistance in order to avoid being caught by the censors.

New technological developments of hardware, software and platforms have played significant roles in making audio and video forms useful strategies for anti-censorship purposes. In the field of hardware, digital recording devices and cameras are becoming cheaper and more popular, which means a netizen can easily shoot his or her own videos and generate audio clips. Plenty of software is also available nowadays to help a beginner to do audio and video editing and remixing relatively easily. New technological developments also function as an accelerating power for the flourishing of various audio and video platforms, enabling prosumers to share audio and video content and to form virtual communities for like-minded netizens. For example, in around 2004, a new kind of blogging technology named podcasting (Boke in Chinese) appeared and became popular. It enabled podcasters to post audio clips (unlike traditional bloggers, who use texts and images to make posts) either on
their own personal servers or on commercial websites, discussing various issues (e.g.,
entertainment, news-related clips, and comments on socio-political events). Meanwhile,
some video-sharing websites have become increasingly popular in netizens’ daily lives, such
as Youku.com (started 2003), Tudou.com (started in 2005), 56.com (started in 2005), and
Aiqiyi (iqiyi.com, started in 2010 and formerly known as Qiyi). These podcasts and video-
sharing sites have helped to cultivate an active audiovisual culture, in which both existing
audio and video content and UGC are likely to be accessed and shared.

The fast development of mobile and WiFi technologies, as well as the increased
affordability of internet connection fees, also encourages Chinese netizens to access audio and
video content more conveniently and easily. According to the half-annual report by CNNIC
(2015), 71.9% of Chinese users view internet videos via their mobile phones; users tend to
watch short videos via mobile phones, and longer videos via computer terminals. Chinese
authorities began to take close control of online audio and video content as early as 1999, and
since then at least seven relevant regulations have been issued (see Appendix B). Upload and sharing pornographic, violent and politically sensitive videos has since been
illegal in China. However, this risky business does not prevent some internet companies from

---

195 One example is Antiwave (www.antiwave.net), a podcast created by two netizens, Pingke, a former
radio presenter, and Feizhu (flypig), a former journalist. Producing Antiwave radio clips was only their part-time
job (which was done after work) and it was active between 2005 and 2007. The podcasts mainly use the
rhetoric of humor (or, to use an internet phrase, egao) to make comments on sensitive topics, including
homosexuality, Sino-Japanese relations, among many others. Although the two creators insisted that they were
not so interested in political issues, they did produce many clips relevant to politics, particularly criticism of
party-owned media. They carefully chose their topics and the wording of these topics in order not to directly
challenge the authorities. The main characteristic of Antiwave was that it functions as a resistance to traditional
radio programmes (which are under strict control of the CCP), as indicated by their website slogan “ALL RADIOS
GO TO HELL!” (The original text is in English.) Antiwave won the Deutsche Welle Global Best Podcast in 2005
(Luo, 2008).

196 Youku and Tudou were merged in 2012 into the Youku Tudou Inc., which reportedly had 500 million
active users.

197 Other means have been used to deal with net pornography as well. As Jacobs (2007) has observed, “the
Guangdong public security department has agreed with local telecommunications companies to pay a reward of
up to ¥ 2,500 ($ 309) to people who report on any type of netporn traffic” (p. 149).
being eager to do it (Jacobs, 2012, p. 31). Besides the pornographic websites mentioned in the previous section that are involved in distributing sex videos, some freely-provided online streaming media players also provide convenient conduits for such materials.198

A user-generated culture has become prevalent in Chinese cyberspace; particularly the online youth culture and DIY culture which values poking fun at those in powerful positions (such as the authorities and the elite) via various media forms. A new term, egao (spoof), has been used to describe this emerging phenomenon (H. Gong & Yang, 2010). The first famous egao product appeared in 2005 when a netizens named Hu Ge poked fun at a domestic commercial movie The Promise (2005, directed by Chen Kaige). This 20-minute long spoof video, titled Yige mantou yinfa de xue’an [The bloody case over a steamed bun], has remixed clips from the original movie, Fazhi Zaixian (The Law on the Line, or China Legal Report, a TV program on CCTV) and revolutionary songs from the Maoist era, to produce a satirical yet funny narrative different from the original movie (X. Liu, 2010; Lugg, 2013; Voci, 2010). Since this case, numerous egao videos have appeared online and formed a prominent egao phenomenon, represented by works of Hu Ge, Houshe Nansheng (back-dorm boys, named after the Backstreet Boys), Laoshi (always wet, a homophone of “teacher” in Chinese) and Jiaoshou Yixiaoxing, among others.

198 Kuaibo is a good example of this. Kuaibo, started by Wang Xin, was a Shenzhen-based online streaming media company and active during 2007-2014. It provided its main product QVOD, once a notorious video piracy app in China, freely for Chinese users via which videos were allowed to download while being watched. This company has made profit mainly from online advertising. Many pirated materials, as well as sensitive materials (such as pornographic, violent and politically sensitive materials), can be freely downloaded and shared between users. Kuaibo’s office was raided by the police in 2014 during a campaign of “eliminating pornography and illegal publications” in Chinese cyberspace. Later, a punitive fine of ¥ 260 million was issued to Qvod by the authorities and its several main staff were arrested. An interesting thing is that when Wang Xin’s wife registered her Weibo account (with the handle “kuaibo wangxin taitai”) in June 2015, she soon attracted over 200,000 followers, and, at the time of writing, her first post was forwarded 3,799 times, with 3,6468 comments and 5,6079 likes; the majority of comments showing support of Kuaibo and its service.
Much egao content is pure entertainment, but a certain number of items poke fun at hard socio-political issues as well. Again, taking Hu Ge for example, his later works extend criticism and/or mockery to issues such as the Spring Festival rush (the traffic problem during Spring Festivals in China), the North Korea Regime, and CCTV (often be mocked as CCAV, see relevant discussion in Chapter Four). Chinese internet censorship has also become a target of his spoof video criticism. In a 2010 video Dongwu shijie: Zhaiju dongwu [Animal world: Otaku animals], he drew an ironic analogy between Chinese netizens and animals, and argued that too much protection (implying internet censorship) from the human-beings (implying the Chinese authorities) had some negative influence on such otaku “animals.” It may be because of this indirect criticism that this video is still accessible within the GFW. Egao audio clips and videos provide a vehicle for “both comic criticism and emotional catharsis” (H. Gong & Yang, 2010) and help to push the boundaries of what can be said and what cannot – only if they push in a tactical way, as shown in the Hu Ge case.

Although not all the user-generated audio clips and videos are targeted at challenging censorship, it is quite normal for users to add a few ironic words and phrases, to use a little bit of satire, parody and black humor, and to show their non-compliance with the authorities (and the ideology being propagandized) here and there. This can be revealed in fan communities of currently popular foreign TV dramas and movies. The fans voluntarily and collectively produce Chinese subtitles for foreign cultural products and make them understandable to ordinary Chinese audiences. These Chinese subtitles often provided loose translations, with politically sensitive phrases sometimes randomly appearing (Q. Wang & Guo, 2014). This group of translators are not only consumers of Western popular cultural products but also
foreign-language-savvy themselves. Their funny yet satirical style of subtitle translation is quite different from the serious (and often censored) way the officials translate imported movies and TV dramas (J. Li, 2012). The ordinary audience may smile knowingly and share the covert, ironic implication behind such alternative subtitles. The existence of such grassroots translators does function as a challenge to official translators as well as censors (B. Meng, 2012; N. Zhou & Wang, 2015) and become a kind of “fan activism” (W. Zhang & Mao, 2013). Though the authorities try to control the emergence of alternative subtitles in Chinese cyberspace – for example, as early as in 2006, some subtitle translation websites were shut down (Hsiao, 2014), and in a recent case in November 2014 SAPPRFT shut down two subtitle websites under the name of copyright protection (L. Lin, 2014) – it seems unrealistic to have full control of these sub-cultural groups, subtitle websites keeping on appearing under new host servers.

Along with the development of P2P sharing technologies (e.g., torrents), an increasing number of sensitive audio and video materials circulate via interpersonal file-sharing method (rather than being posted publicly on a video-sharing site which can easily be censored). It is really hard for censors to clean such materials completely. The recent cloud-data storage technologies make censorship of such material even more difficult. A new form of P2P video website, termed “danmu wangzhan” (bullet-curtain websites), has recently become popular in Chinese cyberspace. As the name suggests, these video websites allow audiences to communicate on screen in sync with videos as they play. The comments from audiences fly

---

199 For example, when I did my bachelors degree in a university in Beijing about ten years ago, maze.com was quite popular amongst university students. After registering on this website, one could search and freely download many copyright materials. Also, one could find many sensitive materials, such as videos about the Tiananmen Incident in 1989, negative stories about the leaders, as well as pornographic materials. With more video-sharing websites having emerged, this situation does not change too much even today.
across the screen like bullets. AcFun.tv and Bilibili.com are two most popular Chinese bullet-curtain websites, which their fans call A Zhan (Forum A) and B Zhan (Forum B) respectively. The Figure 6 is an example of a screenshot of Interstellar (2014) on A Zhan. The white Chinese characters flying across the top of the screen are comments generated by audience members.

Figure 6. A Screenshot of Interstellar (2014) on AcFun.tv

Flying comments can provide audiences with much more fun beyond the narrative of the movie itself, since the comments often vary greatly, from mainly those relevant to the video, actor and actress, to relevant themes revealed in the video and even something very different. The censors may have realized that it has also become easy for some unwelcome contents to slip out to the public, but they seem to have no proper way to take such comments down, at least not yet. For example, the word circled in Figure 6 is “天朝” (Tianchao, Celestial Empire), an ironic phrase referring to Mainland China under the control of the CCP (as discussed in Chapter Four). Many similar ironic expressions and sensitive topics randomly occur in these flying comments.

---

200 Those who cannot bear this bizarre and distractive experience of viewing a video can click a button to turn off the bullet-curtain function and enjoy a “clean and pure” screen.
Though often these resisters have to choose their tones and narratives carefully to avoid being blocked by the censors, under some extreme circumstances, they produce audio and video clips directly mocking and challenging the censors – a kind of “carnivalesque resistance” (a concept from H. Li, 2011, p. 79). In 2009, when the authorities launched a nation-wide movement “purifying the internet” which actually closed down lots of popular websites, netizens created various audio and video items relevant to “Cao Ni Ma” (Grass Mud Horse) to show their anger towards the censors, such as Malegebi shang de Caonima [The Grass Mud Horse on the Mahler Gobi] and Caonima zhi ge [The song of Grass Mud Horse].

In the narratives of these videos, Grass Mud Horses have the appearance of alpacas, being gentle, courageous and tenacious; they feed on grass. “Wo Caonima” (literally, Crunching Grass Mud Horse, but actually meaning “I fuck your mom”) and “Kuang Caonima” (literally, Crazy Grass Mud Horse, meaning “fiercely fuck your mom”) are two typical species of this mythical horse. These horses are fighting with He Xie (River Crab) on the Mahler Gobi for grass, revealing an imaginative battle between the repressed and the authorities. The popularity of Grass Mud Horse and other relevant audio and video items provoked responses from the authorities. The SARFT (now the SAPPRFT) issued a notice in 2009, prohibiting 31 categories of online audio and video content, including violence; pornography; terrorism; and content that might incite ethnic discrimination, hatred, and undermine ethnic unity and social stability (H. Li, 2011, p. 79). However, this is never the end of the story. Netizens keep on

201 In Chinese, Mahler Gobi is also a euphemism for an obscene phrase which means “your mom’s cunt”. These audio and video materials are available on YouTube (see ESATUTUBE, 2011; ideacm, 2009) and shared virally elsewhere on the internet. Stuffed toys and other merchandise, observed Li (2011, p. 79), were also produced for Grass Mud Horses.

202 As noted in the previous chapter, both “River Crab” and “harmony” share the pronunciation of “hexie” in Chinese. River Crab functions as a hidden mockery of the official ideology, directly and obviously “the building of a harmonious society” in the Hu Jintao’ era. And since these river crabs are portrayed as wearing three wristwatches, it also mocks the “Three Represents” in Jiang Zemin’s era.
periodically challenging the censors. The authorities themselves often become the target of online satire.  

As concluding remarks, two issues should be noted. First, although high-profile resisters (e.g., Ai Weiwei, a dissident artist who once produced a video about “tofu-dreg schools” in the 2008 Sichuan earthquake and human rights) may easily be noticed by the authorities and their works banned online, low-profile resisters, if they utilize scattered, low-profile strategies, may not easily be caught or get into trouble. These tricky, scattered and low-profile audio and video weapons function as minimal power for the netizens, which enable them to challenge the dominant group (including censors), most of time covertly yet sometimes overtly. The existence of such weapons guarantees the powerless a minimal space of freedom. Second, audio and video resistance to censorship can be divided into two types: conscious resistance and unconscious resistance. While conscious resistance happens when netizens are aware of the existence of censors and of how to bypass them or challenge them, as shown in the Grass Mud Horse case, unconscious resistance is just as likely to be produced by expressing dissatisfaction and anger, or listening to illegal radio stations, sharing sensitive audio and video materials, and laughing knowingly about satirical images or egao videos – censorship itself tends to make unconscious resistance a conscious choice.

203 A recent case happened in December 2014. A Chinese historical television drama, The Empress of China (2014), was pulled off the air after the female characters appeared on screen showing cleavage (which is treated as sexual content by the authorities). It soon returned to the screen, this time showing only the actresses’ heads. Netizens responded satirically by generating videos to poke fun of the censors’ overreaction and stupidity.
Rhetoric of Symbolic Resistance

Symbolic resistance in Chinese cyberspace has utilized various rhetorical means, such as parody, irony, travesty, black humor, satire, grotesquery, and insinuation. Messages are more likely to be spread if they incorporate some rhetorical means, and are able to invite more participation and amplification. Many cases discussed above involve some kind of rhetoric; in fact, some scholars argue that humor and parody are two characteristics of Chinese cyberculture (Poell, et al., 2014; Voci, 2010; Wallis, 2011). Rhetorical means empower symbolic resistance not only because they help to form critiques (see Boler, 2006; Tang & Bhattacharya, 2011, p. 11) but also because they generate emotional bonding for all participants (such as knowing laughter among users) (B. Meng, 2011, pp. 33-51). Mere laughter (or more generally, humor) may not produce political meaning, but when it involves upsetting the established order, it becomes “a tiny revolution” (Orwell, 1968, p. 1). The political meaning behind many popular resistant memes in Chinese cyberspace such as Grass Mud Horse can be understood from this point of view (e.g., H. Li, 2011, p. 80; Mina, 2011). Online rhetorical means such as satire can be read as a “symbolic power” (Tang & Bhattacharya, 2011, p. 11), which facilitates the grassroots to create and spread satirical ideas, to release and stimulate an enormous reserve of public wit and wisdom, and potentially to generate a chain of related satirical work which can create a satire movement and subject power to sustained shame and ridicule. These rhetorical strategies may vary from one another in nuanced ways, but many of them can be understood from parody, a conjunction of various rhetorical means. In fact, parody is the main rhetoric means of symbolic resistance in Chinese cyberspace. In order to make this point clear, here I analyze some cases.
In late 2007, CCTV (representative of official media in China) produced several programs on “eliminating pornography and illegal publications” in cyberspace. In one of these programs, the reporter from CCTV interviewed a pupil about her attitudes towards online pornography and violence. The teenage girl replied that “I once searched for something online, a browser window popped up, very erotic very violent – I quickly closed it.” The public did not believe that “very erotic very violent” came from a pupil’s mouth – it simply did not match her age and the pupil was believed to be manipulated into saying this. “Very erotic very violent” soon became a great catchphrase and served as a scorching satire on the authority and credibility of CCTV. Considering the close relationship between CCTV and the Chinese authorities (e.g., Latham, 2000, 2009), this program was believed to be a mobilization for a coming campaign to purify the internet. Terms like “very erotic very violent” became symbols of the wider internet resistance to censorship. The rhetorical means behind this case is very interesting – “very erotic very violent” is from the existing text, which reveals a kind of parody in Bakhtin’s (1984) sense:

The author speaks through another person’s word…he [sic] introduces a semantic direction into that word which is diametrically opposed to its original direction. The second voice, which has made its home in the other person’s word, collides in a hostile fashion with the original owner and forces him [sic] to serve purposes diametrically opposed to his

---

204 In another program of CCTV in 2009, a reporter interviewed a university student about his thoughts on Google China’s erotic websites. He said that “… one of my schoolmates was curious about such things and often surfed pornographic websites. For a long period of time, he was very upset. Then the government promoted a cleaning movement on such websites, he could not surf and became good for a while. But when he found via Google he could access such websites, he reverted to type.” The interviewee was confirmed to be an intern in CCTV during the launch of the program. Again people doubted, criticized and mocked the objectivity of CCTV. “Upset” became another catchword in Chinese cyberspace.
[sic] own. The word becomes the arena of conflict between two voices (as cited in Talbot, 2007, p. 64).

By reusing the discourses from the first voice in a very satirical way, the second voice challenges the meanings of these discourses or makes them fight against their original purpose, and thus corners the first voice in an absurd situation. A major premise of such rhetoric is that the second voice is able to recognize the contradictory dimensions within the text of the first voice. Based on this, the second voice thus gains the possibility to dismantle and dismiss the first’s castle of meaning. Bakhtin’s differentiation between two voices within the practice of parody is a provocative starting point here, which means that all kinds of monologue are excluded from the field of parody. Parody, of course, deals with at least two voices. It cannot exist in the one-dimensional discursive system, since there is no space for any alternative voice and the followers may not think critically about what they are following. In this regard, the existence of parody, firstly, signals a break within the dominant discursive system – this break provides some living spaces for an emerging sub-discourse which can challenge the former. Secondly, the existence of parody also suggests that there is an ideological enlightenment among the practitioners of parody. Because of this enlightenment, a new kind of idea is cultivated and turned into a weapon with which to uncover the hypocrisy of the dominant ideology which was represented by the dominant discourses. The conflict between two discourses is fundamentally the conflict between ideologies. By focusing on phrases within the official text, parodying them and laughing at them, the users create and enlarge the fissures in the dominant ideology.
A similar rhetorical strategy is also seen in social events. For example, in 2011 two high-speed trains were involved in a pileup, 40 people eventually died, and over 200 people were injured. This tragedy caused anger towards the authorities and their attempts to sweep away relevant discussions online. When Wang Yongping, spokesman for this disaster, was asked at a press conference “why was a little girl found alive after the government claimed that there were no life symptoms at the scene and the rescue work was abandoned?” He answered that “It was a miracle.” Early the day following the accident, the authorities sent for excavators and dug a giant pit. The carriages were cut and crushed before burial in the pit. Some journalists questioned whether there was an attempt to cover up the truth. Wang responded that the situation at the rescue site was complicated. “Underneath is mud, very difficult to rescue, so they buried the train head and covered it with soil, mainly to facilitate the rescue work.” Furthermore he added, “Their explanation given is this - you believe it or not, I believe it anyway.” But the public were not satisfied with such an explanation; they showed their disbelief by frequently quoting this sentence, “it was a miracle…you believe it or not, I believe it anyway” – again, tactical resistance from the inside of the official text and a challenge to the authorities. This sentence soon became an internet meme. The large-scale circulation of such internet memes create a public pressure on relevant government departments, and becomes an indirect (or sometimes covert) way to find out, and speak for, the truth. From this point of view, parody is not only used as an oppositional reading of the texts, but furthermore, as a means of deconstructing the official texts, or even a powerful means of social critique.

205 My translation. For the original dialogue please refer to The Chinese News (2011). What also should be noted is the use of the word “their” in Wang’s answers. By using the personal pronouns of “their” and “I,” the unspeakable contradiction the spokesman tried to avoid became collapsed. He unconsciously distanced himself from the system, which is likely to suggest the schizophrenic status quo of the officials who work for the system.
As discussed in the previous sections, not only texts but also other forms (such as images, audio and video forms) have become battlefields of resistance. This has provided a wonderland for the circulation of parody and other online rhetorical means. Plenty of UGC features such online rhetorical means, often putting the censors in embarrassing situations. This kind of resistant rhetoric can be fully explained by the aforementioned *egao* phenomenon, which often involves the rhetoric of parody, black humor and satire. Although *egao* products, such as “wicked fun” movies in Voci’s sense, are often more nonsensical than satirical and thus appear quite apolitical and harmless in the eyes of the censors (Voci, 2010, pp. 105-115), because both the encoding and the decoding of these spoofs involves a wide array of critiques of social political issues, they share with medieval carnivals an anti-establishment spirit (B. Meng, 2011, pp. 33-51). Not all *egao* products (including mash-up images, texts and videos which are rapidly proliferating in Chinese cyberspace) are consciously introduced for the purpose of challenging the censors, but they certainly have this effect.

The practice of parody and other internet rhetorical means helps users to build emotional bonds and identity politics. Seen from the perspective of subculture, these rhetorical means function as “tit for tat” from the subculture towards the dominant culture. They extend the possible meanings of a given phrase. By holding the battle field in the enemy’s domain, that is, the products of the dominant culture (texts, images and beyond), they hit the weak part of these products, and are likely to deconstruct what the products try to construct. For the subculture, by using parody and its like means, one does not need to originally build a product oneself in order to fight against the dominant culture (including censors), one just needs to
incorporate some parts of products of the dominant culture, and make them a friendly rather than a hostile weapon for resistant purposes. By using such rhetoric, participants show their tacit non-compliance with the dominant culture (such as knowing laughter) and even perform their symbolic resistance (though at a relatively safe distance) to the latter.

**Silence as Political Rhetoric**

In Chinese cyberspace, many sensitive topics have been swiped away by the censorship system in the first instance. Even if the system has failed to stop the circulation of sensitive topics, it can easily succeed in preventing netizens from making public comments afterwards. Because of such manipulation, when a sensitive topic appears, it seems that the majority of netizens are remaining silent; they are kept quiet by the authorities. This manipulated (and passive) silence does not prove that Chinese netizens are all disinterested in discussing political issues, or even that they are apolitical (though some of them may be like this). As has been discussed in the previous chapters, it is quite normal for some Chinese netizens to find technological and symbolic ways to breach the control system. Despite all these facts, we should bear in mind that what has been revealed in Chinese cyberspace is just a tiny part of the whole story, and what has not been publicly revealed is equally important for our understanding of Chinese internet politics here – silence is “the most powerful implicature” (Bartoli, 2009, p. 83).

---

206 Though, of course, when we analyze this rhetoric more closely, we may probably realize that, much like the unwilling positive function of resistance to a dominant system, in Chinese cyberspace, parody, seemingly a deconstruction of that system, is basically and unconsciously an ironic affirmation of it. It needs to be noted here that the subversive or resistant dimension of rhetoric should be understood within the cultural political context in which such practices are embedded, and in the context of passive resistance (as discussed in the coming section).
Silence in Chinese cyberspace can be divided into three different types: apolitical silence, manipulated and passive silence, and conscious and rhetorical silence. There is no direct means to testify how many Chinese netizens are apolitical. But when a given political issue has happened, it is likely that a certain number of netizens may not care about it. Manipulated and passive silence is a somewhat negative response towards internet censorship. This happens when one tries to express something sensitive straightforwardly, but fails because of censorship, and cannot (or do not bother to) find other ways to bypass the censors and to continue to focus on this topic. This population thus has been manipulated into being a silent group, at least temporarily. Rhetorical silence reveals that netizens are conscious about what is sensitive and what is not, and thus consciously choose when to be silent. These three types of silence are mutually transformational under certain conditions (see Figure 7). Here I place more attention on the third type, rhetorical silence, and its transformation to either apolitical silence or manipulated silence.

Figure 7. Three Types of Silence in Chinese Cyberspace

Those Chinese netizens who choose to remain in rhetorical silence should not be understood as apolitical, since a conscious choice to be silent is a very political activity. Rhetorical silence functions as a form of self-protection and sometimes reflects the chilling effect of internet censorship in quieting political discussion. Take “dajiayou” (literally meaning “buy soy sauce” but actually referring to “none of my business”) as an example. The
phrase was coined in early 2008, when a Guangdong television reporter interviewed a passer-by, and asked for his comment on a recent sexual scandal between two film celebrities. The passer-by answered that “it is none of my fucking business … I’m out to buy soy sauce.” This passer-by might be really indifferent and disinterested in that scandal, but as a specific euphemism, this discourse has become a popular expression of strategic silence to a given socio-political affair in cyberspace: when speakers feel the risk of criticizing sensitive topics directly or try to mock a given fact (such as political taboos) in a relatively safe way, it will be used. In other words, being silent on some given issues is a conscious choice and a covert political activity.

Since the boundary between the public and the private has gradually been blurred in cyberspace – as has the boundary between hard politics and soft politics, many discussions about personal lives may often drift into discussions about public affairs. The concept of politics needs to be updated accordingly to reflect this new context, by taking into account the seemingly-trivialized, symbolic, micro and quotidian dimension. It is quite common in Chinese cyberspace for netizens to be silent on sensitive issues but not silent at all elsewhere (e.g., in the personal realm, and other non-sensitive realms); at the same time, political topics and issues often become references for personal stories and private discussions, and sometimes generate political consequences accordingly. This indirect and “apolitical” manner has become a special tactic for some Chinese netizens’ participation in internet politics. An increasingly significant phenomenon in Chinese cyberspace is “tucao” (meaning “mock unhappy things”). Though most of the time the speakers are mocking issues about themselves (their trivialized daily lives), the objects of mockery can often be extended to wider socio-political issues. But
unlike serious discussion such as an argumentative process (Fischer & Gottweis, 2012) or communicative deliberation (Healey, 1993) about serious socio-political issues in the hard politics realm, the discussion of personal lives and public issues here occurs in a more humorous and ironic way (rather than in a serious, deliberative way).

Rhetorical silence can be understood in the context of a further dimension. Some Chinese netizens choose to directly avoid touching on hard political issues and enjoy themselves with alternative choices, including online games, time-travelling television dramas (the most popular theme is time-travelling to the Qing Dynasty, as shown in the catchword “Qingchuan”), Chinese crosstalk (the most popular artist of which is Guo Degang), light comedy (Zhao Benshan is the most popular actor), various TV programs and books about chicken soup for the soul, and escapism, among many others. From this point of view, netizens have been “positioned as consumers of spectacle rather than as fully enfranchised participants in the democratic process” (Talbot, 2007, p. 27). The prevalence of various alternative choices reveals a kind of stepping back from the public realm into the private realm, or “inner emigration” in Arendt’s sense (as cited in Bewes, 1997, pp. 160-163). With too much boring and empty content circulating in Chinese cyberspace, or self-mocking content about everyday lives, serious discussions have been replaced by gossip, irrelevant topics and meaningless discussions. The more the speakers turn their attentions to personal affairs, the farther away they are from hard political deliberation. This is because personalized, quotidian

207 Escapism is particularly welcomed by intellectuals. For example, Thoreau's book *Walden* has attracted huge number of followers and some escapists in ancient Chinese history also have examples of modern lives. A good case of this is a Sina Weibo user whose screen name is *Laoshu Huahua* (Old Tree Drawing Pictures), self-described as “Luanshi huiben” (Picture books in the times of trouble). He expresses his socio-political escapism by drawing pictures about very personalized and often non-political issues, and in some interviews he has showed his awareness of the boredom of politics and of social life. At the time of writing, his Weibo account has 937,587 followers.
affairs – although able to be extended and connected to sensitive, public affairs – may suck up speakers’ time and energy which otherwise could be used for participating in hard political deliberations. Socio-political issues have been touched on occasionally, but overall Chinese netizens are likely to talk about themselves. As seen from the mutual relationship between three types of silence (Table 3), inner immigration reveals that more netizens may have been transformed from rhetorical silence into apolitical silence, and thus are in a highly dangerous retreat in the sense of public good or civility.

However, it should be noted that it is the involvement of political consciousness that makes rhetorical silence a political activity. The resistant meaning behind rhetorical silence cannot be understood from the perspective of other aforementioned online internet resistant activities, since rhetorical silence is a more deep resistance to (or, an entire negation of) the existing political system: it is because of the meaninglessness of participating in politics (no matter whether they have been controlled or not) that these netizens reject any kind of participation (including resistance) in politics. If the resistance discussed previously is active resistance, then rhetorical silence (particularly inner immigration) reveals a kind of passive resistance in Chinese cyberspace.

**The Power and Limitation of Symbolic Resistance**

From encoded discourses and esoteric writings to images, audio and video materials, and rhetoric, discursive power has greatly been extended to a wider concept of symbolic power. This shift may echo the theoretical discussions by previous Western scholars, such as Foucault who, in *Discipline and Punish*, examines “how the enabling discourses direct the operation of power” (as cited in Turner, 2003, p. 25), and Bourdieu (1984, 1991) who develops Foucault’s
idea and proposes a concept of “symbolic violence,” referring to the unnoticed or partly unconscious domination upon our everyday life. My focus here emphasizes discourses as symbolic power from a bottom-up perspective (rather than the other way around). In traditional society, discourses as symbolic power mainly describes what the powerful dominant group has done to the weaker group (i.e., ordinary people). But in the internet era, the situation seems to have changed to some degree. Increasing numbers of ordinary people can now cultivate a sort of symbolic power through building a special realm of subordinate culture, revealed mainly by resistant discourses, images, audio and video materials, and rhetoric – in a given case of symbolic resistance, more than one of these forms are often involved. A sense of community or in-group can be produced and shared by creating and recreating a kind of encoded language, using and re-using both technological and symbolic means of internet resistance, or, more generally, participating in different ways in this subordinate culture. As Bales argues:

The culture of a group is a fantasy established from the past, which is acted upon in the present. In such moments, which occur not only in groups, but also in individual responses to works of art, one is “transported” to a world which seems somehow even more real than the everyday world. One may feel exalted, fascinated, perhaps horrified or threatened, or powerfully impelled to action, but in any case, involved. One’s feelings fuse with the symbols and images which carry the feeling in communication and sustain it over time. One is psychologically taken into a psychodramatic fantasy world, in which others in the group are also involved. Then one is attached also to those other members. (as cited in Bormann, 1972, p. 398)
The resistant practice in Chinese cyberspace helps to create a “rhetorical fantasy” in Bales’ sense. Of course, it does not mean that this rhetorical fantasy is a monolithic whole. By contrast, the demographic backgrounds of users are different, and different factions do exist. However, compared with negative responses from the dominant system (including the censorship system), responses from like-minded companions within this community are more supportive. Chinese internet resistance and identity politics (as consequences of such resistance) within this rhetorical fantasy help to enhance a sense of in-group belonging, and make this community’s issues even harder for outsiders to understand.

It should also be pointed out that, in the case of China (or similar authoritarian contexts), resistance disguised with various symbolic means, or “resistance through rituals” (Hall & Jefferson, 2006) with Chinese characteristics, has a double-edged sword effect. On the one hand, such euphemistic resistance gains the possibility to circulate while any direct, straightforward resistance may easily be banned. Symbolic means are indispensable tools for internet resistance. Various guerrilla-style tactics taken by the disempowered are able to bring politics closer to the everyday experience of the disempowered, and also have less chance of being policed by ideological powers. In other words, it is much easier and safer to practice, while at the same time, gives tiny yet noticeable challenges to the powerful end of the spectrum.

On the other hand, by using symbolic, euphemistic covers, online resisters hold back the smell of gunpowder from their activities, and generally become tolerable for the authorities. It thus becomes difficult to ascertain whether symbolic resistance is real resistance or just a consequence of the authorities’ adaptive control policies. In order to weaken the power of
symbolic resistance in Chinese cyberspace, or to break down the bottom-up symbolic resistance, the dominant system also has some covert strategies, such as selective incorporation or, simply, turning blind eyes to it and making it function as a valve for “letting off steam.” Selective incorporation means that the authorities are able to bring some popular phrases into official texts, and use some popular forms (such as humorous cartoons and video clips) for internet propaganda. By deliberately stooping to use some elements of this subordinate culture, the dominant system shows its high position and to some degree also its friendly attitude to the subordinate one. However, in Chinese cyberspace, it may not be the case that, as Zizek puts it, “the true victory occurs when the enemy talks your language” (Zizek & Mao, 2007, p. 17), because selective incorporation of some subordinate discourses (or "hegemonic incorporation," see Gal, 1995) may just function as a covert strategy for the authorities to deal with challenges from the subordinate culture. As Dean argues:

When one’s enemy accepts one’s terms, one’s point of critique and resistance is lost, subsumed. The dimension of antagonism (fundamental opposition) vanishes. Other, smaller conflicts emerge. Conflicts that are less significant, less crucial, become sites of intensity, sucking up political energies. Conflicts fusions arise as the multiplicity of small antagonisms, each seemingly central, make finding the key division difficult. (Dean, 2009, p. 9)

When the authorities accept some online discourses, the potential critique and resistance from ordinary people is “lost and subsumed.” Thus, we should not romanticize symbolic

---

208 For example, on 10 November 2010, the breaking news of People’s Daily brought in the popular cyber catchword “geili” (give power, meaning “helpful”), as its key word: Geili, a playful and humorous catchword in cyberspace, is used now in China’s most official newspaper. Similar words, including “diaosi” (though often used in a negative way), have since been used in this newspaper as well (see Gui & Jiang, 2012). Many netizens were cheered up by these usages and believed that it signaled a huge success for ordinary people.
resistance in Chinese cyberspace and ignore a very important dimension of it which has been colored by the authoritarian regime. Bottom-up symbolic resistance is still following the hidden power logic of the top-down. In other words, symbolic resistance, hardly an absolute resistance, seemingly challenges the system, but, ironically and unconsciously, may function as an affirmation of it at the same time, or lead easily to “the reproduction of domination” (Gal, 1995). To bring in the theoretical concept of hegemony (Gramsci, 1971), Chinese authorities seem to be tactical as well, and have utilized an adaptive policy of internet control and potentially give the ordinary users some resistant spaces (as discussed in Chapter Two).209 Symbolic resistance in Chinese cyberspace seems to have served this authoritarian hegemony. Avoiding direct challenges to the system (as the first generation of technological resistance has done), the abundant usage of rhetorical means in symbolic resistance, including silence, covertly signals an escape or retreat from hard politics to soft politics. That is, an escape from a dangerous to a relatively safe realm, from the grand and public to a relatively micro and individual level. This retreat to less significant, less crucial issues may occupy and absorb users’ time and energy, and thus reveals a deep impossibility for the Chinese internet to be a democratic tool or to encourage civil deliberation in the process of hard politics.

Symbolic resistance in Chinese cyberspace has hidden influences on Chinese cyberculture, within which the collective cultural mind of netizens has been framed. This collective cultural mind can be understood through two phenomena. First, paranoid thinking seem to have gained popularity recently in Chinese cyberspace. When their connection times out, users never know

---

209 However, the cultural political space is not automatically available, but has to be won and continually defended by various kinds of struggles between censors and netizens. The core theme of symbolic struggles is meaning making: while the dominant group tries to legitimate itself by pressing the subordinate group to accept its ideological ideas, the subordinate group tries to neutralize the efforts made by the former and create alternative meanings of existing cultural products or new meanings of subcultural practice.
exactly the real reason: whether it is a computer problem, or the firewall, or perhaps the local internet provider’s choice (J. Fallows, 2008). Meanwhile, the black box of censorship creates an atmosphere of unpredictability and thus helps to push users to read and write between the lines. The second phenomenon is that a huge number of netizens have become “low grade subversives, chipping away at the imposing edifice of the party-state with humour, outrage and rueful cynicism” (Epstein, 2013). The satirical images (including those of self-mockery), audio and video materials, often virally circulated in Chinese cyberspace as internet memes, have signaled this internet cynicism and the reproduction of powerlessness.

The apparently trivial forms of symbolic resistance can easily be overlooked by social scientists, but they are “the indispensable and revealing precursors of those elaborate institutional political actions” (Gal, 1995). Increasing numbers of ordinary people are able to present their own opinions and share their personal feelings and stories with others – though for some critical ideas they have to apply various symbolic means to avoid being censored. Internet symbolic resistance also helps to form an atmosphere for other resistant forms in a broad socio-cultural context, that is: youth resistance, feminist resistance, and grassroots resistance in real society. The ideas and rhetorical means utilized in symbolic resistance sometimes even benefit real and serious resistance in the offline world: an increasing number of offline protests and resistance have taken rhetorical means (e.g., of parody, humor and satire) from online resistant cases for the purpose of emotional mobilization, an issue which will be fully discussed in the coming chapter. Internet resistance helps to extend the meaning of traditional politics to a very quotidian, micro and symbolic level, and becomes an important form of political participation for some Chinese people.
CHAPTER VI. A TYPOLOGY OF NETWORKED RESISTANCE

In Chinese cyberspace, technological resistance (hacking resistance in particular) has undergone a shift from organized (e.g., Falun Gong hackers and their hacking activities) to scattered (as noted in Chapter Three), and most symbolic resistance happens at a relatively scattered, micro, and everyday level. This, however, does not mean that there exists no networked resistance; in contrast, instances of such resistance abound, as some cases in the previous chapters have revealed. Internet resistance includes not only scattered and everyday resistance (relatively covert) but also networked resistance (relatively overt and collective). Both technological and symbolic strategies have been greatly used in networked resistance. This chapter focuses on forms and potentials of networked resistance in Chinese cyberspace, and presents a typology of different types of it, in which collective and overt resistance can occur under specific circumstances: networked grassroots resistance, routine resistance, rumors as resistance, and resistance in the guise of entertainment. This typology, of course, does not mean that no other types of resistance exist in Chinese cyberspace. Other types such as feminist resistance and erotic resistance do exit, but their dimensions have either been discussed occasionally in previous chapters, or can be covered by these four types. It should also be noted that these four types may not be entirely mutually exclusive; for example, routine resistance may also involve rumors – my clarification here is mainly for analytic convenience and in the interest of a better understanding of network resistance in Chinese cyberspace (rather than a better classification per se). This chapter concludes, in more general
terms, with a brief discussion of how networked resistance in Chinese cyberspace may contribute to our understanding of internet politics (including identity politics) in China.

**Networked Grassroots Resistance**

The internet has long been believed to provide new changes for grassroots resistance (Sima, 2011; Tai, 2015; G. Yang, 2003c, 2014a). Based on a case study, this section tries to extend our understanding of the dynamics of networked grassroots resistance, including inhibitors, opportunities, and questions, such as that of how a scattered, individual resistance becomes networked.

In February 2008, Yan, a 25-year-old woman from Minqing County (of Fujian Province, Southeast China), was found dead. Though local police insisted that the autopsy showed Yan died of ectopic pregnancy and no violence, poisoning or gang rape was ever involved in her death, Yan’s mother still believed that her daughter was gang-raped to death by eight local ruffians who had a connection with the local police. After her attempts to seek justice from the official system failed, the mother turned to human rights activists for help (B. Guo, 2009). A netizen named Guo Baofeng – alias “amoiist” on Twitter – was one of these activists. In 2009, Guo helped Yan’s mother by uploading a video about her skepticism over Yan’s case.210 This activity received attention from the local police and Guo was soon detained. While in police custody, Guo managed to get back his smart phone and twice asked for help on his Twitter account: “I have been arrested by Mawei police, SOS” and “Pls help me, I grasp the phone during police sleep” (amoiist, 2009a, 2009b). These two messages stirred up a viral

---

210 Several other netizens (e.g., Fan Yanqiong, Wu Huaying and You Jingyou) who helped Yan’s mother to quest online over the injustice of this case had already been taken away by the local police (Branigan, 2009; B. Guo, 2010).
dissemination in the circle of Chinese Twitter users. Another Twitter user named “wenyunchao” started a postcard campaign and asked all netizens to send postcards to the police station where Guo was in custody; on every postcard was written the same sentence “Guo Baofeng, your mom wants you to go home to eat” (Hua & Yu, 2009; Shidai Zhoubao, 2009).211 This campaign received positive responses from its wide audience, and several days later a good many postcards arrived at the police station. It would be hard to determine with certainty that these activities produced real pressure for the local police, but finally Guo was released on bail. The heated discussion provoked by Guo’s case eventually attracted much more attention to Yan’s case. This case is a good example with which to explain why, and how, a publicly invisible case may finally become visible.

Yan’s mother seemed to have tried many means to appeal for her daughter, but for a long time these efforts were in vain. There are some crucial inhibitors that prevent people such as Yan’s mother from making their miserable stories publicly visible to more people. One of these inhibitors is the chilling effect generated by coercion from officials, the police, the security forces, and a pattern of political arrests and intimidation (as discussed in Chapter Two). Economic restriction may function as another inhibitor of networked resistance. People have to worry about the mundane pressures of earning a living which Marx appropriately termed “the dull compulsion of economic relations” (as cited in Scott, 1985, p. 246). It is important for them to bear in mind that they should avoid any online activity that might get them into trouble; trouble in this context means not only the risk of being arrested by the police, but also the risk of losing their jobs. This partially explains why few local newspapers

211 Some photos of the postcards taken before being sent out can be seen at Flickr (see China Digital Times Editor, n.d.).
or television stations tend – or dare – to report the other side of such a case, reporting only the side that the officials want them to do.\textsuperscript{212} Though the internet has generally empowered many ordinary people with a way to speak out, both the risk of being arrested and economic restrictions still exist.\textsuperscript{213} The fact that almost all netizens who were ever deeply involved in helping Yan’s mother to upload information online were detained by the local police shows that the nationwide censorship system is still effective at the local level. Moreover, people like Yan’s mother may not be able to use internet technologies; if they do have the capability to do so, their posts, if not censored and deleted, may be easily be drowned out by other posts.

Under these socio-political conditions, many ordinary people like Yan’s mother cannot circumvent the local power system (which has a directly and indirectly coercive influence upon them) and cannot make their voices heard (either by high-level officials or by a wide audience), at least through traditional means.

The turning point of this case is that Yan’s mother turned to human rights activists for help. Activists like Guo have more experience in using the internet and may, sometimes, be able to break through the agenda set by local media and local authorities; moreover, they have formed a network online and have the power to mobilize relatively more people to participate in their activities. In other words, a story told by these activists may have more chance of

\textsuperscript{212} By contrast, nationwide media often do not think such a piece of local news (though important for local people) is nationally significant and worth reporting.

\textsuperscript{213} Another case in 2009 helps us to understand this obstacle which faces ordinary netizens. A young Shanghai worker named Wang Shuai was arrested on charges of slander for his online posts implying criticism of local officials in his hometown of Lingbao City, Henan. He was soon released without any charge and the local police admitted that the detainment was not appropriate. He was fired finally by his employer with the excuse that “Due to the structural realignment of business strategy, the training department [where Wang worked] was shed.” And he failed to find a new job for a long time. This is not to imply that Wang’s employer did this because of the pressure from the authorities, though this might be the case; they may simply just want to avoid any potential risk by employing someone like Wang. This did have negative effects on Wang, who said later that he would never post things like that again. Refer to Lin (2009).
being heard than a similar story told by ordinary netizens. Despite all kinds of risks, activists still are able to circumvent top-down censorship and threats, and make a covert, scattered resistance overt and collective. Both online activism and general strategies have played crucial roles in helping this to happen.

*The boomerang strategy*

Guo knows quite well how to use Twitter; in fact, according to his profile, he joined Twitter in 2007 and has long been an active user. Since Twitter has been blocked by the GFW since 2009, Guo, as a Mainland Chinese, must have the ability to “fanqiang” (to circumvent the firewall).\(^{214}\) Compared with those who spend time only inside the firewall, Guo shows different habits of internet usage, as do many others who can fanqiang. At the time of his detention, Guo also had personal accounts on Chinese SNSs such as Netease Weibo, but in this case he gave priority to Twitter and posted these two SOS messages on Twitter rather than on domestic websites, and he posted these messages, as he sometimes did, in English rather than in Chinese.

On why he did it in this way, his explanation was that “this … attracted international attention” (B. Guo, 2009). Many activists such as Guo in present-day China have positive images of foreign media and in fact, most of them have personal relationships with foreign media. They are more inclined to make a case like Yan and Guo’s a topic first outside the firewall; after it has successfully become a topic outside, it is then expected to create pressure on the inside and thus become an agenda for the domestic media and/or the authorities.

Through participation and practice in many cases like this, activists have long since learned

---

\(^{214}\) According to articles on his personal website, Guo said he often used “Twitter in English via a twitter’s mobile web interface (www.dabr.co.uk)” (B. Guo, 2009). This mobile web interface is a third-party site which can help Mainland Chinese to use Twitter more conveniently without any need to use other fanqiang tools.
what kind of power relationship exists between foreign media and domestic media, and how to use it for their purposes, including resistant purposes. The information, similar to that in the boomerang pattern (Keck & Sikkink, 1998, pp. 12-13), flows first from the inside outwards, and then from the outside in, generating a kind of “reverberating effect” (Robin, 2004, p. 181) and helping to solve domestic issues.

This boomerang strategy is a common strategy shared by activists nowadays, and used widely in other cases as well.²¹⁵ This strategy has partially been constructed because of censorship itself, since too often netizens have been unable to air their voices freely and get relevant problems solved inside the GFW. By letting foreign media become involved, the internet activists show their awareness of the censorship situation within Chinese SNSs and their distrust in them.

Networked activists

Seen from the perspective of social networking, there are several key nodes in Yan and Guo’s case. The first key node is Guo himself. The second one is the Twitter user named “dupola.” He translated Guo’s English SOS messages into Chinese and made them available for other Chinese Twitter users and objects of numerous retweets (see dupola, 2009). A further key node is the Twitter user “wenyunchao” who initiated the postcard campaign and invited lots of people to participate (see wenyunchao, 2009).²¹⁶

²¹⁵ For example, one case in 2008 happened when a girl in Weng’an County (of Guizhou Province, Southwest China) was found dead from unnatural causes. Hundreds of “seditious” videos were uploaded on YouTube which attracted dense coverage from the international media; while such video could rarely be seen on domestic video websites. Although most netizens inside the GFW cannot access YouTube and see these videos, they can be seen by outsiders. When it becomes “news” outside, it will become “news” inside as well (yushu, 2008).

²¹⁶ According to his personal profile on Twitter, wenyunchao focuses on “news regulation and internet censorship in China and tries to promote China’s democratic transition” [my translation], and he defines himself as a “Chinese Internet Activist” (wenyunchao, n.d.).
These key nodes are opinion leaders (who always have a large number of followers) in their social networks. According to their Twitter profiles, they share similar focuses such as Chinese censorship, democratic transition and internet freedom. Twitter provides them with an alternative platform and enables them to form an online circle. Organizing collective offline activities may thus become much easier for activists. Moreover, the opinion leaders in the circle connect ordinary Twitter users who follow them; a mobilization within this circle thus becomes faster and more effective. A connective circle, with some opinion leaders in it, can always be found in overt, collective resistance that happens in Chinese cyberspace. The network of activists can also be seen in many other cases, including Freelance columnist Lian Yue and his followers in the Xiamen anti-PX event (see Xiao, 2011b, pp. 202-224), the Zhao Lianhai case, and the Sanlu milk scandal (G. Yang, 2013).

Questions may arise about whether social media like Twitter (and activists connected via social media) can bring any social change, as Gladwell (2010) argues. Unlike in the cases of the “Twitter Revolution” (an arguable concept) in the Middle East and Eastern Europe, some activists are physically located within national borders (as was Guo in this case), greatly use Chinese language in their everyday posts and discussions, and are connected with those who are located outside of the GFW. A network has gradually been built. However, in the case of China, as discussed in the previous chapters, internet resistance has been greatly limited to a tolerable scale. Any fundamental challenge to the Central Government is not allowed to happen (MacKinnon, 2008); while at the local level, resistance towards local authorities

217 It needs to be noted that some activists have thus been the focus of censorship. If they are physically located within the GFW, they are often visited by security staff, and sometimes personal computers and hard disks may be confiscated for further checks. If they are physically located outside the GFW, they are more likely to be hacking targets (as seen in the Falun Gong case in Chapter Three). These factors can upgrade the chilling effect, and at the same time, can bring more “capital” to relevant activists.
sometimes does exist, and has been used by the Central Government as a tactical way of controlling local government. Since Yan and Guo’s case was mainly relevant to local authorities, the activities urging local authorities to release Guo were given a green light by high level authorities. Otherwise, it would not be possible for activists to talk in the domestic news media outlets and cyberspace.

*The postcard campaign: collective resistance as symbolic performance*

A very important activist strategy, which happened in Yan and Guo’s case, takes online activism offline too, and creates direct (or indirect) pressure on relevant officials. This strategy is the postcard campaign. After the Twitter user “wenyunchao” began calling for his followers to participate in the campaign that “everyone sends a postcard to Guo,” a huge number of postcards were sent from different parts of China to a small local police station in southeast China. Some were sent from overseas countries including the U.S. and New Zealand. With Guo Baofeng their nominal recipient, all these postcards were in fact sent to the local authorities; none of the postcards ever reached Guo’s hands while he was in police custody. The hidden meaning of this activity was to demonstrate public pressure and to urge the local authorities to release Guo. Mailing postcards was strategically used as a supplement for online (and offline) activism; it provided “a means for people to air their voice without risking unwelcome attention from the authorities.”218 The form of the postcard campaign has since become a popular tactic for activists in China, and been greatly used in resistant activities such as the human rights movement, environment protection and other protest actions.

---

218 My translation. Original text comes from “mranti,” also a very active Twitter user, who participated in the postcard campaign of Guo’s case (as reposted by huyong, 2009).
Further analysis of the expressive dimension of this campaign is worthwhile here. The organizer of this postcard campaign called all participants to photograph their postcards and share them on a given website before sending them out.

Figure 8. Images of the Postcards Sent to Guo Baofeng

Top-down and left-right: A postcard sent from New Zealand; a postcard with a postage stamp of the national flag of the U.S.; a postcard with a stamp of the Constitution of People's Republic of China; a postcard with a hand-drawn Twitter logo; and a postcard with a stamp depicting tanks.
The photo gallery of postcards functions as a database to which everyone including those participants has free access; all the physically isolated participants are thus virtually connected. Some of these postcards reveal hidden, unspeakable political meanings by selecting specific postage stamps depicting tanks (with the metaphor of violence), of the Constitution of the PRC (as an ironic comment on free speech) and of the national flag of the U.S. (with the metaphor of freedom) (see Figure 8). At the same time, the senders are clearly aware of safety issues, since none of the postcards contain any reference to their physical addresses or their real names. Such satirical yet hidden symbolic tactics become indispensable parts of the performance of resistance in Chinese cyberspace – not only to raise the profile of relevant activists but also cause public attention to relevant socio-political issues.

This case may not be able to cover every aspect of networked grassroots resistance. But it does provide a probable explanation of how relatively individual resistance becomes collective. The mechanism and strategies revealed in this case can also been seen in many other cases involving issues such as injustice, housing demolition and relocation (chaidian, suburban houses being bulldozed to make way for development), pollution and food safety. Some of the resistance weapons studied in the previous chapters, such as circumvention tools, discursive strategies and iconic means, can also be seen in networked grassroots resistance.

---

219 Of course, censors or relevant authorities may also have free access to this database and the virtual network of these activists.

220 Most of these postcards were signed only with the senders’ Twitter account names. They reveal that most postcard campaign participants are Chinese Twitter users, and this offline campaign was a continuation of their online activities. For original texts, please refer to the photo gallery of postcards on Flickr (see China Digital Times Editor, n.d.). As seen in many other cases, anonymity functions as a positive factor for networked resistance. Although the information control system becomes “smarter,” and to distinguish the true identity of a netizen becomes easier, anonymity may still be easily created in the cyber context. As mentioned in Chapter Three, there are various technological means to create anonymity online. Collectiveness may help to produce anonymity as well, since within a group an individual participant may share potential risks with the others (see Le Bon, 2001).
Routine Resistance

Unlike networked grassroots resistance which happens in a very random style, routine resistance happens much more regularly and in a routine pattern. When dates of politically sensitive events draw near, for example that of the Tiananmen Incident or the National Congress of the Communist Party of China (R. Deibert, et al., 2010, p. 456; Thornton, 2010, p. 181), the authorities tighten the control over the flow of information in Chinese cyberspace, and routine resistance is thus provoked. During such periods, the so-called “illegal news coverage,” “false news” or “rumors” are more easily filtered than during other periods. The GFW may also raise its surveillance level to stop “dangerous” information from coming in, or going out of, the firewall. This time-dependent feature of Chinese censorship also greatly affects the features of low-profile resisters’ struggles. Talking about something repeatedly every year on a politically sensitive date (e.g., June 4) seems to have been a public ritual for a group of netizens, particularly dissenters and those who want to fight for a free space of speech for those greatly affected by this historical event.

Netizens who have a special interest in knowing, or letting others know, what happened at Tiananmen Square on 4 June 1989, might have already been aware that making relevant posts on Sina Weibo is quite different from posting on Twitter. Twitter users can speak in a much more public and direct way; photos of hunger strikes and of troops involved in the crackdown, names of student leaders, and recent stories of dissidents in exile can all be put straightforwardly and in much detail. Those Twitter users share some overt, public emotional feelings about the regime and relevant political leaders. Meanwhile, for those who are on Sina Weibo, though the feelings they share may still be overt and public, direct discussion of this
historical event is not allowed. Some do try to speak out freely and directly as their counterparts outside the firewall do; the content is soon deleted by the censors. Often they need to utilize much more indirect, disguised means to express their attitudes and feelings. They avoid mentioning any sensitive words, including names of “heroes” of the event and the date of June 4 itself, and create many euphemistic terms (as discussed in Chapter Four) as well as iconic forms (as shown in Chapter Five) to cheat the censorship system. Encoded and indirect writing has also been utilized to make posts about this incident. A netizen showed his disappointment in regard to the insiders’ response of June 4 implicitly:

In my WeChat circle of friends, only Hong Kongers and Taiwanese still remember to make posts about this day. Mainlanders seem to have forgotten it. Memory can be manipulated. Were it not because two days ago a seller of radio-controlled model airplanes reminded me that such airplanes were forbidden these days, I might also forget what day is today. (My translation. For the original post, refer to Hong, 2014)

The post mentions nothing directly about June 4, which is indicated only by the date when it was posted and implied by “this day” and “today” (euphemistic terms for June 4; for more cases, see Appendix B). This indirect way of speaking something politically sensitive is often seen in other online communities. Being aware that censors are always there, netizens need to apply this strategy to maximize the possibility of bypassing the censors. This kind of symbolic resistance is part of a routine ritual shared by like-minded netizens.

Routine resistance can also been cultivated by esoteric reading of official texts. Take posts of Sina Weibo official accounts such as People’s Daily and Life Weekly on 4 June 2014 for example. Unlike many ordinary netizens’ accounts, these official accounts did not directly
mention any piece of information of the Tiananmen Incident that day. People’s Daily shared nine works by illustrator Marta Altes and said “Whatever life owes to you is in fact a blessing for you! Good morning!” While People’s Daily chose to ignore this historical day, Life Weekly posted the Japanese painter Katsushika Hokusai’s representative work The Great Wave off Kanagawa and cited a piece of poetry by Tao Yuangming, one of the most famous poets in Chinese history. Why did Life Weekly choose a picture with boats threatened off the coast by an enormous wave on June 4? Some following commentators believed that Life Weekly was trying to speak its unspoken criticism of what the authorities did 25 years ago, and its hidden worry about the status quo of the Chinese political system. On a politically sensitive day, it is quite common for netizens to gather around official accounts to see what they have said and have not; some official accounts such as Life Weekly may also wish their “art of esoteric writing” (Strauss, 1988) could be “appreciated” by the public. This is much like a game played between some official accounts and some ordinary netizens. By analyzing and comparing their nuanced details, these ordinary netizens try to guess hidden meanings behind different posts of different official accounts, and to interpret the real attitudes of different factions in the dominant group. Or by doing so, they try to re-shape the agenda.

---

221 This is quite different from time periods of other historical events which are allowed to be reported, when huge public coverage may be available. There are, of course, some differences even in the so-called state-owned media as well. People’s Daily and Xinhua News Agency are core party-owned media which stand closer to the party’s policy, while South Weekend and other market-oriented media, though still state-owned, have more possibility and space to step over the mine field of propaganda. This is commonly known as the strategy of “da cabianqiu” (pushing the envelope).

222 It seems to have been a routine for the official accounts on Sina Weibo to say “Good morning” as their first post of every day and “Good evening” the last, often with wise sayings or metaphorical pictures from famous figures in history. The post of People’s Daily was translated by myself; however, the original text seemed to have been deleted when I re-accessed it on 24 April 2015. For the original post of Life Weekly, please refer to their post (Sanlian Shenghuo Zhoukan [Life Weekly Magazine], 2014). Wang and Tao (2000) translate this poetry as follows: “Plunge yourself in Nature’s course with cheers, and then you won’t have any joys or fears. When your life has reached its destined date, it is no use complaining of your fate.”

223 In fact, readers do not gain this ability immediately; the ability is gradually practiced and formed via media practices. Chinese newspapers, argues Pan (2008), have long tried to have the readers “reading between lines.”
set by official accounts and lead the discussion towards the other (sensitive) direction. These ordinary netizens thus make, albeit very limitedly, their presence felt and their voice heard. From this point of view, at least some Chinese netizens can never be treated as passive receivers who forget what the authorities make them forget.

Routine resistance often follows the rhythm of time, thus when politically sensitive dates go by, the magnitude of expression reduces accordingly. Generally, routine resistance in Chinese cyberspace seems more like a ritualized collective activity shared by many netizens for a relatively short period of time – or a kind of “resistance through rituals” (Hall & Jefferson, 2006); after each period, if relevant forms of resistance exist, they are small-scale and happen at a much more individual level. The advantage to be gained through routine resistance may seem trivial but, for those at the margin, the possibility of a marginal gain is never trivial. It is a measurement of the censors and, based on the results, netizens know whether their constraints on a specific issue have become loose or not.

**Rumor as Resistance**

Generally speaking, rumors are provoked when something normal, such as a rule or norm, has been broken, and, at the same time, when people can access the truth only with difficulty. Rumors often require conversations to transmit and interpret them (Stern & Hassid, 2012), and they invite much participation from the public. In the pre-internet era, many Chinese people often relied on rumors to know what was going on (Markovits, 1996, p. 2275). Nowadays, the resistant dimension of rumor has become even more significant and deeply reveals the “everyday production of politics” (Besnier, 2009) in Chinese cyberspace. In some cases, such as the Bo Xilai case in 2012 (H. Gao, 2012), some domestic SNSs (e.g., Weibo) are required
by the authorities to close down their comment function to avoid the rapid spread of “rumors.”

Netizens, however, use the “forward” function to comment (due to Weibo’s design, users can make comments to the original post when forward it). Sometimes, the forward function is blocked as well.224

Former Chinese leader Jiang Zemin’s absence, on 1 July 2011, from the CCP’s 90th Anniversary, sparked great rumors about his death or serious illness. Jiang and other former leaders are often shown at the gatherings: they are staples of similar high level official events. Any public discussion of political leaders has long been a sensitive taboo in China. Since there is no other way to know what has happened inside the black box, the only way those who are curious about changes in the dominant power system can use is to analyze the nuanced clues, the absence or position modification in the list of leaders, for example. These widely circulated rumors were related to the type of illness, gathering of armed police, and the hospital where Jiang was supposed to be cured, etc. It reached its peak time several days later when a Hong Kong television station reported that Jiang had died from hepatic cancer. The authorities tried to deny these rumors via Xinhua News Agency by claiming that “all news around the death of Jiang is nothing more than rumors,” but they did not mention anything further about Jiang’s situation. At the same time, the censorship system was mobilized to keep the online “rumors” about the former leader off-limits. Any attempt to search the name of Jiang Zemin (or even the Chang Jiang, the Chinese name for the Yangtze River), “xinji gengsi” (myocardial infarction), “siwang” (death), “guale” (hung, a euphemism for death), or

224 This was the case during the Jasmine Revolution in 2011 (Canaves, 2011). The control of the “forward” function also happened in 2014. In order to forbid some active Sina Weibo users to share information about the Occupy Central Movement in Hong Kong, Sina Weibo specifically disabled the forward function of these users’ accounts.
“301 Hospital” might have resulted in vain, since “According to the relevant laws, regulations and policies, the results of this search cannot be displayed” (Chin, 2011). Netizens, however, had strategies to circumvent the censorship system, including using images (as discussed in Chapter Five), analogies, argots, homophony, Roman script, and so on (See Branigan, 2011). (See Appendix B for more euphemistic expressions.) Though the censors would no doubt be aware of these tricks soon and adapted their censorship strategies accordingly, this short time lag did provide valuable possibilities for exchanging certain pieces of information between some ordinary netizens.

With an estimated 280 million users by July 2014, Chinese micro-blogging sites, including Sina Weibo, Tencent Weibo and Sohu Weibo, have attracted huge number of Chinese netizens.225 According to a survey (CNNIC, 2014), two netizens in five are micro-blogging users. The collective opinion formed in micro-blogging sites is quite different from that formed by traditional state-run media. Various unidentified rumors, such as news of scandals, protests and public anger at incidents or corruption, keep on circulating in micro-blogging sites. Official media and relative administrative departments have treated rumors as public challenges to their credibility or, worse, to social harmony, and thus rumor needs to be controlled.226 This huge scale population of users and the uncontrolled user-generated content on micro-blogging sites seem to have worried the authorities. In order to control opinions

---

225 It should be pointed out that although nowadays when we talk about Weibo we normally refer to Sina Weibo, since Sina Weibo is “by far the most significant such site in China today,” (see Ng, 2013, p. xiii), the first Weibo service was not provided by Sina but by Fanfou (fanfou.com), an imitation of Twitter which was created in May 2007. Nowadays, there are many active Weibo services in China, Hexun Weibo, NetEase Weibo, People’s Weibo, Phoenix Weibo, Souhu Weibo, Tencent Weibo, Xinhua Weibo, Tianya Weibo, to name a few. Sina Weibo as the most significant one has undergone a significant decrease in its registered accounts in the last several years, with its peak population only ever reaching 350 million. For the history of Weibo in China refer to Sullivan (2012).

226 For example, in the Bo Xilai case in 2012, the comment function of some Weibo sites were blocked for 72 hours and sixteen “rumor-spreading” websites were shut down (Wertime, 2012).
online (particularly on SNSs), the Supreme People’s Court of the PRC issued a new policy in 2013, with one clause reading that “Netizens who share defamation information that is defamatory or harms other people face up to three years in prison if their posts are viewed 5,000 times or forwarded 500 times” (2013). A hard crackdown on online rumors was launched afterwards. Netizens are not frightened by this policy. Some micro-bloggers finish their posts on Weibo and jokingly add words like “be kind to me, don’t forward more than 500 times” – in order to mock this policy; some others forward nonsensical messages, press releases or posts from government accounts more than 500 times (see FlorCruz, 2013), as a kind of spoof and hidden defiance.

The first case relevant to this rumor rule happened several days after it came into effect. A 16-year-old middle school student in Zhangjiachuan County (of Gansu Province, Northwest China) made a post on his personal Tencent Weibo about an irregular death due to local police negligence, which was forwarded more than 500 times. The post was treated as rumor by the local authorities and the teenager was detained by the local police; this sparked a public outcry for resistance – fierce criticism of both the local authorities and the rumor rule itself abounded. Rather than directly challenging the detainment, netizens responded strategically by pointing out via “human flesh search engine” (as discussed in Chapter Two) (Herold, 2011a) that the office building of the local government of Zhangjiachuan was so luxurious that it did not match its title of national-level poverty-stricken county, and that the head of the county owned expensive watches. While the local authorities’ harsh responses in this case did provide a chilling effect on other netizens, particularly on those who have offline connections with this student and have reposted his Weibo post (see S. Zhang, 2013), the criticism of it also put
pressure on the authorities. Eventually, the teenager was released and some relevant officials were discharged from their positions. The Zhangjiachuan case reveals that “rumor” sometimes is an excuse for censorship: since the post was a potential threat to the local authorities, the latter expected to legitimize the detention by firstly defining the post as rumor.

Because of their enormous power to shape online public opinion, da V (big Vs) such as aforementioned Charles Xue (as mentioned in Chapter Two) also received close attention from the authorities. Several big Vs were later arrested, and official media used a stigmatic title, “dayao” (big rumor raisers), to describe this group of people. As a result, some of those with verified accounts on Weibo lowered their profiles by giving up their verified status. It may be impossible to tell how effective these surveillance actions are, but evidence does exist which indicates that the population scale of Sina Weibo users has decreased since 2013 (CNNIC, 2013, 2014). This reveals that harsh actions taken by the authorities can shrink the politically discursive cyberspace; they also affect cyberculture at the invisible level, by not only pushing some ordinary netizens into alternative spaces and means but also by making their online expression even more hidden and disguised.

Rumor as an alternative way to approach truth reflects a public skepticism towards official discourses and a hidden resistance to the status quo. This phenomenon can be seen both online and offline, in almost all kinds of censorship context. By sharing the non-official information,

---

227 The “V” here means “verified.” According to Sina Weibo system, when a person has used his or her real name to register an account, his or her account name will be shown together with a “v”. Big Vs refers to those verified account holders who have more than a million followers. Most big Vs are entertainment celebrities, business tycoons, writers and commentators.

228 In August 2013, Charles Xue, a businessman who was active in Chinese cyberspace and had over 11 million followers on Sina Weibo at the time of writing, was arrested by Beijing police on a charge of soliciting a prostitute. He was arranged to appear later on CCTV, one of the most influential state-owned media institutions in China, to seek forgiveness. This case was widely interpreted as the Chinese authorities’ plan to tighten the control of information online.
participants make themselves connected. Rumor itself becomes a kind of social protest (Y. Hu, 2009), and enable participants to challenge information control policy and wide socio-political issues collectively.

**Resistance in the Guise of Entertainment**

Much research has suggested that Chinese netizens are more likely to use the internet for entertainment purposes (e.g., L. Guo, 2007; B. Meng, 2011; G. Yang, 2011). However, this does not imply that Chinese netizens are very apolitical; on the contrary, the once entertainment-focused fan communities, argue some scholars (W. Zhang & Mao, 2013), have undergone a recent change in the content they translate – from pleasure-seeking entertainment to content of educational and social value. Though not every entertainment community has become activist groups or political pressure groups, entertainment activities and political activities do sometimes overlap one another, with many political activities being mobilized through social networks in the guise of leisure-oriented activities (Poell, et al., 2014).

The cases discussed previously have revealed how internet resistance can be overt and collective at the same time. This is not to assume that every publicly visible resistance is potentially made as such by an explicit group of participants, although most of the time this is the case. In a given act of resistance, it might be problematic to claim that ordinary resisters, in particular, are fully aware of what they participate in, or at least, to claim that they are as fully aware as other “professional” participants such as environmentalists, activists and dissenters. The resistant part is likely to be a small part of their online activities; when they hang around online, most of them just “entertain themselves by playing games, listening to music, watching movies, chatting and so on” (F. Liu, 2011, p. 128). However, as Yu (2007a, 2007b) points out,
the existing scholarship seems to have overlooked the political potential of entertainment, since sometimes, entertainment consumers also get involved in very “resistant” activities. “Jia Junpeng, nimama hanni huijia chifan” (Jia Junpeng, your mom wants you to go home to eat; hereafter “Jia’s case”) is a good case to demonstrate this phenomenon.

This cryptic and apparently innocuous phrase originally appeared in July 2009 as a post in a Chinese online community of the popular online computer game World of Warcraft. After sparking nearly eight millions clicks and over 300,000 responses within the first 48 hours, it soon became a popular phrase – a new internet meme – that has spread across Chinese cyberspace and even Anglophone cyberspace (Baidu Tieba, n.d.-b). People’s Daily equates this case to a “ridiculous and meaningless” one (People’s Daily Online, 2009), since it seems that there is no reason why this weird case would be so popular. Another popular comment refers to a frequently forwarded reply to that post – “what we were following was not the post, but loneliness” [my translation] – to indicate its oddness. The case, however, seems not as simple as that.

The online community in which this case happened is the biggest virtual gathering place for players of World of Warcraft (WOW) in Mainland China. While most players have simply tried to enjoy the game, conflicts of interest, censorship – or, generally, politics – have all had an impact on their experience. By the time of this post, the Chinese WOW players had not been able to play this game for at least 40 days, as the gaming service had experienced a temporary blackout, which would have been really unbearable.229 The industry of online games, including imported ones, has long been censored by the Chinese authorities (MOC,

---

229 “It’s hard to imagine that in the West where people get grumpy over a few hours of [WOW] scheduled maintenance,” as Andrews (2014) argues.
2004, 2010; X. Zhang, 2012). In 2009 Blizzard changed its Chinese partner from The9 to NetEase, which meant that, from the point view of the authorities, the game needed to be reviewed. The blackout was due to content censorship and the conflict of interest between different regulating agencies of the Chinese Government. During this period of time, many Mainland Chinese players fled to the Taiwanese servers of the game. All these facts together help to explain, at least partially, the reasons for, and circumstances of, Jia’s case, and thus how this case reveals a hidden resistant meaning.

It may be arguable to conclude that players potentially made this case happen, since none of the participants in Jia’s case ever directly mentioned that they were fighting against the authorities’ content censorship over online games – they were simply performing the act of resistance in an entertaining way. This feature is slightly different from that of other resistant forms; under the cover of entertainment, it can easily be overlooked as a case of resistance. Their resistance against censorship, which highly depends on the censorship itself, is only a tiny part of their online activities. The game matters much more and, if there is no censorship of the game industry from the authorities, there might, accordingly, exist no resistance from this group of game players.

Sometimes, resistance by online game players may also be just as overt and collective as that by those from backgrounds such as human rights or environmental protection. In 2010, after the new expansion of WOW was launched in Mainland China, Chinese players found that a weird keyword filter had been added to the game. Any information which mentioned words such as “freedom,” “sexy,” or “temptation” would be either forbidden or shown as messy code (Refer to Sanjidao, 2010). Many commentators believe that a possible explanation
for why “freedom” was censored by the authorities is that this word is connected with “Western liberal propaganda.” Angry players threatened to boycott the game until “freedom returns” (Beyer, 2014, p. 8). Anti-censorship methods soon appeared. The game players strategically used the two-character Chinese words “mutian” (目田, literally meaning “eye-field” in English) to refer to “ziyou” (自由, freedom), revealing a kind of discursive resistance (as discussed in Chapter Four). The pictorial changes between these two Chinese words mean, metaphorically and satirically, that the head of “freedom” has been cut off. “Eye-field,” which did not make any sense in Chinese until now, has become a catchphrase and circulates widely in Chinese cyberspace.

Internet entertainment communities such as game groups can also become involved in relatively hard political activities. For example, the relationship between entertainment and nationalism becomes very significant in online games on the War of Resistance against Japan (Nie, 2013). As Jenkins (2006b) argues, some entertainment products can also be translated and transferred into activism in politics. The activists in the postcard campaign to free Guo, as discussed previously in this chapter, obviously borrowed the popular phrase created in Jia’s case – “Guo Baofeng, your mom wants you to go home to eat” – and used it as a political slogan for mobilization purposes (G. Yang, 2014a). The politicization of Chinese internet entertainment is partially a consequence of censorship over entertainment materials.230 With the sphere of entertainment becoming an increasingly important site for political resistance, we should treat resistance in the guise of entertainment as being as serious as other kinds of resistance.

230 It seems to be a tradition that the CCP tries to control people’s daily entertainment activities. A recent case happened in April 2011 when the authorities prohibited all stories that contained alternate reality or time travel on TV, films and novels (see Zizek, 2011).
Politics of Networked Resistance: The Case of China

After discussing the main types of networked resistance in the previous sections, I now move to a more general issue, i.e. the political dimension of such resistance. Again, it needs to be noted that these different types of networked resistance are not entirely mutually exclusive, and sometimes may overlap with one another. I approach internet resistance, as discussed in the introduction, mainly from the technological, symbolic, quotidian and micro perspective (rather than the traditional, institutional perspective), and define internet politics within Chinese cyberspace as, fundamentally, symbolic politics which is mainly about balancing the activities of resistance and compliance. Although there are all forms of resistance in Chinese cyberspace, it should be pointed out that most of the time compliance (or rhetorical silence as discussed in Chapter Four), rather than resistance, is a wise choice for some ordinary netizens. The commonly occurring self-censorship well indicates how compliance may be practiced, as discussed in Chapter One. Resistance and compliance are actually two sides of the same coin. Here, I focus more on the relationship between compliance and resistance, particularly on compliance as resistance, such as cases of overt compliance with simultaneous covert resistance, strategic silence and similar strategies, in Scott’s sense (1985, 1990). Sometimes, it is the other way around: resistance may sometimes be read as compliance.231

In a general sense, without the capability to make significant socio-political changes as occur in large-scale movements of bottom-up rebellion, resistance or politics in a symbolic and everyday sense seems to be very “insignificant” and “useless.” However, this fact may not

---

231 As discussed in the previous section, Mainland Chinese players of World of Warcraft have to put up with the censorship, endless waits, and intense bureaucratic meddling that shut the servers down for months. At the same time, they show their anger, both overtly and covertly, towards the censors and launch delays of expansions (Andrews, 2014).
be able to devalue the political significance of everyday symbolic resistance. Internet politics in Chinese cyberspace emphasizes micro and symbolic resistance, but it at the same time, shares some general themes with traditional, institutional politics. Almost all bottom-up resistance against censorship can be categorized as a struggle by citizens for “freedom of speech.” Moreover, many cases of internet resistance (e.g., networked grassroots resistance) in present-day China can be traced back to political issues and problems in the real society, such as food safety, air pollution, polarization between the rich and the poor, corruption, and human rights, on which a close eye is kept by the authorities (from different levels within the power system).

The particular feature of everyday forms of internet resistance in Chinese cyberspace is that it can meld into other online activities such as online activism. As shown in the aforementioned resistant case of Grass Mud Horse, bottom-up symbolic resistance against censorship may provoke overt, collective defiance as well, and sometimes has an influence on the authorities’ policies. The activists in Yan and Guo’s case were able to incorporate a sentence from a resistant case in the online game field, and use it as a political slogan in the human rights protest. This occurred even though the resisters in Jia’s case are very different from those in Yan and Guo’s case, and their respective goals were very different as well. Here I do not want to overstate the effects of symbolic resistance, and symbolic politics in general; on the contrary, the effects should be analyzed objectively in specific cases. But we should bear in mind that internet politics does not merely mean expressive politics: it can definitely refer to real and hard politics (also see Y. Zhao, 2007) and, under some circumstances, may
empower the weak to threaten the political system in a fundamental way (as happened in the Arab and African Spring).

Another important issue of internet politics in Chinese cyberspace is the identity issue. As discussed in this chapter, there are various types of internet resistance, and various participants become involved. It would be quite hard to argue this political identity falls under a single and monolithic concept, such as the “digital proletariat” or “wireless working-class” (J. L. Qiu, 2009), or to simply define it by titles such as “urban,” “youth” or “middle-class.” The identity here is far more complicated than these terms, comprising activists, environmentalists, feminists, famers, workers, officials and all kinds of demographic groups with various backgrounds. Bearing this in mind, I want to promote a concept of “heterogeneous political identities” to explain the identity politics in Chinese cyberspace. By heterogeneous political identities, I mean that political identity in the context of internet resistance is not a monolithic identity, but rather various and multiple identities co-existent and potentially fluid in nature. This can be revealed by the resistant events discussed previously. At ordinary times, resisters practice their identities in their own fields. However, when a resistant event happens, different kind of participants may become involved in it and be connected – though with different purposes such as entertainment, rights-protection, enlightenment, education, or something else; and, respectively yet also mutually, they have their identities performed and, probably, enhanced. In other words, though there is certainly no homogeneous identity of the resisters, they share a general culture or politics, and the heterogeneous political identities may be joined together and become interdependent parts of an emergent resistant event.
CONCLUSION

Unlike mainstream research, which seems to have taken the power of internet censorship in China for granted, this research questions this power and argues that some Chinese netizens are not simply passive objectives of censorship; on the contrary, they frequently create and utilize various weapons of resistance to challenge the internet control system and make it less effective and thorough. Approaching from the bottom-up perspective, this research provides an ethnographically rich yet complex picture of the resistance faced by the Chinese internet censorship system. It at the same time raises attention to the theoretical issue of internet politics; in other words, how we should understand the political influence of internet resistance (as well as the internet technology per se) in China. Four guiding research questions for this research have been: (i) what are the developments and socio-political influences of anti-censorship technologies in China? (ii) how do Chinese netizens utilize other forms (and what are these forms) to challenge the control system? (iii) can internet censorship resistance become connected and collective, and if so, how? (iv) what are the political meanings of internet resistance in China? I have addressed the first and third questions respectively in Chapters Three and Six, the second question in Chapter Four and Five, and the fourth question all through these four chapters.

Building on the theoretical writings of James Scott, Michel de Certeau and others, whose work reveals how everyday forms of resistance challenge the powerful system in minor ways yet makes domination unsuccessful – or, at least, incomplete – at the micro and everyday level, this thesis adopted a resistance framework in exploring the active role some Chinese
netizens have played in the processes of fighting for free speech, human rights, and anti-corruption, among others, in cyberspace. Studies about Chinese internet censorship resistance are still very rare in current scholarship; those who do focus on this issue are inclined to emphasize the role of resistant technologies, while overlooking the variety of resisters and their resistant activities. This thesis has paid equal attention to both technologies and human beings, and also tried to rethink those seemingly trivialized or even apolitical activities, and to understand the political meanings behind such activities. Two main research findings should be emphasized here. One is the initiative of some Chinese netizens and their demonstration of non-compliance with the censorship system by creative involvement in various resistant activities. The other is two dimensions of political meanings of Chinese internet resistance. I will clarify these two issues respectively in the following two sections.

Everyday Forms of Internet Resistance

The theoretical term “internet resistance” includes not only resistance arising in cyberspace (i.e., resistance against internet censorship) but also offline resistance extended online (such as protests and rights-protection via the internet), both situations being targets of internet censorship: internet resistance in Chinese cyberspace is in essence resistance against censorship. By using the analytical term “internet resistance,” I do not mean to wipe out the internal differences of this phenomenon; I keep on reminding readers (and myself) to pay attention to the differences between types and forms of resistance that occur in Chinese cyberspace. Also, this thesis does not intend to treat internet resistance as conscious action from the very beginning – though this is the case for some resisters – it argues that for average ordinary netizens, there exists a shift from unconscious resistance towards conscious
resistance (discussed in Chapters Three and Five), the process of which has been deeply shaped by the tight control of the Chinese internet per se. This thesis has defined the weapons utilized in Chinese internet resistance as falling into two main types: technological weapons and symbolic weapons (see Figure 9).

**Figure 9. Everyday Forms of Resistance in Chinese Cyberspace**

Everyday forms of resistance can be understood mainly from circumvention tools and hacking activities (discussed in Chapter Three). Since almost the beginning of the internet in 1995, some Chinese netizens have practiced guerrilla resistance to the CCP’s attempts at control. They strategically use existing internet platforms for sharing and communicating freer information. Though in the early days many netizens might not have performed such “offensive” activities consciously and intentionally, some, particularly dissident netizens (e.g., exiles of the Tiananmen Incident, and Falun Gong members), do use the internet as a new tool for resistant purposes. Alongside the building of the GFW and other censorship designs, some Chinese netizens’ technological resistance has become more conscious and intentional, or more political, with more and more anti-censorship tools being created and even the involvement of hacking activities for resistant purposes. Two generations of circumvention tools have been observed in Chinese cyberspace. The first generation anti-GFW tools are products of a much more organized and centralized movement (e.g., Falun Gong hackers), and
they serve – from a technological perspective – a much larger religious and/or political purpose. Though some tools of the first generation are still active even today, many of them have been completely blocked by the GFW. Since about 2007, various new tools have been created and circulated, particularly those tools compatible with smart phone systems (e.g., Android) and other existing programs. This new generation of circumvention tools reveals a trend of technological resistance from relatively organized and centralized to small-scale and scattered.

If technological weapons are used more by net-savvy users, then symbolic weapons are used more often by ordinary Chinese netizens. Symbolic weapons here include discursive weapons, iconic weapons, audio/video weapons and rhetorical weapons. Discursive weapons are bottom-up responses to the keyword censorship design of the censorship system (discussed in Chapter Four). Many Chinese netizens not only practice various discursive techniques such as euphemisms, homophones and pictography to avoid being caught by auto-censors, but have also gradually become used to writing in an esoteric way (as well as reading between the lines) to communicate sensitive information. Iconic weapons (e.g., satirical images and political cartoons), spoof audio and video material, and rhetorical means (e.g., parody) are important supplements to discursive resistance; they can not only help users to access and share sensitive content but also enable users to voice criticism of sensitive issues (discussed in Chapter Five). Rhetorical silence in Chinese cyberspace reveals a kind of passive resistance among some Chinese netizens (discussed in Chapter Five). Most symbolic resistance happens at the relatively scattered, micro, and everyday level.
Internet resistance includes not only scattered and everyday resistance (relatively covert) but also networked resistance (relatively overt and collective). Besides organized hacking resistance (discussed in Chapter Three), there are some more different types of networked resistance in Chinese cyberspace (as shown in Chapter Six), varying in tools used, participants, aspects, levels, possibilities and purposes: networked grassroots resistance (e.g., environmentalist movements, anti-corruption activities, and rights-protection movements), routine resistance, rumors as resistance, and resistance in the guise of entertainment. This typology does not suggest that respective resistant forms happen in Chinese cyberspace in isolation; on the contrary, many cases become interrelated, and sometimes one case may be able to – or be used to – mobilize more participants to become involved in other cases, including offline cases.

**Understanding Internet Resistance**

Before discussing the political influences of internet resistance in Chinese cyberspace, it is important to make clear the theoretical term of “internet politics.” This thesis defines internet politics as comprising two parts: politics via the internet and politics of the internet. Politics via the internet functions as the extension of real-world politics in a traditional, formal, bureaucratic or institutional sense, and emphasizes the actual effect of the internet on the transformation of the formal political process and institutions of governance. By contrast, the politics of the internet refers to, and emphasizes, political issues that appear from the internet itself (which touch on not only traditional, institutional and “hard” political issues, but also relatively micro, everyday and “soft” political issues). These two parts are not entirely mutually exclusive, though. For example, Falun Gong may use the internet intentionally for
political purposes (an extension of their offline political agenda) – an issue of politics via the internet. But since issues relevant to Falun Gong are blocked in Chinese cyberspace, it thus is also an issue of internet censorship and resistance – an issue of politics of the internet. Internet politics may differ from real-world politics in various dimensions. Particularly in terms of resistance, internet resisters cannot be equated to real-world resisters, though they may overlap one another to some degree (as shown in networked grassroots resistance in Chapter Six).

This thesis focuses more on the politics of the internet, and tries to understand the political implications of Chinese internet resistance from both the “soft” and “hard” dimensions of internet politics. It should be noted that these two understandings do not contradict each other, since Chinese internet resistance per se is quite complex and nuanced and often goes beyond a simple, either/or answer.

**Positive implication in terms of soft politics**

This thesis places more emphasis on the soft dimension of the political influence of internet resistance in China – an updated perspective on politics which broadens our understanding of politics and emphasizes the everyday, micro and symbolic dimension of politics. By winning seemingly trivial and small victories over the dominant censorship machine, or, more broadly, the dominant political power, the resisters produce an alternative space for themselves, which is relatively difficult to reach from the powerful end of the spectrum. Everyday forms of resistance thus reveal “the weapon of the weak” in the information age. These everyday forms of resistance are often too scattered to be controlled entirely; in a collective sense, they help to create fissures in the internet governance and make the grand internet governance less effective (if not completely futile).
The resistance in Chinese cyberspace helps to form a special kind of identity politics (discussed in Chapter Six). Existing research is inclined to assume the homogeneity of Chinese netizens. This thesis argues that the diversity of forms and types of resistance makes the issue of political identity in Chinese cyberspace diverse as well. Since various participants take part in various forms of internet resistance, it is hard to argue that the participants’ political identity falls under a single and monolithic concept. Activists, environmentalists, feminists, farmers, workers, officials and all kinds of demographic groups with various backgrounds may become involved in internet resistance, which suggests a theoretical concept of “heterogeneous political identities” here. By heterogeneous political identities, I mean that the political identity in the context of internet resistance is not a monolithic identity, but rather various and multiple identities which co-exist and are potentially fluid. At ordinary times, resisters practice their identities in their own fields, often isolated from other fields. However, different kinds of participants may become involved in a resistant event – though with different purposes. By participating in various resistant events, they are able to perform – and probably enhance – their identities. Their identities become more fluid, adaptable, and possibly converged. In other words, though there is certainly no homogeneous identity of the resisters, a general culture or politics is shared by these resisters, and their heterogeneous identities may be joined together and become interdependent parts of an emergent resistant event in Chinese cyberspace.

The focus on internet resistance in Chinese cyberspace does not mean that political struggle (between censors and resisters) is the “only game in town.” In fact, plenty of alternative choices have been created for Chinese netizens, which enable them to focus on
personal issues, entertainment issues, and other issues that can be termed apolitical issues. However, as I have argued in this thesis (particularly in Chapter Five), the existence of various alternative choices has deeply revealed the failure of direct participation (e.g., deliberative discussion). Within a culture marked by heavy censorship, whilst engaging in small and personal activities such as sending an email, sharing a photo, or responding to an article on a blog, people can definitely be pushed to feel their political dimensions – if these personal activities have crossed over the line and become targets of censorship.\(^{232}\) Internet resistance thus functions as a certain form of political participation and way of enlightenment for some Chinese netizens. From this point of view, Chinese netizens have gradually built a globally unique cyberculture that avoids and sometimes subverts the authorities’ close control, meanwhile enjoying a relative freedom of expression (S. Perry & Roda, n.d.).

**Limited implication in terms of hard politics**

Though this thesis argues that internet resistance sometimes does bring direct changes to the existing political system (for instance, in the case of Green Dam Youth Escort discussed in Chapter Five), it is clear that we should not overstate the influence of internet resistance in the hard politics realm. Based on the evidence so far, Chinese internet resistance may not be able to help to bring Western-style democracy into China; the encoded language and esoteric writings widely utilized by some ordinary Chinese netizens are more likely to encourage the circulation of conspiracy theories and cynical ideas about the powerful end of the spectrum in Chinese cyberspace, rather than to cultivate an open, rational, and deliberative environment for political discussion. Paranoid thinking is also popular among technological resisters, the

---

\(^{232}\) This point has also been echoed by some observations that China’s tightening censorship has fostered a backlash, since many netizens who were previously not interested in politics have become more active in resisting the controls and choosing to protest. Refer to French (2008).
second generation anti-GFW programmers in particular (as revealed by the WCP hackers’ understanding of the design philosophy of the GFW in Chapter Three). Some resisters have realized that their resistant activities may only help to induce a kind of registration effect that supports an authoritarian hegemony, and become a part of the adaptive control policy. Various rhetorical means such as satire, parody, self-mockery, and rhetorical silence have become a significant part of Chinese cyberculture, which suggests a kind of cyber cynicism towards the existing “hard politics.” Many Chinese netizens show cynical attitudes (or, apolitical attitudes, a popular interpretation of the Chinese internet in existing academic discourse) towards socio-political issues and stay in rhetorical silence, revealing a kind of passive resistance and a deep rejection of the existing hard politics (as shown in Chapter Five). It should be noted that this limitation of internet resistance has been fundamentally determined by the adaptive internet control system and, more broadly, the resilience of the political regime.

Based on existing evidence, current Chinese internet resistance may not be able to bring fundamental challenge to the Chinese political system (as the internet helped to accomplish in the Arab Spring). The internet for Chinese authorities seems to be more like a tool with which to enhance their authoritarian hegemony; the authorities learn and adjust. The hard political influence of internet resistance should be understood in the context of a broad socio-political structure, such as types of political regimes (e.g., adaptive vs. rigid regime), and scales of offline socio-political crises (large vs. small). In the context of an adaptive regime and small-scale crises (which have still been under control), internet resistance may not erode the system in essence, but when the political regime becomes unable to adjust to challenges promptly and
crises become large and out of control, internet resistance may reveal some pervasive power (as shown in the Arab Spring).

**Contributions, Limitations and Future Implications**

This thesis applies a resistance framework to explain the struggles and dynamics of the Chinese internet. This framework does not mean that resisters are always on the right side of morality and censors on the wrong side, particularly in the case of online pornography, violence, and terrorism. We should always bear in mind that both sides have their own diversities, and it is this diversity that makes issues about internet censorship and resistance more complicated and harder to make simple judgments about. In focusing on the specific forms and types of internet resistance in Chinese cyberspace, this research aims to provide a nuanced understanding of this rapidly modernizing society, including the ethos of ordinary people, and the crisis in political, social and cultural realms. This study contributes to current academic debates about what changes the internet can bring to allegedly non-democratic countries. With the case study of China, this thesis suggests that the internet alone cannot function as a determining tool in socio-political change. When we discuss the socio-political influence of the internet, we should first discuss the role of social structure, political regime, and even cultural tradition, in the whole discussion, and then the role of ordinary participants in it. Although this research is a case study of the Chinese internet, it may benefit our understanding of the internet in other authoritarian countries, regarding issues such as adaptive control policies and resistance to censorship. (Actually there is an increasing number of research focusing on similar issues in other authoritarian contexts, see for example Aryan, Aryan, & Halderman, 2013; Calingaert, 2010; Yalkin, Kerrigan, & Vom Lehn, 2014).
However, again, we need to bear in mind the differences between different authoritarian countries. This research may also benefit our understanding of other resistant forms in a broader socio-cultural context, for example, the youth resistance, feminist resistance, and grassroots resistance in real society.

This research focuses mainly on bottom-up resistance online, while as mentioned briefly in Chapter One, resistance to censorship also happens in the middle of the hierarchical structure. For example, internet companies often apply some tactics to “cheat” the authorities and please ordinary users – not only occasionally involving themselves in direct censorship resistance but also helping to provide resistance spaces for ordinary users. This research would be strengthened if there were greater access to in-depth data collected from resistant activities by internet companies. I should admit as well that none of the statistical surveys to which I refer in this thesis (in order to provide some background information) target the specific purpose of my research. Although my research mainly uses methods of netnography and multimodal analysis, a methodological approach which does help me to reach a better understanding of the Chinese internet, it will be valuable if some more first-hand materials can be collected. As I have clarified in the Introduction, there are objective reasons why I have chosen these methods: research into internet censorship itself is a politically sensitive topic in the Chinese context, and what might be useful elsewhere might not be useful here. But it should be pointed out that if I have more time, I may also choose to do field research in the real world as a supplement to existing methods – such as conducting participatory observation in hacking groups (both the first generation and the second one), in fan resistant groups, and activist groups – which would definitely bring more perspectives and ideas to research such as this. A
further issue could be the comparison of Chinese cyber resistance with resistance in other socio-political contexts, for example to examine how, in other authoritarian regimes or even more democratic cultures, ordinary netizens see monitoring, surveillance and censorship, and how they resist such coercive pressure in their everyday lives.


dupola. (2009, 15 July). RT: @amoist: i have been arrested by Mawei police, SOS. [Twitter post]. Retrieved 10 June, 2014, from https://twitter.com/arrested/status/2659218961


Han, R. (2012). *Challenging the regime, defending the regime: Contesting cyberspace in China*. PhD, University of California, Berkeley.


J.M. (2013, 22 August). Why is the Bo Xilai case so important? The Economist.


Kuah-Pearce, K. E., & Guiheux, G. (Eds.). (2009). *Social movements in China and Hong Kong: The expansion of protest space*. Amsterdam: Amsterdam University Press.


Guanyu jisuanji yuzhuang lvse shangwang guolv ruanjian de tongzhi [The notice of pre-installing the internet filtering software on computers]. (2009).


Wangluo youxi guanli zanxing banfa [Interim provisions of the Ministry of Culture on administration of internet games]. (2010).


Shan, R. (2014). @Lichengpeng bei xiaohao, zaowan zhuding fasheng [Li Chengpeng’s Weibo account has been deleted, which is deemed to happen]. *Huanqiu Shibao* [the Global Times]. Retrieved from http://opinion.huanqiu.com/shanrenping/2014-07/5051535.html


of law in the handling of criminal cases of Internet defamation by means of the information
Retrieved from http://www.theguardian.com/media/2008/dec/30/facebook-breastfeeding-ban
Szablewicz, M. (2010). The ill effects of "Opium for the Spirit": A critical cultural analysis of China's
Popular Communication, 13(2), 120-131.
SARS epidemic in China. New Media & Society, 9(6), 987-1009.
Press.
Taneja, H., & Wu, A. X. (2014). Does the Great Firewall really isolate the Chinese? Integrating access
blockage with cultural factors to explain web user behavior. The Information Society, 30(5),
297-309.
Sociological Research Online, 16(2), 11.
Tang, L., & Sampson, H. (2012). The interaction between mass media and the Internet in non-
Tang, L., & Yang, P. (2011). Symbolic power and the Internet: The power of a "horse". Media, Culture
& Society, 33(5), 675-691.
Taubman, G. (1998). A not-so world wide web: The Internet, China, and the challenges to
First Monday, 7(9).
Media & Society, 7(5), 625-646.
tiwen [Ministry of Railways press conference: Spokesman Wang Yongping answer questions
from journalists]. [Video file]. Retrieved 21 June, 2013, from
https://www.youtube.com/watch?v=1mlI5Nag1Qs
The Economist. (2006, 27 April). China and the internet: The party, the people and the power of
cyber-talk.
Computer information network and internet security, protection and management regulations
(1997).
http://www.omniglot.com/language/articles/achineselanguagejourney.htm
Massachusetts: Newbury House.


Zhai, I. (2013). China may only have 18,000 active Twitter users: infographic. *South China Morning Post*. Retrieved from http://www.scmp.com/comment/blogs/article/1119055/china-may-only-have-18000-active-twitter-users-infographic


## Appendix A: Main Sites of Netnographic Observation

<table>
<thead>
<tr>
<th>Title</th>
<th>Address</th>
<th>Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>News Media</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 Beijing Ribao</td>
<td>bjrb.bjd.com.cn</td>
<td>2015.7.1</td>
</tr>
<tr>
<td>3 Bloomberg Business Week</td>
<td><a href="http://www.bloomberg.com/businessweek">www.bloomberg.com/businessweek</a></td>
<td>2014.10.27</td>
</tr>
<tr>
<td>5 Caixin Online</td>
<td>english.caixin.com; china.caixin.com</td>
<td>2014.8.26, 2015.7.1</td>
</tr>
<tr>
<td>6 CCTV</td>
<td>english.cnvt.cn</td>
<td>2015.2.12</td>
</tr>
<tr>
<td>9 Financial Times Chinese</td>
<td><a href="http://www.ftchinese.com">www.ftchinese.com</a></td>
<td>2014.11.25</td>
</tr>
<tr>
<td>11 Nanfang Zhoumo</td>
<td><a href="http://www.infzm.com">www.infzm.com</a></td>
<td>2014.7.16</td>
</tr>
<tr>
<td>14 Shidai Zhourao</td>
<td><a href="http://www.time-weekly.com">www.time-weekly.com</a></td>
<td>2014.6.1</td>
</tr>
<tr>
<td>16 Ta Kung Pao</td>
<td>news.takungpao.com</td>
<td>2015.1.5</td>
</tr>
<tr>
<td>17 The Atlantic</td>
<td><a href="http://www.theatlantic.com">www.theatlantic.com</a></td>
<td>2014.10.1</td>
</tr>
<tr>
<td></td>
<td>Website</td>
<td>Dates</td>
</tr>
<tr>
<td>---</td>
<td>---------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>23</td>
<td>Time</td>
<td>time.com/world</td>
</tr>
<tr>
<td>24</td>
<td>Voice of America</td>
<td><a href="http://www.voachinese.com">www.voachinese.com</a></td>
</tr>
<tr>
<td>25</td>
<td>Wired</td>
<td><a href="http://www.wired.com">www.wired.com</a></td>
</tr>
<tr>
<td>26</td>
<td>Xinhuanet</td>
<td>news.xinhuanet.com</td>
</tr>
<tr>
<td>27</td>
<td>Xin Kuai Bao</td>
<td>epaper.xkb.com.cn</td>
</tr>
<tr>
<td>28</td>
<td>Zhongguo Qingnian Bao</td>
<td>zqb.cyol.com</td>
</tr>
</tbody>
</table>

**Blog**

<table>
<thead>
<tr>
<th></th>
<th>Website</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>An Xiao Studio</td>
<td>anxiaostudio.com</td>
</tr>
<tr>
<td>2</td>
<td>Biancheng Suixiang</td>
<td>program-think.blogspot.com</td>
</tr>
<tr>
<td>3</td>
<td>Botong’s Blog</td>
<td>blog.caijing.com.cn/botong</td>
</tr>
<tr>
<td>5</td>
<td>GFW Jishu Pinglun</td>
<td>gfwrev.blogspot.co.nz</td>
</tr>
<tr>
<td>6</td>
<td>Guo Baofeng’s Blog</td>
<td>amoiist.blogspot.co.nz</td>
</tr>
<tr>
<td>7</td>
<td>J. Halderman’s website</td>
<td>jhalderm.com/pub/gd</td>
</tr>
<tr>
<td>8</td>
<td>Lin Guofen’s Blog</td>
<td>blog.ifeng.com/2068300.html</td>
</tr>
<tr>
<td>9</td>
<td>Rebecca MacKinnon’s Blog</td>
<td>rconversation.blogs.com</td>
</tr>
<tr>
<td>10</td>
<td>Yao Youwei’s Blog</td>
<td><a href="http://www.yaoyouwei.com">www.yaoyouwei.com</a></td>
</tr>
</tbody>
</table>

**Portal**

<table>
<thead>
<tr>
<th></th>
<th>Website</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Boxun Wang</td>
<td><a href="http://www.boxun.com">www.boxun.com</a></td>
</tr>
<tr>
<td>2</td>
<td>China Digital Times</td>
<td>chinadigitaltimes.net</td>
</tr>
<tr>
<td>3</td>
<td>Computerworld</td>
<td><a href="http://www.computerworld.com">www.computerworld.com</a></td>
</tr>
<tr>
<td>4</td>
<td>Engadget</td>
<td><a href="http://www.engadget.com">www.engadget.com</a></td>
</tr>
<tr>
<td>5</td>
<td>Foreign Policy</td>
<td>foreignpolicy.com</td>
</tr>
<tr>
<td>6</td>
<td>GIFC</td>
<td><a href="http://www.internetfreedom.org">www.internetfreedom.org</a></td>
</tr>
<tr>
<td>8</td>
<td>Ifeminists</td>
<td><a href="http://www.ifeminists.com">www.ifeminists.com</a></td>
</tr>
<tr>
<td>No.</td>
<td>Source</td>
<td>Website/Link</td>
</tr>
<tr>
<td>-----</td>
<td>-------------------------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>9</td>
<td>InfoWorld</td>
<td><a href="http://www.infoworld.com">www.infoworld.com</a></td>
</tr>
<tr>
<td>10</td>
<td>Meiboyuan</td>
<td>allinfa.com</td>
</tr>
<tr>
<td>11</td>
<td>OpenNet Initiative</td>
<td>opennet.net</td>
</tr>
<tr>
<td>12</td>
<td>Sina Keji</td>
<td>tech.sina.com.cn</td>
</tr>
<tr>
<td>13</td>
<td>Tea Leaf Nation</td>
<td>tealeafnation.com</td>
</tr>
<tr>
<td>14</td>
<td>Tech Crunch</td>
<td>techcrunch.com</td>
</tr>
<tr>
<td>15</td>
<td>Tor project</td>
<td>media.torproject.org</td>
</tr>
<tr>
<td>16</td>
<td>Ultrasurf</td>
<td>ultrasurf.us</td>
</tr>
<tr>
<td>17</td>
<td>WikiLeaks</td>
<td><a href="http://www.wikileaks.org">www.wikileaks.org</a></td>
</tr>
</tbody>
</table>

**Social Media**

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Website/Link</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>China Digital Times</td>
<td><a href="http://www.flickr.com">www.flickr.com</a>; doc.google.com</td>
<td>2014.6–2015.6</td>
</tr>
<tr>
<td>2</td>
<td>Diao Jinpin</td>
<td>plus.google.com</td>
<td>2014.11</td>
</tr>
<tr>
<td>3</td>
<td>ESATUTUBE</td>
<td><a href="http://www.youtube.com">www.youtube.com</a></td>
<td>2015.1</td>
</tr>
<tr>
<td>4</td>
<td>Fangong Heike</td>
<td>twitter.com/fangongheike</td>
<td>2014.8–2015.3</td>
</tr>
<tr>
<td>5</td>
<td>Fqrouter</td>
<td>tieba.baidu.com; fqrouter.tumblr.com</td>
<td>2014.8–2015.4</td>
</tr>
<tr>
<td>6</td>
<td>goagent</td>
<td>code.google.com</td>
<td>2014.11</td>
</tr>
<tr>
<td>7</td>
<td>greatagent</td>
<td>github.com</td>
<td>2014.11</td>
</tr>
<tr>
<td>8</td>
<td>ideacm</td>
<td><a href="http://www.youtube.com">www.youtube.com</a></td>
<td>2015.1</td>
</tr>
<tr>
<td>9</td>
<td>Peter Guo’s Twitter</td>
<td>twitter.com/amoist</td>
<td>2014.7–2015.8</td>
</tr>
<tr>
<td>10</td>
<td>Rebel Pepper</td>
<td>plus.google.com</td>
<td>2014.11–2015.6</td>
</tr>
<tr>
<td>11</td>
<td>Sina Weibo</td>
<td><a href="http://www.weibo.com">www.weibo.com</a></td>
<td>2011.3–2015.8</td>
</tr>
<tr>
<td>12</td>
<td>The Chinese News</td>
<td><a href="http://www.youtube.com">www.youtube.com</a></td>
<td>2013.6</td>
</tr>
</tbody>
</table>
Appendix B: Major List of Internet Regulations Regarding Censorship (1994-2011)\(^{233}\)

- Provisions on Administrating the Examination and Approval of Telecommunication Equipments Entering into the Public Telecommunication Networks (14 November 1995)
- Measures for Administration of International Inward and Outward Channels for Computer Information Networks (9 April 1996)
- Interim Regulations on Networking of Private Networks and Public Networks (24 July 1996)
- Interim Regulations of the People’s Republic of China for Management of International Networking of Computer Information Networks (20 May 1997)
- Public Multi-media Information Service Administration Measures for China Golden Bridge Information Network (March 1998)
- Circular on Strengthening the Administration of Disseminating the Radio, Film and Television Programs to the Public through Information Network (October 1999)
- Interim Measures for Administration of Education Websites and Online Schools (29 June 2000)
- Detailed Rules for Implementation of Interim Measures for Administration of Commercial Websites Archiving and Registration (1 September 2000) [Local Regulations of Beijing]
- The People’s Republic of China Telecommunications Regulations (25 September 2000)
- Administration of Internet Information Services Procedures (25 September 2000)

\(^{233}\) This list includes, but is not limited to, major regulations regarding internet censorship (refer to CNNIC, n.d.-a) and relevant websites of regulations.
• Approval and Administration Procedures of Internet Websites’ Engaging in News Publication Services in Beijing City (10 November 2000) [Local Regulations of Beijing]
• Interim Measures for Internet Websites Administration of China Securities Regulatory Commission (24 November 2000)
• NPC Standing Committee’s Decision on Safeguarding Internet Security (28 December 2000)
• Measures for Administration of Medical and Health Information Services over Internet (8 January 2001)
• Interim Provisions on Management of the Interconnection between Internet Backbone Networks (18 January 2001)
• Interim Provisions on Administration of Drug Information Service over Internet (1 February 2001)
• Interim Measures for Administration of Online Advertisement in Beijing City (1 May 2001) [Local Regulations of Beijing]
• Notice on Strengthening the Administration of Publication’s Utilization of Internet Information (14 August 2001)
• Interim Provisions on Interconnection Services between Internet Backbone Networks (29 September 2001)
• Notice on Governance of Internet Cafes and Other Internet Access Services (29 June 2002)
• Interim Provisions on Administration of Internet Publication (1 August 2002)
• Anti-Spam Regulation of Internet Society of China (25 February 2003)
• Interim Provisions on Administration of Internet Culture (1 July 2003)
• Self-Discipline Pact on Prohibiting the Dissemination of Pornography and Other Unhealthy Information on the Websites (10 June 2004)
• Measures for Administration of Drug Information Service over Internet (8 July 2004)
• Several Opinions of Beijing Higher People’s Court on the Trial of Administrative Cases regarding Rectification of Internet Cafes and Other Internet Access Services (Trial) (29 July 2004) [Local Judicial Interpretation of Beijing]
• Notice on Implementation of Principles Concluded on Video and Telephone Conference regarding Cracking down the Pornography Websites To Strengthen the Administration of Video-Audio Programs Transmission over Internet (4 August 2004)
• Internet Public E-mail Service Regulation of Internet Society of China (Trial) (2 September 2004)
• Interpretation of the Supreme People’s Court and the Supreme People’s Procuratorate on Several Issues concerning the Concrete Application of Law in the Handling of Criminal Cases of Making, Reproducing, Publishing, Selling and Spreading
Pornographic Electronic Information by Means of the Internet, Terminal of Mobile Communications and Sound Message Stations (6 September 2004)

- Measures for Administration of the Publication of Audio-Visual Programs over Internet and Other Information Networks (11 October 2004)
- Self-Discipline Pact on Search Engine Service Provider’s Boycott of Illegal and Unhealthy Information (22 December 2004)
- Measures for Archival Administration of IP Address (20 March 2005)
- Measures for Archival Administration of Non-operational Internet Information Services (20 March 2005)
- Measures for Administrative Protection of Internet Copyright (30 May 2005)
- Provisions on Administration of Internet News Information Services (25 September 2005)
- Detailed Rules for Internet Websites Management (1 December 2005)
- Measures for Administrating the Internet Access Services in Xining City (1 February 2006) [Local Regulations of Xining]
- Regulations on Protection of Information Network Transmission Right (1 July 2006)
- Blogging Service Self-Discipline Pact (21 August 2007)
- Notice on Strengthening the Administration of TV Dramas and Films Transmitted over Internet (28 December 2007)
- Administrative Rules for Audio-visual Programs Transmitted over Internet (31 January 2008)
- Interim Measures for Monitoring and Administration of Communication Quality among Backbone Networks on the Internet (15 March 2008)
- Notice on Strengthening the Issues Concerning the Administration of Internet Audio-video Programs with the Receiving Terminal of Television (11 August 2009)
- Notice on Issues Related to the Administration of Internet Audio-Video Programs License (15 September 2009)
- Interpretation of the Supreme People’s Court and the Supreme People’s Procuratorate on Several Issues concerning the Concrete Application of Law in the Handling of Criminal Cases of Making, Reproducing, Publishing, Selling and Spreading Pornographic Electronic Information by Means of the Internet, Terminal of Mobile Communications and Sound Message Stations (II) (4 February 2010)
- Plans for Further Executing the Authenticity Examination of Record-filing Information on Websites (Trial) (23 February 2010)
• Measures for Administration of Communication Network Security Protection (1 March 2010)
• Catalogues of Internet Audio-Video Programs (Trial) (17 March 2010)
• Interim Provisions of the Ministry of Culture on Administration of Internet Games (3 June 2010)
• Notice on the Examination and Approval on Delegating the Administrative Permission of Operating Internet Culture Entities (30 July 2010)
• Notice on Punishing the 11th Batch of Illegal Cultural Activities on the Internet (17 March 2011)
• Notice on Further Strictly Clamping Down on the Illegal Drug Sales through Publicizing False Drug Information on the Internet (18 May 2011)
• Notice on Implementation of Newly Amended Interim Provisions on Culture Administration on the Internet (18 March 2011)
• Interim Provisions on Administration of Internet Culture (Revision) (1 April 2011)
• Internet Terminal Software Service Industry Self-Discipline Pact (1 August 2011)
Appendix C: Major List of Cyber Slang Relevant to Censorship

**Anti-Censorship Tools**
- 套 (tao, Tor, literally means condom; as the pronunciation of Tor is similar to “tao” in Chinese): 带套 (daitao, “dai” means “use”, literally means “use condoms” but in the anti-GFW community it means “use Tor”)
- 无界浏览 (wujie liulan, UltraSurf, an anti-GFW tool)
- 自由门 (ziyoumen, Freegate, an anti-GFW tool)

**Media Relevant**
- 被庹 (beituo, be censored; Tuo is the unusual Chinese surname of a local censor who has become known to the public for his censorship activity on Nanfang Zhoumo [South Weekend])
- CCTV (acronym for China Central Television, the state television broadcaster in PRC): CCAV (China Central Adult Video), 影视 (yangshi, calamity TV, as “calamity” shares the same pronunciation of “central” in Chinese)
- 广电总局 (guangdian zongju, refers to SARFT [State of Administration on Film, Radio and Television], a former name of SAPPRFT [State Administration of Press, Publication, Radio, Film and Television]): 光腚仲菊 (guangding zhongju, bare bottom swollen anus, SARFT, as “guangding zhongju” is a near homophone with “guangdian zongju”), 广电总急 (guangdian zongji; as “ji” is a near pronunciation of “ju” in Chinese, this term mocks SARFT as State of Anxiety on Film, Radio and Television).
- 猴蛇 (houzhe, monkey and snake, refers to mouthpiece, as “monkey and snake” shares the pronunciation of “mouthpiece” in Chinese)
- 环球屎报 (Huanqiu Shibao, Global Shit Times, a mockery of Global Times, an affiliated newspaper of People’s Daily, as “shit” is pronounced like “shi” in Chinese); 坏球时报 (Huaiqiu Shibao, Bad Global Times, a mockery of Global Times, as “坏” is pictorially similar to “坏”), 混球屎报 (Hunqiu Shibao, Muddled Shit Times, a mockery of Global Times, as “muddled” is pronounced like “huan” in Chinese)
- 媒体 (meiti, media): 媚体 (meiti, pleasing body, a mockery of “media,” as “pleasing” is pronounced like “mei” in Chinese)

---

234 The list of terms in this Appendix has been compiled with reference to various sources, in particularly the open-source project on Sina Weibo sensitive terms conducted by CDT (which has collected near 3,000 sensitive terms since 2011). For more details, refer to China Digital Times (n.d.-b). In general, terms in this Appendix follow this order: firstly, the original Chinese character(s) (Pinyin of this term, English meaning); secondly, the euphemism(s) of the original term (Pinyin of the euphemism, English meaning). Both the Pinyin word and English meaning are bracketed. Furthermore, all Pinyin words in this Appendix are italicized.
- People’s Daily Explosion (Renmin Ribao, People’s Daily Explosion, a mockery of People’s Daily, a state newspaper controlled by the CCP, as “explosion” is pronounced like “bao” in Chinese)
-伟光正 (weiguangzheng, an ironic combination of three words of weida [great], guangrong [glorious] and zhengque [correct], main criteria for good cultural products required by the Publicity Department and other cultural organs)
-中宣部 (Zhongxuanbu, the Publicity Department): 萱萱 (Xuanxuan, a playful way of expressing the Publicity Department), 真理部 (Zhenlibu, the Ministry of Truth, a mockery of the Publicity Department)

Names

- 艾未未 (Ai Weiwei, the name of a dissident Chinese artist): 爱未来 (Ai Weilai, love the future), 艾瓜子 (Ai Guazi, Sunflower Seeds Ai, since he is famous for his artwork “Sunflower Seeds”), 艾虎 (Ai Hu, Tiger Ai), 艾 ww (Ai ww), 艾末末 (Ai Momo, since “末” pictorially resembles “未” in Chinese), 艾借款 (Ai Jiekuan, Ai lend money), 艾捐款 (Ai Juankuan, Ai donate), 艾汇款 (Ai Huikuan, Ai remit money), 艾债主 (Ai Zhaizhu, creditor Ai), 艾神 (Ai Shen, the god Ai), 艾婶 (Ai Shen, Aunt Ai, as “Aunt” is a near homophone with “god” in Chinese), 艾虎子 (Ai Huzi, Tiger Cub Ai), 幸福大街储蓄所 (Xingfu Dajie Chuxusuo, Happiness Avenue Savings Agency, the address of his bank account)
- 薄熙来 (Bo Xilai, the name of the former Party Secretary of Chongqing Municipality; the family name, Bo, means “thin”): 平西王 (Pingxi Wang, literally “the King who pacifies the west [Chongqing]”), 不厚 (buhou, not thick, another way of alluding to “bo” in Chinese), 窝督 (Bo Du, Bo the Governor), 都督 (Dudu, the Governor-General)
- 陈光诚 (Chen Guangcheng, the name of a blind human rights lawyer): CGC (initials of the Pinyin of his name), 陈光 C (Cheng Guang C), 陈 G 诚 (Chen G Cheng), C 光 C (C Guang C), CG 诚 (CG Cheng), 墨镜哥 (Mojing Ge, Sunglasses Brother, as he often wears sunglasses), 眼镜哥 (Yanjing Ge, Glasses Brother), 瞎子 (xiazi, blind man), 盲人 (mangren, blind man), guangcheng, GC, 阿炳 (A-bing, a very famous Chinese artist who was also blind), 要有光 要有诚 (yao youguang yao youcheng, let there be light let there be truth), 光+诚 (guang + cheng), 东师古 (Dongshigu, the village where he lives), 冻尸骨村 (dongsishigu cun, frozen skeleton village, as “frozen skeleton” shares syllables with “dongsishigu”), 东尸骨村 (dongsishigu cun, east skeleton village, as “east skeleton” also shares syllables with “dongsishigu” in Chinese)
- 江泽民 (Jiang Zemin, the name of a previous president of PRC, 1993-2003): jzm (initials for Jiang Zemin), 江贼 (Jiang Zei, Jiang Thief), 贼民 (Zemin, Steal the people), 三表哥 (san biaoge, three-watches brother, as he promoted the ideological slogan of “Three Represents” which is a near homophone with “wearing three watches”
in Chinese), 江三表 (Jiang Sanbiao, Jiang Three-watches), 蛤蟆 (hama, toad, as a mockery of his appearance), 江核心 (Jiang Hexin, Jiang Core), jiangmin (the first and last Pinyin words of his name), 江爷爷 (Jiang Yeye, Grandpa Jiang), 老江 (Lao Jiang, Old Jiang), 姓江的 (Xing Jiang de, the person surnamed Jiang), 太上皇 (Taishang Huang, Emperor Emeritus, indicating his powerful influence even after his retirement)

- 胡锦涛 (Hu Jintao, the name of the former president of PRC, 2003-2013; his given name, Jintao, literally means “Brocade-waves”): 胡 X 套 (Hu X-tao, Hu X-cover, X is a euphemistic way to refer to “Jin” and “cover” is a near homophone with “waves” in Chinese), 胡涛 (Hu Tao, Hu Waves), 胡 X 涛 (Hu X-tao, Hu X-waves), 胡紧 x (Hu Jin-x, Hu Tight-x, as “tight” shares the same pronunciation of “brocade” in Chinese), 胡锦 x (Hu Jin-x, Hu Brocade-x), 涛哥 (Taoge, Brother Waves), 胡萝卜 (Huluobo, Carrot), 胡紧掏 (Hu Jintao, Hu Tight-pulling, as “pulling” shares the same pronunciation of “waves” in Chinese), hjt (initials of Hu Jintao)235

- 胡锦涛 (Hu Xijin, the name of the chief editor of the Global Times): 胡编 (Hu-bian, Hu the Fabricator; as “hubian” also means “fabricator” in Chinese), 胡叼 (Hu-diao, Hu Bite, literally “to hold something in the mouth like a dog” and a mockery of Hu as a watchdog for the Party), 飞盘胡 (Feipan Hu, Hu the flying disc, since “feipan” [flying disc], or frisbee, can be used as a toy for dogs)

- 刘云山 (Liu Yunshan, the name of a current member of the Politburo Standing Committee, the de facto top decision-making body of China, and in charge of publicity and censorship affairs): 刘云删 (Liu Yunshan, Liu Yun-delete, as “delete” is pronounced as “shan” in Chinese)

- 毛泽东 (Mao Zedong, the name of the founding father and first president of PRC): 毛腊肉 (Mao La-rou, Mao Cured-meat, as Mao’s corpse continues to lie impervious to rot in Tiananmen Square), 太祖 (Taizu, Original Emperor), 毛贼东 (Mao Zei-dong, “Zei” means “thief” which is a near homophone with “Ze” in Chinese).

- 王立军 (Wang Lijun, the name of a former deputy mayor of Chongqing and Bo Xilai’s top lieutenant): 护士长 (hushizhang, head nurse, as “hushizhang” is a near homophone with “fushizhang” [deputy mayor]); 王护士长 (Wang Hushizhang, Head-nurse Wang)

- 温家宝 (Wen Jiabao, the name of the previous Prime Minister of China, which literally means “Warm Home-precious”): 瘟家保 (Wen Jia-bao, Plague Home-protect, as “plague” and “protect” share respectively the same pronunciation of “warm” and “precious” in Chinese), 瘟假报 (Wen Jia-bao, Plague Fake-report, as “fake” and “report” share respectively the same pronunciation of “warm” and “precious” in Chinese), 温假报 (Wen Jia-bao, Warm Fake-report), 温夹包 (Wen Jia-bao, Warm Grip-wallet, as “grip” and “wallet” share respectively syllables with “warm” and

235 Netizens commonly use “x” or asterisks to hint that some words have been hidden or censored.
“precious” in Chinese), 温佳宝 (Wen Jia-bao, Warm Fine-precious, as “fine” shares the same pronunciation of “home” in Chinese), 温加 (Wen Jia, Warm Add, as “add” shares the pronunciation of “home” in Chinese), 温加饱 (Wen Jia-bao, Warm Add-satiety, as “satiety” shares the pronunciation of “precious” in Chinese), 温家 x (Wen Jia-x, Warm Home-x), 温宝宝 (Wen Baobao, Warm Precious-precious), 家宝 (Jia-bao, Home-precious), 温影帝 (Wen Ying-di, Warm Best-movie-star, since he was believed to perform as a good politician), 影帝 (Yingdi, The best movie star), 温度计 (Wenduji, Thermometer, as this term shares its first character with his family name), wjb (initials of Wen Jiabao)

- 习近平 (Xi Jinping, the name of the current president of PRC): 习近平 (Diao Jinping, as “刁” is pictorially similar to “习” in Chinese but means “bloody, unruly” in English), 刁总 (Diaozong, as “zong” means “boss” in Chinese), 庆丰包子 (Qingfeng Baozi, the steamed bun from the Qingfeng restaurant, as Xi once went to this restaurant and ate some steamed buns there), 庆丰帝 (Qingfeng Di, Qingfeng Emperor), 新皇帝 (Xin huangdi, New emperor), 习包子 (Xi Baozi, Steamed Bun Xi, “steamed bun” also means “coward” in Chinese), 席梦撕 (Xi Mengsi, Xi Dream-tore), as Xi has promoted a new ideological slogan of the “Chinese Dream” with a reference to the “American Dream”), 习大大 (Xi Da-da, Xi Big-big, “Da-da” means “uncle” in Chinese), 习二逼 (Xi Erbi, Xi the Fool, as “bi” shares the first letter with “big” and “erbi” means “two b[ig]s” as well as “fool”), 习禁评 (Xi Jinping, Xi Cannot-comment), 习特勒 (Xi Tele, sounds like Hitler), 废习 (Fei-Xi, Waste Xi), 当今皇上 (dangjin huangshang, reigning emperor), 今上 (jinshang, short for dangjin huangshang, reigning emperor), 半羽 (banyu, half-feather, as “习” is pictorially half of “羽” in Chinese), 西晋平 (Xi Jinping, West Promoting-peace), 西金平 (Xi Jinping, West Gold-peace), 洗尽平 (Xi Jinping, Wash All-peace), 洗净平 (Xi Jingping, Wash Clean-peace), 洗进瓶 (Xi Jinping, Wash Enter-bottle), 锡金瓶 (Xi Jinping, Tin Gold-bottle)

- 俞正声 (Yu Zhengsheng, the name of a current member of the Politburo Standing Committee and the former party secretary of Shanghai Municipality): 鱼素鸡 (Yu Suji, Fish Veggie-chicken, as his previous title “Yu Shuji” [Secretary Yu] is pronounced like “Fish Veggie-chicken” in Shanghai dialect).

- 周永康 (Zhou Yongkang, the name of a former member of the Politburo Standing Committee and was once in charge of social security affairs; his given name, Yongkang, literally means “forever healthy”): 康师傅 (Kang Shifu, Master Kang, the largest instant noodle brand in China; but since it shares one character with Zhou’s given name, it has been used as a disguised way to refer to Zhou), 方便面 (fangbian mian, instant noodles), 康, 周康康 (Zhou Kang-kang), 康康 (Kang-kang), 周勇康 (Zhou Yong-kang, Zhou Brave-healthy, as “brave” shares the pronunciation of “forever” in Chinese), 周永糠 (Zhou Yong-kang, Zhou Forever-bran, as “bran” shares
the pronunciation of “healthy” in Chinese), 州永康 (Zhou Yong-kang, State Forever-healthy, as “state” is pronounced like “zhou” in Chinese), 洲永康 (Zhou Yong-kang, Continent Forever-healthy, as “continent” is pronounced like “zhou” in Chinese), 粥永康 (Zhou Yong-kang, Porridge Forever-healthy, as “porridge” is pronounced like “zhou” in Chinese), 粥永糠 (Zhou Yong-kang, Porridge Forever-bran), 舟永康 (Zhou Yong-kang, Boat Forever-healthy, as “boat” is pronounced like “zhou” in Chinese), 粥永 (Zhou Yong-kang, Porridge Gush-healthy, as “gush” is pronounced like “yong” in Chinese), 咏康 (Yong-kang, Intone-healthy, as “intone” is pronounced like “yong” in Chinese), 咏糠 (Yong-kang, Intone-bran), 涌康 (Yong-kang, Boat Forever-healthy, as “boat” is pronounced like “zhou” in Chinese), 粥涌康 (Zhou Yong-kang, Porridge Gush-healthy, as “gush” is pronounced like “yong” in Chinese), 咏康 (Yong-kang, Intone-healthy, as “intone” is pronounced like “yong” in Chinese), 咏糠 (Yong-kang, Intone-bran), 濡康 (Yong-kang, Swollen-healthy, as “intone” is pronounced nearly like “yong” in Chinese), 周永 (Zhou Yong-kang), z 永康 (Z Zhou Yong-kang), z 永 (Z Zhou Yong-kang), zy 康 (Zy kang), “z” and “y” are short for “zhou” and “yong” respectively), z 永 k (Z Zhou Yong-kang), 安全沙皇 (Anquan Shahuang, Czar of Security), 百鸡王 (Baijiwang, King of the Hundred Chickens, chicken being a euphemism for prostitute in Chinese; he was believed to have many mistresses), 方便面下架 (fangbianmian xiajia, instant noodles expired, means Zhou was arrested and removed from the powerful position), 康师傅下架 (kangshifu xiajia, Kang Shifu expired, similar to fangbianmian xiajia)

**Party Relevant and Political**

- 查水表 (chashuibiao, check the water meter, a euphemism for a house call from the police)
- 大麻时代 (dama shidai, the era of marijuana, refers to Xi Jinping’s era, as a satirical contraction of “Daddy Xi” and “Mama Peng,” terms of endearment for President Xi Jinping and the first lady Peng Liyuan)
- 独裁 (ducai, dictatorship): 毒菜 (ducai, poisoned vegetable, a euphemism for dictatorship as it is a near homophone with “dictatorship” in Chinese)
- 给人民一个胶带 (gei renmin yi ge jiaodai, give the people a tape, a mockery of the famous party saying – give the people an explanation, as “tape” and “explanation” share the same pronunciation of “jiaodai” in Chinese)
- 国民党 (Guo Min Dang, Kuomintang, a political party active in Taiwan): GMD (the initials of Guo Min Dang)
- 和谐 (hexie, harmony, a term out of Hu Jintao’s ideological slogan “Goujian hexie shehui” [Building a harmonious society]): 河蟹 (He Xie, River Crab; since “river crab” is a near homophone with “harmony” in Chinese, this term is used as a mockery of the ideological slogan), 溪蟹 (Xi Xie, River Crab; Since both “xi” and “he” means “river” in Chinese, this term is another way of mocking the ideological slogan), 被和谐 (bei hexie, be censored, literally means “be harmonized”), 被河蟹 (bei hexie, be censored, literally means “be river-crabbed”)
快递到了 (kuaidi daole, here comes the courier, another euphemism for a house call from the police)

跨省 (kuasheng, cross provincial borders, be chased across provincial lines by local police and because of political offence against local authorities)

零八宪章 (lingba xianzhang, Charter 08, a manifesto signed in 2008 by over 350 Chinese dissident intellectuals and human rights activists including the 2010 Nobel Peace Prize laureate Liu Xiaobo): 08 县长 (lingba xianzhang, 08 county head, as “county head” is pronounced like “xianzhang” in Chinese)

民主 (minzhu, democracy): 鸣猪 (mingzhu, mooing pig, as it shares syllables with “democracy” in Chinese), 敏猪 (minzhu, nimble pig, as it shares syllables with “democracy” in Chinese), mz (initials of minzhu)

民主党 (Minzhu Dang, Democratic Party): mzd (the initials of minzhudang)

请喝茶 (qing hecha, be invited for tea, get into trouble with security department mainly for political reasons)

人权 (renquan, human rights): 人权 (renquan, human dogs, refers to human rights, as “dog” shares syllables with “right” in Chinese)

游行 (you-xing, demonstration): 散步 (sanbu, leisure walk, a euphemistic way of expressing demonstration in some protests); you 行 (you-xing, demonstration, a combination of a Pinyin word “you” [travel] and a Character “xing” [walking])

雨伞革命 (yusan geming, Umbrella Revolution, refers to the Hong Kong pro-democracy movement in 2014): 雨遮革命 (yuzhe geming, Awning Revolution), 伞花革命 (sanhua geming, Umbrella Flower Revolution)

占中 (zhanzhong, Occupy Central, the Hong Kong pro-democracy movement in 2014): 站中 (zhanzhong, Stand Central, as “stand” shares the pronunciation of “occupy” in Chinese)

自由 (ziyou, freedom): 自由 (ziyou, literally meaning “this reason” but a homophone with “freedom”), 目田 (mu-tian, eye-field, a disguised way of talking about freedom since it is pictorially like “自由”), 自曲 (ziqu, self-twist, a disguised way of talking about freedom since it is pictorially like “自由”)

中国共产党 (Zhongguo Gongchandang, Chinese Communist Party): 朝廷 (chaoting, royal court, an ironic reference to the CCP), 你党 (nidang, your party, the CCP), 我党 (wodang, my party, the CCP), 共惨党 (Gongchandang, literally meaning “commu-cruel party” but a homophone with “communist party”), 共铲党 (Gongchandang, literally meaning “shared shovel party” but a homophone with “communist party”), 共餐党 (Gongchandang, literally meaning “shared food party” but a homophone with “communist party”), 共残党 (Gongchandang, literally meaning “shared disability party” but a homophone with “communist party”), 土共 (Tu Gong, indigenous communists, a mockery of the CCP), TG (the initials of Tu Gong), 共匪 (Gong Fei, commie bandit, a mockery of the CCP), GF (the initials of
Gong Fei), 共 c 党 (Gong c dang, “c” is short for “chan”), gcd, gc 党 (gc dang, “g” and “c” are short for “gong” and “chan” respectively), 補中央 (dangzhongyang, crotch central committee, a mockery of the Chinese Communist Party Central Committee as “crotch” is a near homophone with “party” in Chinese)

186: since “1” means the first generation and “86” is the country code for China, “186” thus refers to the first generation of leadership in PRC (the Era of Mao Zedong); accordingly, “286” refers to the second generation of leadership (China under Deng Xiaoping’s control), “386” the third generation (Jiang Zemin’s era), “486” the fourth generation (Hu Jintao’s era) and “586” the fifth one (currently Xi Jinping’s era).

Places

重庆 (Chongqing, a direct- controlled municipality in Western China and a place where Bo Xilai fell from his powerful position): 西红柿 (Xihongshi, west red tomato; as “tomato” is pronounced like “shi” which can mean “city” in Chinese, this term means “west red city,” a reference to Chongqing and its Cultural-Revolution-styled ideological campaign under Bo Xilai’s governance), 火锅 (huoguo, hotpot, a representative way of having meals in Chongqing and thus sometime metaphorically referring to this city)

帝都 (didu, imperial capital, refers to Beijing)

芬兰国 (fenlan guo, Finland country, shared the initials with Falun Gong and thus a euphemism for Falun Gong, also means being censored)

魔都 (modu, demoniac capital, refers to Shanghai)

日本 (Riben, Japan, literally means “sun basis”): riben, ri (sun), 日本 (yueben, say basis, as “yue” is pictorially like “ri” in Chinese), rb (initials of the Pinyin term “riben”), 扶桑 (Fusang, an ancient Chinese term for Japan), 日, Japan, 大和 (Dahe, Yamato), 大和民族 (Dahe minzu, Yamato)

乌坎 (Wukan, black ridge, a village in Southern China where a mass protest broke out in 2011): 鸟坎 (niaokan, bird ridge; as this term looks pictorially like “鸟坎” in Chinese, it has been used to refer to this village), WK (initials of Wukan), 乌鸦 坎坷 (wuya kanke, crow bumpy, with the first character in each word together reading wukan)

性都 (xingdu, sex capital, refers to Dongguan, a city in Southern China and famous for its sex industry)

中国 (Zhongguo, China): 天朝 (Tianchao, Celestial Empire, originally referring to the traditional Empire of China, now satirically used to mean China under the control of the CCP), 西朝鲜 (Xi Chaoxian, West Korea, since China is located west of Korea), 天朝 (Wangba Chao, Tortoise Empire, as “天” [wangba, tortoise] looks pictorially like “天” [tian, celestial] and “tortoise” is a swearword in Chinese), 你国 (niguo, your country, a satirical expression for China – though the speakers themselves
often are Chinese people), 贵国 (guigu, your honourable country, an ironic expression of China similar to niguo)

**The Tiananmen Incident**

- Euphemisms for the date: 五月三十五日 (Wuyue sanshiwu ri, May 35th, refers to June 4), 柳丝 (liusi, willows, a homophone with “June 4” in Chinese), 64 (Arabic numbers as a coded reference for June 4), 535 (similarly as May 35th), 6.4 (liu dian si, six point four, June 4), 六四 (liusi, six-four, June 4), 陆四 (liusi, “liu” in traditional Chinese and “four” in simplified Chinese), 六肆 (liusi, “liu” in simplified Chinese and “four” in traditional Chinese), 陆肆 (liusi, both “liu” and “four” in traditional Chinese), 六四 (liusi, “liu” in simplified Chinese and “four” in form of Arabic number), 6 四 (liusi, “liu” in form of Arabic number and “four” in simplified Chinese), bajiu (eight nine, refers to the year when the Tiananmen Incident happened), 1989 (the year in which the Tiananmen Incident happened), 89 (the year in which the Tiananmen Incident happened), 摭九 (bajiu, “ba” in traditional Chinese and “jiu” in simplified Chinese), 八玖 (bajiu, “ba” in simplified Chinese and “jiu” in traditional Chinese), 摭玖 (bajiu, both “ba” and “jiu” in traditional Chinese), 六四 (liu point four, “liu” and “four” being broken-up by a point), 六十四 (sixty-four, refers to June 4), 63+1 (sixty-three plus one equals sixty-four), 62+2 (sixty-two plus two equals sixty-four), 65-1 (sixty-five minus one equals sixty-four), 八八 (ba-ba, ba times ba equals sixty-four), 六四 (liu-four, a combination of “six” in simplified Chinese and “four” in English), 六四 (six-si, a combination of “six” in English and “four” in simplified Chinese), six four, sf (initials of sixty-four), 4698 (8964 reversed), 春夏之交 (chunxia zhijiao, the transition from Spring to Summer, refers to June 4), 五月三十四与五月三十六之间的一天 (the day between May 34 and May 36), 二十五周年 (ershiwu zhounian, the twenty-fifth anniversary), 己巳月乙未日 (Jisi yue Yiwei ri, Jisi month and Yiwei day, as in the traditional 60-year cycle, Jisi month is equivalent to May-June and Yiwei to a number of dates in the same year including June 4); in a given context, even 今天 (jintian, today), 明天 (mingtian, tomorrow), 昨天 (zuotian, yesterday), 那年 (nayan, that year), 那天 (natian, that day), 这一天 (zheyitian, this day), or 特殊的日子 (teshu de rizi, special day) can be used to refer to this sensitive date.

- 广场 (guangchang, refers to Tiananmen Square)
- 蜡烛 (lazhu, candle, sometime refers to the commemorative activities of the Tiananmen Incident)
- 维园 (Weiyuan, the Victoria Park in Hong Kong, a place for yearly commemorative activities of the Tiananmen Incident).
- TAM (initials of Tiananmen)
坦克人 (tanke ren, tank man, refers to the brave man who tried to stop tanks during the massacre of the Tiananmen Incident)

占占人 (zhan-zhan-ren, occupy-occupy-man; since “ren” means “man” and the Chinese character “占” (zhan, occupy) looks pictorially like a tank, the term means a man in front of two tanks)

占占点 (zhan-zhan-dian, occupy-occupy-point; the Chinese character “点” (dian, point) looks pictorially like persons under a tank, the term means tanks crushing persons)

占点占 (zhan-dian-zhan, occupy-point-occupy, similar to zhan-zhan-dian)

Others

草泥马 (Cao Ni Ma, Grass Mud Horse, a euphemistic expression for “fuck your mom” in Chinese and a kind of mysterious internet animal)

法克鱿 (Fa Ke You, literally meaning “French-Croatian Squid” but actually referring to the English phrase “fuck you;” a kind of mysterious internet animal)

鹳狸猿 (guanliyuan, literally meaning “stork-weasel-ape,” a mysterious internet animal, refers to internet administrators who are often believed to get involved in censorship activities)

吉跋猫 (Ji Ba Mao, literally meaning “Lucky Journey Cat” but a homophone with “pubic hair;” a kind of mysterious internet animal)

绿坝花季护航 (lvba huaji huhang, the Green Dam Youth Escort, the name of a software that was officially declared to be used for protecting young users online but believed to be used for censorship purposes): 滤霸 (lvba, filter tyrant, as “filter” and “tyrant” are respectively pronounced like “green” and “dam” in Chinese), 驴爸 (lvba, donkey father, as “donkey” and “father” are respectively pronounced like “green” and “dam” in Chinese), 绿爸爸 (lvbaba, green daddy), 绿坝娘 (lvbaniang, green dam girl), 蓝爸爸 (lanbaba, blue daddy, as “blue” is pronounced similarly to “green” in Chinese)

敏感瓷 (minganci, literally means “sensitive porcelain” but refers to “sensitive word,” since “porcelain” and “word” share the same pronunciation in Chinese)

脸书 (nianshu, the Chinese translation of Facebook): 非死不可 (feisibuke, deserve to die, transliteration of Facebook)

墙 (qiang, wall, refers to the GFW): 被墙 (bei qiang, be walled, be censored by the GFW), 翻墙 (fan qiang, jump over the wall, breach the GFW), 破墙 (po qiang, break the wall, punch a hole in the GFW)

推特中文网 (tuite zhongwenwang, the Chinese community of Twitter)

油管 (Youguan, the oil tube, refers to YouTube)
网络神兽（wangluo shenshou, mysterious internet animals, refers to a list of sensitive terms which are euphemized as names of animals, such as stork-weasel-ape, River Crab, Grass-Mud Horse, French-Croatian Squid, Lucky Journey Cat, etc.）
尾申鲸（Wei Shen Jing, literally meaning “Stretch-Tailed Whale” but actually referring to “menstrual pads;” a kind of mysterious internet animal）
五毛党（wumaodang, the Fifty-cent Party, web commentators, particularly fake opinion makers): 五毛 (wumao, fifty-cents, short for wumaodang)
吟稻雁（Yin Dao Yan, literally meaning “Singing Field Goose” but actually referring to “vaginal infection;” a kind of mysterious internet animal）