CRACKS IN THE GOLDEN SHIELD:
THE RISING CHALLENGE OF EXPANDING CHINESE INTERNET CENSORSHIP TECHNOLOGIES

A Thesis
Submitted to the Faculty of the
Edmund A. Walsh School of Foreign Service
of Georgetown University
in partial fulfillment of the requirements for the
degree of
Master of Arts
In Security Studies

By

Elizabeth Kathleen Dodson, B.A.

Washington, D.C.
April 19, 2010

Table of Contents

Introduction

The number of Internet users in China is now greater than the entire population of the United States[1], even as the use of the technology continues to expand rapidly to new demographic groups and locations within China. As personal Internet use in China becomes pervasive, and commercial dependence on the Internet becomes an ever-more integral part of the Chinese economy, the Chinese Communist Party (CCP) continues to struggle with how best to control the flow of information in order to maintain national stability. The CCP developed a hugely ambitious system, the Golden Shield Project (sometimes referred to as the Great Firewall of China) to monitor and control all information passed over the Internet in China. That system uses firewalls, Internet gateway controls and IP address blocking to ban access to certain content and websites from mainland China. However, due to the technical difficulty of effectively filtering content solely through technical means, the CCP also employs tens of thousands of people to monitor the Internet and maintain a dynamic list of sensitive terms to be eliminated from online discussions.

This paper seeks to directly address how the rapid growth of Internet use in China, as well as changing online demographics, will affect Chinese censorship techniques. Younger Chinese netizens are generating different types of content than older generations, and more young people are gaining access. The study will examine the question of how the Chinese government censorship methods cope with changing

[1] China Internet Network Information Center (CNNIC), "Zhongguo hulian wangluo fazhan zhuankuang tongji baogao [China's Internet Network Development Situation Statistical Report]", January 2010. Accessed online 20 February 2010, http://www.cnnic.cn/uploadfiles/pdf/2010/1/15/101600.pdf.

demographics and Internet content. More specifically, the paper will analyze incidents of censorship failure to determine if they reveal any longer term problems of scalability in Internet censorship techniques. This paper will hypothesize that the recent attempts by the Chinese government to change Internet censorship methods stem from the difficulty of maintaining control over an ever-expanding population of Chinese netizens.

Background: CCP Internet Censorship Philosophy, Methodology and Challenges

Propaganda, Censorship and CCP Legitimacy

The CCP is a guiding institution with far reaching influence over Chinese society.[2] Propaganda and indoctrination was a central feature in Maoist China,[3]and remains important during China's push for stable economic growth and foreign investment. Deng Xiaoping, Jiang Zemin and Hu Jintao all recognized the importance of propaganda in justifying the Party's legitimacy to the people.[4] As the party moves away from traditional communist ideals, the need to redefine its public perception is increasingly imperative. The newly packaged political philosophy, exemplified by Jiang Zemin's "three represents" and Hu Jintao's "Harmonious society," show how the party is attempting to reshape its image in a way that both supports its legitimacy and discourages

[2] Anne-Marie Brady, "Guiding Hand: The Role of the CCP Central Propaganda Department in the Current Era," *Westminster Working Papers in Communication and Culture,* 3.1 (2006), 58-77.

[3] David Shambaugh, "China's Propaganda System: Institutions, Processes and Efficacy," *The China Journal*, vol. 57 (2007): 25-58.

[4] Anne-Marie Brady, "Guiding Hand: The Role of the CCP Central Propaganda Department in the Current Era," *Westminster Working Papers in Communication and Culture,* 3.1 (2006), 58-77.

dissent. Propaganda is not the only source of CCP power, but it is a key feature in its legitimacy and control.[5]

In determining government policy for the Internet, the CCP made the calculation that the economic growth that would result from allowing the Internet outweighed the political risk, especially because CCP legitimacy is pegged to the country's economic growth.[6] As long as citizens are satisfied that quality of life is improving, China is willing to tolerate some loss of control that results from widespread Internet use. To moderate that loss of control, the Chinese government undertook extraordinary censorship efforts. The government has a two-pronged strategy that includes both active filtering of content and a policy of encouraging self-censorship.[7] The CCP uses both technical and non-technical censorship techniques. Technical methods include packet filtering, keyword blocking, monitoring software and total control over the communications infrastructure. Non-technical methods include active censorship of content, co-opting corporations in monitoring content and shaping online discussion through news outlets and online forums.

When the Internet first came to the People's Republic of China, there was brief hope in the democratized world that the new communication medium would act as a liberalizing force. By the early 2000s, however, the question of whether the Internet

[5] David Shambaugh, "China's Propaganda System: Institutions, Processes and Efficacy," *The China Journal,* vol. 57 (2007): 25-58.

[6] Nina Hachigian, "China's Cyber Strategy," *Foreign Affairs*, 80.2 (Mar-Apr 2001): 118-133

[7] Shanthi Kalathil and Taylor Boas. *Open Networks, Closer Regimes: the impact of the Internet on Authoritarian Rule*, Washington, DC: Carnegie Endowment for International Peace, 2003, and Robert Deibert et al, *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge, MA: Harvard University Press, 2008.

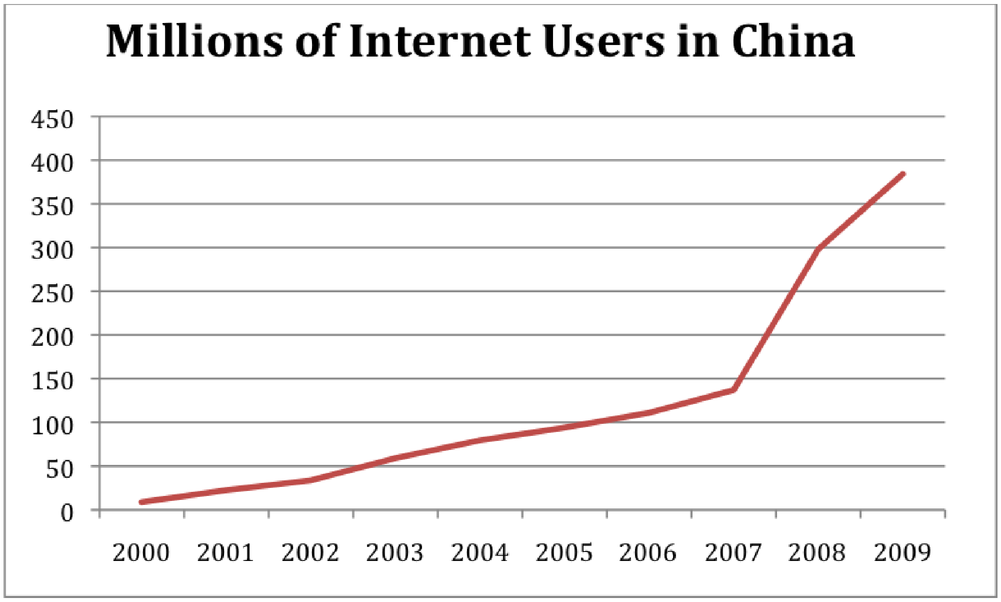
would democratize China seemed almost irrelevant. The majority of reviews on the subject acknowledged that, while Chinese censorship was not without its flaws, the Internet had not proved to be an agent of political change.[8]

Changing Internet Demographics

When Chinese Internet censorship technologies were initially developed, use of the Internet in China was extremely limited. Many of the initial studies on the effectiveness of CCP Internet censorship were conducted when Internet use in China was in its infancy. Growth over the last decade has been monumental, and over the last two the three years it has been explosive. According to the China Internet Network Information Center, a government office, Internet use grew from under 10 million to 384 million between 2000-2010, tripling between 2006 and 2009.[9]

[8] See Nina Hachigian, "China's Cyber Strategy," *Foreign Affairs*, 80.2 (Mar-Apr 2001): 118-133, Andrew Shapiro, "The Internet," *Foreign Policy* 115 (1999): 14-27, and Tamara Renee Shie. "The Tangled Web: does the Internet offer promise of peril for the Chinese Communist Party?" *Journal of Contemporary China* 13.40 (2004): 523-540.

[9] China Internet Network Information Center (CNNIC), "Zhongguo hulian wangluo fazhan zhuankuang tongji baogao [China's Internet Network Development Situation Statistical Report]", January 2010. Accessed online 20 February 2010, http://www.cnnic.cn/uploadfiles/pdf/2010/1/15/101600.pdf.



Source: China Internet Network Information Center.

Monitoring 384 million users is a significant challenge for the Chinese Government, but it may represent only the tip of the iceberg. Very recent statistics (December 2009) put China's Internet Penetration Rate, or the percentage of the population that uses the Internet, at about 28.4%.[10] Internet Penetrations in Europe and North America are around 75%.[11] Frequency and location of use is also changing. Previously, Internet usage was concentrated in Internet cafes, where it was possible to collect detailed statistics on individual users. Cheap broadband has made it more affordable for users to spend more time online, often from home. 80% of users had access the Internet in their own homes in 2007,[12] and 346 million had a broadband

[10] *Ibid*.

[11] Source: http://www.internetworldstats.com/

[12] Guo Liang, "China Internet Project Survey Report, 2007: Surveying Internet Usage and its Impact in Seven Chinese Cities," *Chinese Academy of Social Sciences*, 2007.

connection to the Internet in 2009[13]. Average weekly Internet use increased by 12.65% (from 16.6 hours/week to 18.7 hours/week) in a single year between 2008 and 2009.[14]

There is also some evidence to suggest that the way people are using the Internet is changing. Most Chinese users are looking for entertainment on the web (83.5%),[15] but an increasing number are spending more time online chatting and generating content on online Bulletin Board Systems (BBS).[16] The dramatic rise in the online population, in combination with the rise of online chat, social media and BBS use, logically generate much more content for censors to monitor.

A significant study, conducted by the Chinese Academy of Social Sciences, and underwritten by the Merkle foundation, identified critical trends in Chinese Internet use. First, Chinese Internet growth continues to be explosive in urban areas. Second, citizens are widely mistrustful of the Internet; from 2005 to 2007 there was a drastic increase in the proportion of Chinese users who believe that government control of the Internet is necessary. On the other hand, those who use the Internet have a much more positive opinion of the Internet than non-users. Users are also generating much more content through the increasing use of chat applications such as QQ, MSN, as well as using blogs and BBS forums.[17] Another Chinese Internet culture expert notes that there is a growing cultural gap between those who read their news online, and those who get it through

[13] China Internet Network Information Center (CNNIC), "Zhongguo hulian wangluo fazhan zhuankuang tongji baogao [China's Internet Network Development Situation Statistical Report]", January 2010. Accessed online 20 February 2010, http://www.cnnic.cn/uploadfiles/pdf/2010/1/15/101600.pdf.
[14] *Ibid.*
[15] *Ibid.*
[16] Guo Liang, "China Internet Project Survey Report, 2007: Surveying Internet Usage and its Impact in Seven Chinese Cities," *Chinese Academy of Social Sciences*, 2007.
[17] *Ibid.*

television.[18] In fact, Chinese Internet Users overwhelmingly say that the Internet is a more important source of news to them than television or newspapers.[19]

Recent Challenges

Despite the success of the CCP propaganda machine, it is not immune to the effects of mass communication and globalization. People are growing more skeptical about the government and State media outlets,[20] in no small part because of the way the Internet and mass communications have played a role in revealing the SARS epidemic and the melamine milk scandal. David Shambaugh remarks that the ways in which the propaganda has changed over the years reflect a general trend of atrophy and adaption in the CCP. The propaganda apparatus is still an effective tool for the CCP, but it is not as ironclad as it once was. [21]

While much of the external discussion surrounding the Internet in China centers around the possibility that the Internet might be a democratizing force, the Chinese government is much more concerned about its effects on domestic stability. Internal security is critical to economic development, but any threat to security within Chinese borders undermines the CCP's hold on authoritarian rule.[22] Events of 2008-2009 lend some credence to the idea that the danger from the Internet might come more from its

[18] Guobin Yang, *The Power of the Internet in China: Citizen Activism Online,* New York: Columbia Universiry Press, 2009.
[19] Open Net Initiative, "*Internet Filtering in China,*" 15 June 2009. Accessed online 20 November 2009, http://opennet.net/research/profiles/china.
[20] *Ibid*.
[21] David Shambaugh, *China's Communist Party: Atrophy and Adaption*, Ewing, NJ: University of California Press, 2008.
[22] Andrew Scobell, "Terrorism and Chinese Foreign Policy," in *China Rising: Power and Motivation in Chinese Foreign Policy*, ed. Yong Deng and Fei-ling Wang, Lanham: Rowman and Littlefield, 2005.

potential to generate civil unrest and disillusionment with the government rather than a direct threat to authoritarian power through organized political dissidence.

In 2008, videos of the riots in Tibet were leaked online. The videos caused embarrassment for the government, which closed access to YouTube and censored much of the international coverage of the riots. Just a few months later, the Chinese milk scandal broke, in which numerous government officials were found to be complicit in the cover up of contaminated milk that killed 4 babies and sickened tens of thousands of small children. While the government wanted to downplay the scandal, the Chinese public and Internet users were outraged that quick action was not taken to remedy the problem. Meanwhile, the Chinese public was grumbling about the government failure to prevent shoddy construction in Sichuan, where the May earthquake exacted a high death toll.

Challenging times for Internet censors continued in 2009. Early in the year, the anti-censorship movement got a new mascot in the "Grass Mud Horse," a popular Internet video blatantly mocking Internet censors through puns and double entendres that the filtering system would not recognize. Next was the Government's aborted attempt to deploy a new censorship mechanism, the Green Dam Youth Escort, which largely failed due to international and domestic outrage. In June, the government censors were extremely successful in squashing any online (or other) outpouring from pro-democracy supporters during the 20th anniversary of the Tiananmen Square Massacre. However, just a month after they effectively contained a political threat on the Internet, they were blindsided by an incident in which the Internet seriously threatened internal security.

Riots broke out in Xinjiang in July after news of an altercation between a Han Chinese woman and two minority Uyghur workers in Southern China spread over the Internet.

The juxtaposition of censorship success and failures over the last two years shows that, while the Propaganda Machine and China watchers tend to focus on the threat from traditional political challengers, the Internet might be most dangerous because it sheds additional light on government corruption and social inequities.

Analytic Scope and Methodology

The main section of this study will use a comparative case study approach to explore the question of censorship efficacy and scalability. I will examine the primary non-technical and technical means of censorship inside of China. For each censorship approach, I will examine a series of questions that are relevant to scalability. For example, I will analyze how each censorship technique works, what its strengths are, whether it is a user-level or system-level approach and whether the strategy is targeted at content or influencing online culture. For each Internet monitoring technology, I will examine a case study that shows some of the challenges facing that approach, and more specifically whether any of the current censorship technologies will become unfeasible as the number of Internet users in China explodes.

The CCP's active attempts to obscure its Internet censorship regime present challenges for a case study approach. The danger is that specific incidents of failure (and likely the causes of that failure) are easy to identify because they leak out of China, but CCP successes are not clearly identified for the outside world. The scope of this study does not extend to judgments about the relative success or failure of the current censorship program (widely regarded as fairly successful), but rather is limited only to identifying what aspects of the system, if any, are vulnerable to weakness or failure as the burden grows.

From a non-technical perspective, the Chinese government engages in the active manipulation of public discourse through online monitoring, propaganda campaigns to shape public opinion about the Internet, and clandestine government participation in online discourse. The CCP also co-opts foreign companies that wish to play a role in the Chinese online market. For example, Yahoo! and Microsoft both willingly censor their search results in exchange for the privilege of doing business in China.

China's technical approaches include the immense "Golden Shield Project," which involves a series of technical methods that target controversial keywords through a series of network wide methods such as IP blocking, DNS filtering, URL filtering and packet filtering. As a means of last resort, the Chinese government will actually turn off Internet access in an entire region if they are concerned about social stability. Finally, the government recently attempted to mandate the installation of client-based censorship software on all new computers sold in China.

For each of these censorship techniques, I will select a representative case in which the hand of the censorship apparatus was apparent. For the non-technical methods aimed at active manipulation of online opinion, I will examine the Chinese media's fixation on "Internet Addiction" and its relationship to government propaganda objectives. In the co-opting of private companies to participate in censorship, I will look at the case of Yahoo. A fair amount of information about how Yahoo cooperates with Chinese authorities was revealed in the investigation surrounding the arrest of human rights activist Shi Tao.

I will examine three cases that speak to the technical censorship technologies in China. First, I will look at the problem of psuedo-homonymns and technical keyword filtering. The Chinese language is particularly susceptible to the use of words that sound like, but are not exactly identical to, banned terms. For this, I will look at the Grass Mud Horse phenomenon of 2009, in which a clever Internet video full of off-color language and government criticism gained in popularity with certain groups inside of China. Next, I will look at the government enforced telecommunications blackout in Xinjiang, China following the 2009 riots. Finally, I will look at the attempt in 2009 to deploy a new software client, the Green Dam Youth Escort, on every new computer sold in China. Each of these incidents are timely and well documented. They also address some of the challenges facing the Chinese government in controlling content.

This study seeks to re-evaluate the current prevailing wisdom that the Chinese Internet censorship apparatus is generally sound by examining the underlying methods and technologies that support the CCP propaganda strategy. Although the Chinese government has been extremely successful in Internet censorship to date, it is worth examining whether their technologies will continue to fare as well as they have in the past as the Internet environment changes. This study on scalability is especially relevant given the enormous growth in Internet usage over the last 3-4 years.

Case Studies: Chinese Censorship Strategies

The Chinese government appears to be a firm believer that there is more than one right way to control online discourse. Kalalthil and Boas divide Internet control methods into proactive and reactive censorship techniques.[23] They classify proactive measures as use of the Internet to spread the government's message and prevent the discovery of information. Reactive strategies are more direct restrictions on Internet Use such as limiting access to the Internet, monitoring users online and blocking web sites with software tools. Kalalthil and Boas argue that proactive measures are especially powerful because they can be used iteratively to shape the online environment in a way that suits the interests of the authorities.[24]

Another way to classify the many censorship methods is to look at technical and non-technical approaches to the online threat. This approach, taken by Mulvenon and Chase, is the approach that I will take in this paper,[25] although the distinction between proactive and reactive measures is a useful one and will be referenced in each of the case studies below. The division between high-tech and low-tech (or non-technical) methods is useful because it highlights where the strengths and weaknesses of the Internet control apparatus lie.

Non-Technical Censorship

[23] Shanthi Kalathil and Taylor C. Boas. "The Internet and State Control in Authoritarian Regmies: China, Cuba and the Counterrevolution," *Carnegie Endowment for International Peace Working Papers*, No. 21, July 2001. Accessed online 5 March 2010, http://www.carnegieendowment.org/files/21KalathilBoas.pdf

[24] *Ibid.*

[25] Michael Chase and James Mulvenon, *You've Got Dissent: Chinese Dissident Use of the Internet and Beijing's Counter Strategies,* Santa Monica, CA: Rand, 2002.

Active Manipulation of the Online Environment

Mention the Great Firewall of China, and most people are inclined to think of sophisticated packet filtering and routers. In addition to these technical methods, however, there are numerous ways in which the CCP and the Propaganda Department seek to shape the online experience before a single user packet hits a router. The Chinese government works hard to shape an online environment that is conducive to commerce without posing a threat to the government. Part of this is accomplished by selecting who is fit to provide Internet services. Over the last decade, the Chinese government has pushed media outlets to become more self-sufficient and profitable, rather than simply government mouthpieces. At the same time, the government must ensure that media still has an incentive to keep the government's best interests at heart.

The Chinese have a massive Internet control bureaucracy, under the State Council Information Office (SCIO) and the Ministry of Industry and Information Technology (MIIT). MIIT closely controls licenses for Internet Service Providers, search engines and news outlets. There are a set number of sanctioned online news providers, like Xinhua and Sina, that operate at the pleasure of the Government and in close coordination with the Propaganda Department. Having a license to feature a news service brings more traffic, and therefore advertising income to a website.[26] As a result, search engines like Baidu and Sina that feature news content have an added incentive not to offend the regime.

[26] Open Net Initiative, "*Internet Filtering in China,*" 15 June 2009. Accessed online 20 November 2009, http://opennet.net/research/profiles/china.

Another non-technical way in which the government discourages online dissent and anti-government sentiment is through uneven enforcement of murky regulations. When government dissidents, such as Tan Zuoren and Guo Baofeng, are arrested, it is usually under some nebulous charge of harming national security, just as journalists are often arrested for "disclosing state secrets." In fact, Internet users are prohibited from using the Internet to engage in any of the following poorly defined activities:

- Harm national security, disclose state secrets or injure the interests of the state or society;
- Create, replicate, retrieve or transmit information that incites resistance to the PRC Constitution, laws or administrative regulations, promotes the overthrow of the government or socialist system, undermines national unity, distorts truth, spreads rumors, destroys social order, provides sexually suggestive material, or encourages gambling, violence or murder
- Engage in activities that harm the security of computer information networks
- Use networks without prior approval.[27]

These Internet regulations are so loosely defined that just about anything the Government wishes to prosecute can fit one of the above criteria. Furthermore, though in the aggregate many users do escape official punishment, those who are punished face severe sentences. For example, journalist Tan Zuoren was sentenced to five years on charges of subversion for his work establishing a database containing the names of 5,000

[27] Michelle Lau, "Internet Development and Information Control in the People's Republic of China," *Congressional Research Service Report for Congress*, Washington, DC: Government Printing Office, 2005.

children who perished in collapsed buildings during the Sichuan Earthquake. Tan's partner in the project, Ai Weiwei, has as yet evaded arrest, in part because he is an internationally respected artist and the son of a legendary Chinese writer. In another case, the CCP made an example of Liu Xiaobo, a Chinese intellectual who signed Charter08, a petition for greater freedom of speech and improved human rights in China. While Liu was one of hundreds of Chinese intellectuals who signed the charter, he was singled out and arrested just before the document was to go online. Liu was sentenced to 11 years in jail. The cases of Tan and Liu are examples of the uneven but stark enforcement of China's nebulous legal code. Ai Weiwei and Liu Xiaobo's Charter08 cosignatories are also good examples of how the Chinese government feels it has to be cautious and selective in draconian enforcement.

The government actively participates in the shaping of the online environment by hiring a cadre of Internet censors. Some of those censors are public security personnel who troll through content looking for sensitive discussions or taboo subjects. Others are hired on a part-time basis to engage in "astroturfing." Astroturfing is said to have occurred when an organization, usually a political or corporate entity, generates online content that are meant to look like part of a spontaneous grass-roots opinion, when in reality it is an orchestrated effort to shape public opinion. For example, those engaged in astroturfing for the Chinese government post pro-CCP comments on BBS forums threads discussing current events, or sympathize with the CCP position on controversial issues. While no one knows exactly how many Internet censors are employed by the government, the most often cited number of 30,000 cyber cops seems to date back to a late 2003 article in the Epoch Times covering a cyber security conference.[28] If the number of cybercops scaled up in proportion to the number of users, the number in 2010 would now be approaching 200,000.[29] This guess might not be too far off; a 2008 article by Hong-Kong based researcher David Bandurski put the number at 280,000 employed in astroturfing and online commentating alone, although many of these people work on a part-time basis.[30] These people would be in addition to those engaged in other types of Internet monitoring. This estimate of 280,000 was endorsed by Chinese Internet expert Rebecca MacKinnon in recent Congressional testimony.[31]

Case Study: The Perils of Internet Addiction

The use of online propaganda is an effective means of shaping the online environment used by the CCP. In order to spread its message and influence public opinion on a variety of issues, including perceptions of the Internet, the Chinese government encourages reporting that is consistent with its policy objectives. For example, Chinese official media often portray the Internet as a double-edged sword; while the Internet is a useful tool for commerce and research, in this portrayal it can also be dangerous, addictive and unhealthy.

[28] Epoch Times article. It is worth noting that the Epoch Times is not a pro-Mainland source and was started by practitioners of the banned Falun Gong movement. The paper focuses (although not exclusively) on human rights Issues. This figure has been cited numerous times by trustworthy news outlets such as the New York Times and Congressional Research Service. I've searched extensively for any English or Chinese language media that provides an updated or alternate number, with no success. However, given the number of Internet users in China, the number seems highly plausible.

[29] Based on figures provided by the China Internet Network Information Center.

[30] David Bandurski, "China's Guerilla War for the Web, " *Far Eastern Economic Review*, July 2008.

[31] Rebecca MacKinnon, "Testimony Submitted for the Record for the Hearing 'Google and Internet Control in China,'" Congressional-Executive Commission on China, 24 March 2010. Accessed online, 10 April 2010, http://rconversation.blogs.com/MacKinnonCECC_Mar24.pdf.

One of the biggest features in the campaign to influence public opinion on the Internet has been coverage of Internet addiction. Chinese news media has enthusiastically embraced this new phenomenon. The Chinese Government was the first to classify Internet addiction as a separate mental health disorder and recommended that the World Health Organization officially recognize it.[32] In contrast, there has been significant debate outside of China about whether or not Internet addiction should be classified as a mental disorder at all. The majority of the mental health community argues that Internet addiction is a symptom of another mental disorder, rather than a cause of one on its own. That is, the Internet does not cause addiction, but compulsive behavior can lead to excessive use of the Internet. For this reason, the American Psychiatric Association declined to list Internet addiction as a disease in the newest addition of the diagnostic bible, the Fifth Diagnostic and Statistical Manual of Mental Disorders (DSM-5).[33]

Chinese online news reporting of Internet addiction has grown drastically over the last 5 years, with reporting really starting to take off from 2004 to 2005.[34] The number of articles in simplified Chinese language press greatly exceeded the number in English language press. A Google News archive search shows that there were 376 articles total in English language online press sources mentioning Internet addiction in their titles between 2000-2009. 99 of those 376 articles either mentioned or were about China.

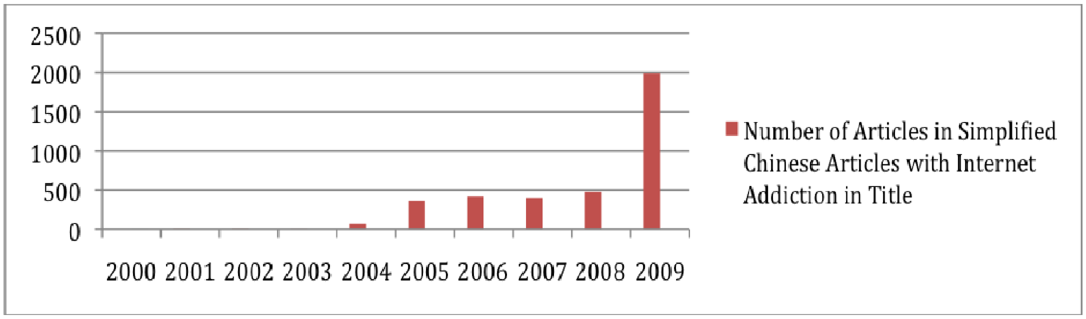
[32] Jane Macartney, "Internet Addiction Made an Official Disorder in China." *The London Times,* 11 November 2008.

[33] *Ibid.*

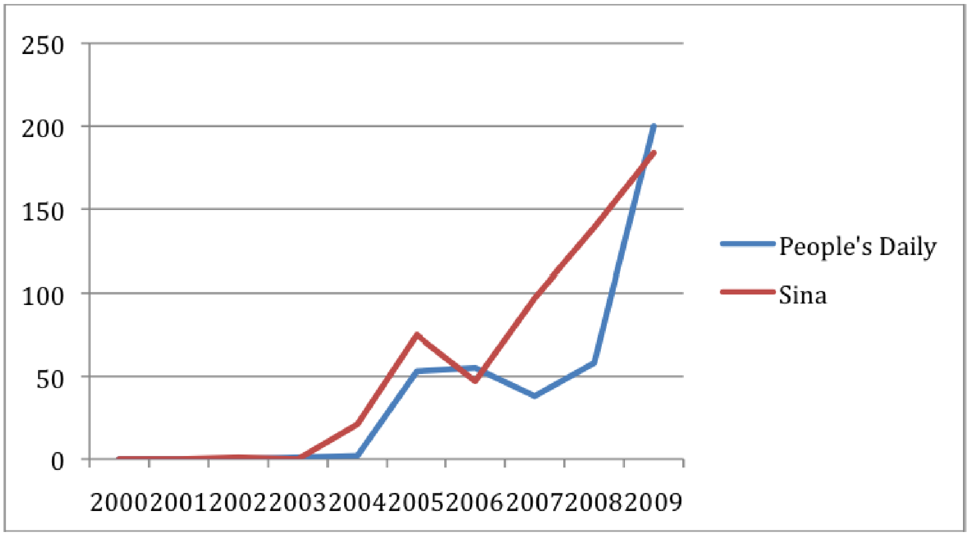
[34] According to archival searches of Simplified Chinese news sources conducted on Google's news archives.

During the same time period, there were 4830 such articles in simplified Chinese language press.[35]

News Articles with “Internet Addiction/网瘾” in the Title: All Simplified Chinese Press



Number of Chinese News Articles with “Internet Addiction/网瘾” in the Title: Sina.cn and People’s Daily



[35] This stands in contrast to reporting numbers on other types of addiction. For example, according to Google’s advanced news archive search engine, there were 2460 articles with “毒▪ [drug addiction]” in the title in the Simplified Chinese language press between 2000-2010, and 3260 news articles with “drug addiction” in the title in the English language press. Search conducted 12 April 2010.

Source: Google News Archives

The relatively similar rise in stories between Sina.cn news stories and *The People's Daily* is interesting because Sina is a more entertainment-oriented website, while *The People's Daily* is the official Government mouthpiece. The dramatic rise in such stories in 2008-2009 mirrors the government campaign to "clean up" the Internet in reaction to the Charter 08 petition[36] and in anticipation of the 20th anniversary of the Tiananmen Square incident.[37]

The tone of reporting on Internet addiction is nothing short of alarmist, with repeated emphasis on the danger and prevalence of this disease. An early 2010 news story, featured in the major Chinese news outlets, cited a government study claiming that 24 million young Chinese Internet users were Internet addicts, a total of 14.1% of the youth accessing the Internet in China.[38] Xinhua stressed that there was a particular danger from online games, as nearly half of all Internet addicts cite gaming as their primary purpose in going online.[39] As is consistent with other Chinese media reporting on the ills of Internet use, *The People's Daily* points out that too much time in the virtual

[36] The Charter 08 petition was a letter calling for government reforms and democracy. The document was signed by several prominent Chinese intellectuals as the document circulated online. One organizer of Charter 08 was imprisoned.

[37] More on the 2009 ramp up in Internet censorship in Open Net Initiative, "*Internet Filtering in China,*" 15 June 2009. Accessed online 20 November 2009, http://opennet.net/research/profiles/china.

[38] Yu Yang. "Diaocha jieguo cheng woguo qingshaonian wangyin renshu po 2000 wan [Investigation Finds Number of Chinese Youths Addicted to the Internet Exceeds 20 Million]" *The People's Daily* 8 March 2010. Accessed online 9 March 2010, http://game.people.com.cn/GB/48644/48662/11091513.html

[39] Xinhua News, "Zhongguo qingshaonian wangying baogao (2009) fabu [2009 Report on Chinese Internet Addiction Published]" 3 February 2010, Accessed online 15 February 2010, http://news.xinhuanet.com/internet/2010-02/03/content_12922533.htm

world can affect the probability of success in the real world.[40] A frequent theme in the articles is the effect of Internet addiction on school performance. This is a particularly sensitive issue in China, as academic competition is an integral part of the education system. Many Chinese parents and students will take any threat to educational performance seriously.

At times, the reporting of cautionary tales about Internet addiction can become comically dire. The Chinese press has gone so far as to emphasize coverage of incidents where Internet addiction has let to death. From 2000-2010, there were 53 stories in the Chinese press with "Internet addiction" in the title that also mentioned either death or murder in the text of the article; there were no such articles in English language press.[41] For example, Chinese media gave extensive coverage to the case of a young man who went on an all-night online gaming bender, then jumped off a building because of depression. Articles also mention grades and performance at school.

The strengths of this approach, if successful, are that citizens are more likely to rely on non-online news if they have been led to mistrust the Internet. Some striking statistics seem to confirm that this approach an impact on how the Chinese perceive the Internet. A study conducted by a respected Chinese-government think tank, the Chinese

[40] Yu Yang. "Diaocha jieguo cheng woguo qingshaonian wangyin renshu po 2000 wan [Investigation Finds Number of Chinese Youths Addicted to the Internet Exceeds 20 Million]" *The People's Daily* 8 March 2010. Accessed online 9 March 2010, http://game.people.com.cn/GB/48644/48662/11091513.html

[41] Source: Google News Archive. These numbers exclude 3 English language articles and 30 Chinese language articles covering one incident in which a young man died in an Internet addiction camp. Interestingly, the English language media emphasized the harsh methods used at the camp, while the authorized Chinese news outlets tended to stress the tragedy that Internet addiction led to the young man's death.

Academy of Social Sciences (CASS)[42], found a dramatic change in Chinese views on Internet control over a two-year period. In 2003, 52% of survey respondents said they believed the content found on the Internet was, "most or completely reliable." That percentage dropped to 42% in 2005 and 26% in 2007. Those who thought information on the Internet to be, "most or completely not reliable" increased over the same period, from 9% in 2003 to 21% in 2007. [43] While there was a small but significant increase in the percentage of users who felt the Internet should be controlled between 2001and 2007 (from 67.8% to 82.7%), there was a striking increase in the percentage of users who felt that political content should be controlled, from 8% in 2005 to 41% in 2007.[44] At the same time, there was a notable jump in the number of users who felt the government should control political content online.

Given that China's control over the media is complete and well documented, it seems likely that such an increase in coverage of "Internet addiction" was the result of a coordinated effort on the part of the government. Though there is no publically available information to prove their involvement, the campaign appears to have had the effect of advancing distrust in the Internet, which benefits the CCP as it seeks to shape opinion over the Internet and maintain control over information dissemination.

[42] The Chinese Academy of Social Sciences is a well-respected think tank inside and outside of China and is often entrusted with advising the government. While CASS members might be hesitant to publish sensitive information, their views are well respected. In this case, the study was conducted with the sponsorship of a Western organization, the Markle Foundation. CASS's trusted position within the government and society makes them uniquely capable to conduct survey research in China, where Western researches would not have access.

[43] Guo Liang, "China Internet Project Survey Report, 2007: Surveying Internet Usage and its Impact in Seven Chinese Cities," *Chinese Academy of Social Sciences*, 2007.

[44] *Ibid.*

One possible drawback of this sort of approach is that people will start to resent the government pressure to get offline or disbelieve government campaigns. While there is no indication of a massive pushback against the government on this issue, China's active online gaming community has begun to show resentment. One creative online gamer created a video entitled "The War of Internet Addiction", shot entirely inside the game *World of Warcraft,* that cleverly depicts a character battling the forces of evil (a thinly veiled reference to government censors), and complains about the inconvenience of having to work around censors to get onto international *World of Warcraft* servers. The video received some two million hits shortly after coming online, and outside press coverage pressured the Chinese government to restore the videos, which were taken offline when discovered by censors.[45] While the video wasn't wildly popular with all Chinese netizens, it does hint at the possibility of a growing irritation in the online gaming community.

On the other hand, this type of indirect approach potentially scales very well. The government gets a lot of bang for its buck, as the CCP Propaganda Department can simply instruct news agencies to ramp up coverage. As there are only a limited number of news agencies, the number of Chinese users this tactic reaches will probably grow along with the number of Internet users.[46]

[45] Loretta Chao and Juliet Ye. "Corndog Speaks of 'War of Internet Addiction'" *Wall Street Journal China Real Time Blog*, 19 February 2010, accessed online 2 March http://blogs.wsj.com/chinarealtime/2010/02/19/corndog-speaks-on-war-of-internet-addiction/.

[46] It is worth noting that this sort of campaign is always paired with media coverage on television and in regular newspapers as well, increasing the reach of such efforts beyond those who currently use the Internet.

Co-opting corporations

China's policy of co-opting corporations to assist in Internet censorship is a frequent target of Western media (and U.S. Congressional) scrutiny. Most recently, China's alleged hacking into Google's U.S.-based servers to access the email accounts of human rights activists both inside and outside of China led Google to threaten to pull out of the country, although they have not yet done so.[47] The case refocused international attention on the role Internet companies play in assisting the government by limiting search queries, monitoring online content and providing access to private user data.

In order to do business in China, websites like Google, Yahoo and Microsoft Bing must sign a pledge to be diligent in self-discipline, or censorship.[48] As part of this agreement, the web service provider is responsible for all of the content that their users post and transmit. Search engines are required to cooperate with the government and refrain from disrupting state security. This is similar to the legal concept of "intermediary liability," as Chinese service providers are legally responsible for all actions conducted by their users.[49] Such a high burden provides the service provider with a high incentive to be proactive in censoring, at the risk of large fines or even larger losses should their access to the Chinese market be revoked.

Despite the uniform pledge, there has long been a discrepancy in how willing Internet search companies were in cooperating with the government. China's most

[47] Michael Wines. "China Warns Google Again About Censorship" *The New York Times*, 12 March 2010.

[48] Internet Society of China, "Zhongguo hulianwang xingye zilu gongyue [Public Pledge of Self Regulation and Professional Ethics for China Internet Industry]," 24 March 2002. Accessed online 5 March 2010, http://www.isc.org.cn/20020417/ca39030.htm

[49] Rebecca MacKinnon, "Are China's Demands for 'Self-Discipline' spreading to the West?" *McClatchy Newspapers Syndicated Service*, 18 January 2010, accessed online 20 February 2010.

popular search engine, Baidu, is very cooperative with the government and tends to have the most restrictive results for controversial terms. Google long justified its controversial presence in China, despite its “Don’t be evil” motto, by arguing that the slightly less restrictive search results provided by Google made the Chinese Internet user better off.[50] Microsoft’s new Bing search engine was so deferential to CCP opinion that it censored simplified Chinese searches originating outside of China as well as inside of China.[51] In the face of bad press, Microsoft altered their search engine so that simplified Chinese language search results originating outside of China would no longer be censored, but the image search engine results remain distorted against anti-government content as of March 2010.[52]

Relying on the web service providers to do their own censorship has many advantages for the government. Most obviously, it pushes some of the burden of monitoring discourse onto the private sector companies, who must pay for staff to monitor content. The cost of having a censorship or monitoring department is simply the cost of doing business. It also helps facilitate Internet censorship at lower levels. Rather than shutting down all BBS systems, the Internet service provider can monitor content

[50] David Drummand. “A New Approach to China,” *Google Public Policy Blog*, 12 January 2010, http://googlepublicpolicy.blogspot.com/2010/01/new-approach-to-china.html

[51] Nicholas Kristof, “Boycott Microsoft Bing,” *New York Times On the Ground Blog*, 20 November 2009, http://kristof.blogs.nytimes.com/2009/11/20/boycott-microsoft-bing/?scp=1&sq=kristof%20microsoft%20bing&st=cse .

[52] *Ibid.* For example, a 14 April 2010 English language search on “Tiananmen Square 1989” on bing.com’s image search engine resulted almost exclusively in pictures of the government crackdown on democracy protestors, but the same search in Chinese, “天安▪一九八九［Tiananmen1989]” shows mostly peaceful pictures of the square with only a couple non-descript photos of the protest. A 14 April 2010 search of Google’s image search engine showed no such discrepancy.

and close one board, delete one comment or lock one thread. In this way, the censorship can be less blatant.

Internet companies take both a proactive and reactive role in this system-level censorship. On the proactive side, the limitation on results for controversial political keywords helps shape what the public can read or see about certain events, and consequently what people think about such events. On the reactive side, the Internet companies employ a cadre of censors who take action after incidents by deleting posts with questionable content and preventing creation of content that might contain offensive topics.

The downside to this type of monitoring is that it places a large burden on providers, who must pay for skilled labor to police their networks. As the number of Internet users increase, the financial burden this activity places on the companies will also grow. Chinese government policy is that media companies must make a profit and should not be subsidized by the State. It is important to keep in mind that the CCP made a calculated decision to allow the Internet into China on the basis that it would help spur more economic growth. The amount of money that the Chinese government, Chinese Internet Service Providers and Internet companies spend on censorship might offset some of those gains, although the lack of any government data on the topic makes a concrete judgment on the matter impossible. The government might also need to be worried about the Internet companies' motivation. There is no immediate reward for excelling at censorship, although the punishment for failing to catch something that leads to an incident can be a negative incentive. This might tempt Internet companies to overlook long-term Internet liberalizing trends that are not going to result in immediate problems.

It is difficult to say how well this approach will scale. As more Internet users come online, Internet censors will have more income from advertising that might offset the rising cost of monitoring more users. However, Internet companies are already struggling to keep up with content on Chinese web forums. It often takes quite a while for a user to say something so objectionable or become visible enough for that user to become the object of censors. Furthermore, Chinese censors tend to pay more attention to content that gets a lot of hits; one potential problem with this is that social networking sites like Twitter make it possible to forward out that same content through multiple different user accounts, distributing the traffic accordingly.

Case study: Shi Tao and Yahoo!

Prior to the hacking of Google in late 2009, the most famous interaction between a foreign Internet service company and the Chinese government was probably the controversy over Yahoo's provision of user emails to government authorities. The email content provided by Yahoo was part of the evidence used to convict Chinese journalist Shi Tao for revealing state secrets.

During the lead up to the 15th anniversary of the Tiananmen Square Massacre, the Chinese Propaganda Department sent out directives to newspaper department heads providing guidance for news organizations during the politically sensitive time. During a staff meeting at the newspaper, these directives were provided to employees, including

Shi. While Shi claims that no one told him not to take notes, his boss testified that he was warned. After the meeting was over, Shi emailed his notes on the meeting to a New York-based democracy rights activist, who posted the text on pro-democracy websites. The document was subsequently classified a top state secret by the Chinese National Administration for the Protection of State Secrecy (NAPSS).[53]

The Yahoo case is notable for several reasons. First, because the emails were cited in publically available court documents in the case, it was immediately apparent that Yahoo provided assistance. That public acknowledgement led Congress to call for hearings on the incident in which the CEO of Yahoo had to testify. Yahoo was caught being less than truthful with Congress; during the first round of testimony Yahoo claimed to have less understanding of the incident than it actually did; during a second round of testimony Yahoo admitted that employees at Yahoo's partner in China provided the information.[54] Yahoo defended itself by claiming that, if the Chinese employee had failed to comply, they would have faced personal retribution – an assertion that seems quite believable. The Chairman of the House Committee on Foreign Relations, Tom Lantos, told the CEO of Yahoo, "While technologically and financially you are giants, morally you are pygmies."[55] Yahoo ultimately settled lawsuits filed on behalf of Shi's

[53] Chain of events according to Choy Dick Wan, 'The Shi Tao Case: its development in Mainland China', *Journal of Contemporary China*, 18.61 (2009), 517 - 539.

[54] U.S. House, Committee on Foreign Relations. *Yahoo! Inc.'s Provision of False Information to Congress*, Hearing 6 November 2007, Washington: Government Printing Office, 2007.

[55] *Ibid.*

family and another dissident who was arrested on the basis of information provided by Yahoo.[56]

The CCP may or may not be concerned about the public relations aspect of working with Internet Service companies to censor the Internet. In the grand scheme of things, maintaining a hold on power and domestic stability is much more important than international perceptions. But, as China moves to a more open market, and as international Internet companies come under greater scrutiny for their cooperation with the authorities, companies could argue that unreasonable requirements for government cooperation represent an anti-competitive policy. These sorts of policies put a unique burden on foreign companies who generally do not run the day-to-day operations of the company, but must deal with the public consequences.[57]

Given China's access into Yahoo, it is logical that Government authorities have even better access into domestic providers such as Baidu. In fact, *The New York Times* reported in 2006 that the government had developed a technological system and infrastructure to search all email messages in China in real time, allowing it to instantly scan through the content of emails and bypass the Internet companies altogether.[58] This would allow them to target specific individuals for investigation with extreme ease, but it would not prevent the creation of undesirable content in the first place. Partnering with Internet companies to investigate problem users and content after it has been created is an

[56] Associated Press, "Yahoo! Settles Lawsuit by Families of Chinese Journalists," *The International Herald Tribune*, 14 November 2007. Accessed online 1 March 2010, http://www.iht.com/articles/2007/11/14/business/yahoo.php.

[57] Corey Boles, Don Clari and Pui-Wing Tam, "Yahoo's Lashing Highlights Risk of China Market," *The Wall Street Journal*, 7 November 2007.

[58] Howard French. "Chinese Censors and Web Users Match Wits," *The New York Times* 4 March 2005.

approach that may not scale well, because increased users will logically mean an increase in unacceptable content that has yet to be identified and removed. Relying on this approach too heavily would leave the CCP in the unenviable position of perpetually conducting damage control.

On the other hand, partnering with corporations and getting them to conduct censorship work on behalf of the government may suit CCP purposes better. By requiring the Internet companies to take on the responsibility, the CCP basically pegs the cost of Internet censorship to a percentage of Internet use and commerce. This requires much less effort on the part of the government, which would instead devote resources into providing guidance rather than implementing it. The costs of such an approach, to the Internet companies and the general economy, may well be perfectly reasonable from the perspective of the CCP.

For the Chinese government, these sorts of incidents with Yahoo, and, more recently, its less cooperative interaction with Google, mean that heavy-handed tactics are on display for the entire world. It is hard to say how much the Chinese government minds this cost, relative to the benefit of security. The Chinese Government vehemently denies doing anything illegal, and has denied the use of hackers in response to the Google case.[59] The fact that Yahoo continues to operate in China and cooperate with the Chinese government indicates that the Chinese authorities have a strong hold over such companies. They will likely continue similar behavior, and China’s access to users private communications may only be limited by its ability to process content.

[59] Anonymous, “Guoxinban huiying ‘zhongguo xianzhi wangluo ziyou’ shuo [State Council Information Office Responds to claims that ‘China Restricts Internet Freedom’]” *Beijing Youth Daily,* 26 January 2010.

Technical Censorship

China's technical censorship methods are the world's most advanced,[60] and the technologies developed in China, such as packet filtering on routers, are now being used in other Southeast Asian countries. China uses a wide variety of technical measures, including absolute control of infrastructure (allowing the Government to simply cut off access), keyword filtering on search engines, packet filtering and use of monitoring software.

Keyword Filtering

Site blocking and keyword filtering are two of the best-known methods in Chinese Internet Censorship. The Open Net Initiative, a collaborative research effort between leading scholars in the field at Harvard University, the University of Toronto and Cambridge University, is at the forefront of studying Chinese technical filtering methods. These researchers argue that the Chinese approach to Internet monitoring is different from those of other countries because Chinese authorities keep an active and dynamic list of sensitive content to be blocked by firewalls and system controls.[61]

Keyword packet filtering works as packets of information are transmitted across routers. If a user is searching for a blacklisted term ("June 4th incident", for example), a telecommunications router is designed to recognize the key terms and send a reset packet

[60] Open Net Initiative, "*Internet Filtering in China,*" 15 June 2009. Accessed online 20 November 2009, http://opennet.net/research/profiles/china.

[61] Robert Deibert et al, *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge, MA: Harvard University Press, 2008.

to the originator in order to reset the connection.[62] Repeated attempts will cause the search to "time out." Contrary to the popular perception, a technical probe of the system finds that it the "Great Firewall of China" is not a firewall and it is not aimed at preventing information from coming into China, but rather to prevent forbidden information flowing within China. Most of the Internet filtering occurs on large telecommunications provider routers well within the telecom infrastructure. Of all the filtering measured by a U.S.-based research group, only ¼ of the filtering occurs on the first router they hit in China.[63] Filtering is not always consistent, perhaps because the requirement to filter packets can slow down routers. As a result, not every router filters packets. The same researchers found that, at times they could get communications all the way to their destination, 14 hops within China, without going through a router that scanned packets. [64] The system is, however, designed to frustrate and discourage the user into giving up on an "inappropriate" search.

Government censors maintain and frequently update a list of banned keywords and provide those lists to Internet service providers, like China Unicom and China Telecom, as well as to Internet companies charged with monitoring, like Baidu and Sina. In March 2009, a Baidu employee leaked a compressed file containing the lists of

[62] Jeddidiah Crandall, Daniel Zinn, Michael Byrd, Earl Barr and Rich East, "Concept Doppler: A Weather Tracker for Internet Censorship," (Paper Presented at the 14th ACM Conference on Computer and Communication Security October 2007).

[63] *Ibid.*

[64] *Ibid.*

hundreds of websites and key terms that the government sent to Baidu.[65] The list included some expected terms, like more than a dozen ways to search for Tiananmen and June 4th [66] as well as the names of adult children of prominent leaders, and some unexpected terms, like "test answers" and "AIDS." The long list of banned websites includes a large number of BBS websites; BBS systems are extremely popular in China, and are often used to publically discuss taboo subjects.[67] Keywords were divided into terms to be banned, and terms to simply monitor.

The keyword filtering system has a number of strengths. It is part of a general strategy to push disruptions in Internet service down to the user level.[68] Rather than delete an entire website containing a banned term or type of service, the system is simply designed to frustrate and obstruct individual users as they attempt to access unacceptable content. The regular updating of the blacklist of terms allows for a more nuanced approach; topics can be added or dropped as needed. This suits the purposes of the government and might also serve to make the system a little less predictable and obvious to users.

While Chinese routers are not catching everything in the current environment, the CCP might hope to adopt a comparative advantage approach to filtering. Censors aim to stop just enough traffic to frustrate and discourage a user, and prevent "unhealthy"

[65] Xiao Qiang, "Baidu Internal Monitoring and Censorship Document Leaked," *China Digital Times*, 30 April 2009, http://chinadigitaltimes.net/2009/04/baidus-internal-monitoring-and-censorship-document-leaked/

[66] Chinese Internet users interested in discussing Tiananmen quickly took to referring to June 4th as May 35th to get around this list.

[67] Rebecca MacKinnon, "Will the Revolution Be Blogged?" *Public Choice*, 134.2 (2008), available online http://www.springerlink.com/content/u65456nm4j3tx7p7/.

[68] Open Net Initiative, "*Internet Filtering in China,*" 15 June 2009. Accessed online 20 November 2009, http://opennet.net/research/profiles/china.

content from going viral online. The CCP can be successful even if they do not catch all banned content, because the objective could be to prevent such content from gaining traction. By obstructing the flow of information, the CCP buys time to catch harmful information trends before they have the chance to "go viral" among larger numbers of users.

However, there are a number of problems with this approach. One phrase that is commonly used to discuss Internet use in China (as well as cross-straits politics) is "playing edge balls."[69] Users can skirt right up to the line of acceptability, toeing the line until their activities are finally censored. This is partially true because the censors may not wish to be overly proactive in removing content, but it is also because the censors do not have time to review every single post. Even blatantly unacceptable posts can go undetected for a long time. Censors tend to focus on web pages that get very high volume.[70] In the process of creating a post on a BBS or blog, the automatic scanning terms may replace the offending item with some asterisks, but censors may not get to it until much later, even if it is obvious what the user was talking about.[71]

Censors face serious challenges from users talking around issues. For example, in the lead up to the anniversary of Tiananmen, those who wished to discuss the events referred to May 35th. Censors had already banned more than a dozen ways to say June 4th, so users relied on their readers' knowledge that there are only 31 days in May – the 35th day of May would therefore be the fourth day of the next month.

[69] Chabianqiu, a ping pong term, meaning to hit the ball that is on, but not quite over, the line.
[70] Nicholas Kristof. "In China It's ****** vs. Netizens," *The New York Times,* 20 June 2006
[71] *Ibid.*

The Chinese language is also particularly susceptible to another trend involving "psuedo-homonymns." The Chinese language has fewer actual syllable sounds than many Romance languages, but uses tones and different written characters to distinguish words. Savvy Chinese Internet users who know what the banned terms are can simply use different characters that are pronounced using the same sounds. There are more than 50 homonyms that sound like "Hu Jintao", including the proper tones, while using different written characters that are not so recognizable as related to the President. If the user is also willing to sacrifice tones, keeping only syllables, there are 300 ways to write the pseudo-homonyms for Chinese President's name. In China's popular BBS culture, that might be all that's required to get around the censors.

The increasing number of Chinese web users, exercising a growing array of tactics for getting around the censors, make scalability of this approach a challenge for the Chinese government. If China had 30,000 cybercops in late 2003, that force would have needed to grow considerably to keep up. The absolute cost of Internet monitoring has certainly increased as the number of users increased, although, because the cost and labor for Internet monitoring is partially undertaken by Internet companies, the cost to the Government may not increase linearly. All the same, the sheer increase in the number of users, who are generating more and more content on BBS forums, blogs, chat applications and social networking sites make the challenge daunting. The relative ease with which people are circumventing the censors may indicate that the increase in content is putting pressure on the system.

Certain aspects of keyword targeting, such as influencing search engine results for certain terms, probably will scale up well as more users come online. Once the system is set up to come back with certain results, there is no added per-user cost to operating the sanitized search engine. On the other hand, the large-scale packet filtering is hugely expensive and resource intensive. Filtering strategies rely on intervention at a relatively small number of points of control, or chokepoints.[72] Buying technological infrastructure for this is costly, and it leads to a reduction in connectivity speeds. Serious efforts to scan most of the content cannot happen without either huge investments in processing facilities needed to screen terabytes of data or the cost of a noticeably slowed Internet infrastructure.[73] This is likely why technical researchers find that not every search is censored at packet-monitoring routers.

Case study: Grass mud horse

In February of 2009, a very popular Chinese Internet video detailing the adventures of "grass mud horses" started gaining popularity on Chinese video hosting sites. The clip seems innocuous at first glance. It features a song about cute little grass mud horses that thrive in harsh deserts and defeat evil river crabs; the background music is a catchy children's ditty sung by young, innocent voices. Soon after the video begins, it becomes very apparent that the whole video is a satire. Grass mud horse is a pun, or pseudo-homonym, for a fairly offensive curse in Chinese (involving one's mother). The

[72] Open Net Initiative, "*Internet Filtering in China,*" 15 June 2009. Accessed online 20 November 2009, http://opennet.net/research/profiles/china.

[73] *Ibid.*

song thumbs its nose at censors, who are supposed to block foul language, by pushing the pun further and further into the obscene. The video also gets very political, by talking about how the grass mud horses will continue to thrive in harsh, unfriendly environments (Chinese cybersphere) and will defeat evil grass crabs. The crabs are a pun for harmonization, a thinly-veiled reference to Hu Jintao's political philosophy of a "harmonious society" which serves the government will by encouraging people to avoid conflict and work together to find problems. When Internet users have their posts deleted, they will often repost and point out that they have been "harmonized."

The video got a fair amount of attention online in China, and the grass mud horse has come to be the symbol of censorship resistance online. The Chinese dissident community has warmly embraced grass mud horses as a mascot for their cause. Prominent intellectual blogger Ms. Cui Wei-ping wrote a serious essay in support of the ideals behind the video entitled, "I am a grass mud horse."[74] There have even been sales of stuffed grass mud horses. Blogger Ai Weiwei, son of famous Chinese author Ai Qing and a prominent thorn in the side of Beijing authorities, posted an iconic picture of himself naked, holding a strategically placed stuffed grass mud horse, on his blog. Western media also picked up on the story. By late March 2009, Chinese Propaganda officials called for a grass mud horse "clean up", citing the international media attention on grass mud horses as an embarrassment.[75]

[74] Wei-ping Cui, "Wo shi yi ji caonima [I am a grass mud horse]," 19 February 2009. Accessed online 5 March 2009, http://www.hecaitou.net/?p=4723.

[75] Michael Wines, "Censors Bar Mythical Creature," *The New York Times.* 20 March 2009.

It is possible to overstate the significance of the grass mud horse phenomenon. After all, it is possible, and even likely, that the video resonated with so many Chinese netizens more because it is so funny than because it is subversive. Most Chinese Internet users primarily go online for entertainment[76] and not to engage in forbidden discussions of political topics. To these netizens, censorship efforts aimed at foul language and sexually charged content are much more of a real infringement on their personal choice than restrictions on political content.

Despite the lack of insight into exactly why Chinese netizens enjoyed the grass mud horse video, it is still a useful case. The video exemplifies the technical burden and challenges of packet filtering. Chinese censors cannot block all pseudo-homonyms for banned key terms without impeding legitimate communication. If Chinese censors banned or flagged all homonyms and pseudo-homonyms for sensitive terms from the Internet, all Internet communications would come to a halt. Certainly the Government's hand in censorship would become strikingly apparent to the user.

Furthermore, scanning audio and video content for terms is more technically challenging than scanning text. In order to attempt this, the CCP would have to develop new technologies that could scan and accurately recognize voice. This, too, might be rendered next to impossible because of the use of tones in the Chinese language. The file size of such communications would also substantially increase the burden on China's

[76] China Internet Network Information Center (CNNIC), "Zhongguo hulian wangluo fazhan zhuankuang tongji baogao [China's Internet Network Development Situation Statistical Report]", January 2010. Accessed online 20 February 2010, http://www.cnnic.cn/uploadfiles/pdf/2010/1/15/101600.pdf.

already burdened packet-filtering routers. This might explain why video hosting sites in China are often slow, and YouTube is almost always inaccessible.

Using a Heavy Hand: Cutting off Internet Access

The CCP maintains a firm grip on the telecommunications infrastructure through the Ministry of Industry and Information Technology (MIIT). MIIT can grant and revoke licenses to operate, which is a key part of Chinese control, as seen in the discussion of Internet service companies operating in China. MIIT also oversees infrastructure development for censorship. MIIT can and does instruct telecom providers like China Unicom, Telecom and Railcom to install packet-filtering routers and remain in compliance with censorship strategies. This includes informing telecom companies what kinds of services they can and cannot provide. At its most drastic, it involves cutting off all Internet access to a city or geographical region.

The advantages of having so much control are obvious. The CCP, through MIIT, can immediately halt all communications that might threaten government power or domestic stability. Television and hard-copy newspapers can serve as a source of news for a city or region while Internet access is cut off. When the Chinese government is threatened and they do not feel they can effectively monitor all web content into and out of an area, this is an effective, if blunt, weapon. In terms of scalability, this type of action is equally effective regardless of how many users are going online.

Of course, its downsides are just as easily apparent. For a long time, no one believed that the Chinese government would actually cut Internet access to an entire region. After all, the initial purpose of allowing the Internet in was to fuel the economic growth that underpins CCP legitimacy, so severing service would defeat the purpose; it might even lead to an economic setbacks. Furthermore, MIIT and the CCP are not immune to pressure, especially from elites in society. The party does not wantonly arrest certain dissidents and outspoken critics and sentence them to years in prison because it does not wish to alienate affluent intellectuals in the city. For every prominent government critic arrested in China, there are several more that continue to "play edge balls."

MIIT also occasionally has to loosen its control on the infrastructure under pressure from consumer demand and telecom lobbying. For years, MIIT did not legally allow the use of Voice over Internet Protocol (VoIP) service or the use of an alternate cell phone technology, the "little smartie." This could have been because such technologies are hard to monitor, but it could also be because providers of other types of service didn't want something new to manage. In both instances, however, consumer demand and unauthorized use grew to such a level that bowing to pressure and legalizing the technologies seemed the only logical solution.[77]

Case study: Xinjiang 2009

The summer 2009 riots in Xinjiang are a quintessential example of how the Internet plays a role in exacerbating threats to domestic stability, and how the Chinese government can still exercise absolute control. In July 2009, tensions in Urumqi

[77] Irene Wu, *From Iron Fist to Invisible Hand: The Uneven Path of Telecommunications Reform in China,* Stanford: Stanford University Press, 2009.

exploded over news of a conflict between Uyghurs, the Muslim ethnic minority primarily settled in Xinjiang, and a Han Chinese woman hundreds of miles away from Xinjiang in Guangdong Province. The problems started when a Han Chinese woman was supposedly frightened by some Uyghur workers and screamed. During a police investigation, the Uyghurs, who are regularly the target of discrimination in China, were falsely accused of assaulting the woman. News of the incident at the Southern Chinese factory spread like wildfire on the Internet. Chinese Uyghurs hundreds of miles away in Xinjiang felt that this was yet another example of Uyghurs being singled out by Chinese authorities, usually ethnically Han Chinese, and protested in front of Government buildings on 5 July.

What happened next is disputed. Chinese authorities claim the Uyghurs initiated violence during their protests. The Uyghurs claims that Chinese authorities took initiative in shooting some of the Uyghurs. The Chinese authorities later admitted to having shot some of the Uyghur protestors, but claimed that they were only targeting the most violent and provocative of the Uyghurs.[78] Riots followed as the Uyghurs dispersed. According to official figures, 200 were killed and 1700 were wounded. Official media claimed that Han Chinese were overwhelmingly the victims of the violence. A few days later, outraged Han Chinese vigilant groups took to the streets to seek revenge. More destruction, violence and looting occurred until the authorities were able to regain order in the city by imposing strict curfews.

The Internet undoubtedly played a role in the quick dissemination of the story from Guangdong Province to Urumqi in Xinjiang Province. The Director of the Xinjiang

[78] Gillian Wong, “China Says Recent Urumqi Unrest was Premeditated,” *The Guardian*, 20 July 2009.

Telecommunications Administration Yang Maofa cited intercepted telephone calls as evidence that an American Uyghur expatriate, Rabiya Kadeer[79], played a role in fanning the flames and encouraging anti-government violence.[80] Ms. Kadeer denies having encouraged violence and the government and the Chinese authorities have failed to produce their intelligence.[81] Uyghur expert Gader Bovington at Indiana University pointed out that the Chinese authorities have a great deal of incentive to describe the riots as premeditated and incited by outside forces, because it completely avoids the need to discuss the underlying causes for Uyghur discontent.[82]

In response to the violent situation, Chinese authorities cut off all Internet service into Xinjiang, as well as text messaging service, with a few limited exceptions. Journalists were allowed to use a central Internet center in Urumqi to report on events, showing that the Chinese learned from the messy handling of Tibet in 2008.[83] In fact, several articles were devoted to the Chinese authorities' uncharacteristic permission for unfettered reporting, although some journalists pointed out that no Uyghurs would speak to them out of fear of retribution from public security forces.[84]

[79] Ms. Kadeer is a much despised figure amongst Chinese authorities, and is quickly becoming to Xinjiang what the Dalai Lama is to Tibet in the eyes of the authorities.

[80] Gillian Wong, "China Says Recent Urumqi Unrest was Premeditated." *The Guardian*. 20 July 2009.

[81] *Ibid.*

[82] *Ibid.*

[83] Lucy Hornby, "China Says Xinjiang Riot Openness a Success," *Reuters* 31 July 2009, accessed online 4 March 2010, http://in.reuters.com/article/worldNews/idINIndia-41464520090731?pageNumber=1&virtualBrandChannel=0

[84] Jonathan Ansfield, "China Starts to Lift Region's Web Blackout," *The New York Times*, 30 December 2009.

The Internet blackout lasted until 30 December 2009, when two official news media outlets, *The People's Daily* and *Xinhua* were made available online in Xinjiang.[85] At the time access was re-granted, users were not allowed to use BBS forums or send email. While some large Chinese businesses were able to apply for a special permission to get Internet access, small businesses could not. The loss of Internet connection was a huge disruption to commerce and researchers in the area.[86] In mid-January 2010, text-messaging services returned. Gradually full service is being restored.

Xinjiang authorities acknowledge that the Internet ban brought significant inconvenience to the region, but asserted it was necessary to regain stability in the region. Although reliable estimates of the economic cost may never be accurately measured, it is likely that the complete freeze on online communications was hugely costly. Businesses struggled and people traveled hundreds of miles to collect necessary information.[87] The economic impact may not even be limited to the June-December Internet blackout. The very fact that the government is willing to consider such measures against critical infrastructure might make businesses less enthusiastic about investing in Xinjiang. China's official end-of-year Internet statistics report shows that while China's poorer provinces experienced double-digit growth in Internet penetration (some as high as 50%), Xinjiang's growth in Internet penetration in 2009 was 1.4%,[88] likely indicating that rapid growth in the first half of the year came abruptly stopped with the Internet outage.

[85] *Ibid.*

[86] Richard Stone. "Internet Blockade in Xinjiang Puts a Strain on Science," *Science* 326.5959 (2009): 1471.

[87] *Ibid.*

[88] China Internet Network Information Center, "Twenty-third Statistical Survey Report on the Internet

New Technical Approaches: Monitoring Software

Most Chinese approaches to Internet monitoring are proactive measures aimed at the entire system, rather than specific users. As seen in several of the above cases, however, the system is far from perfect. Users who wish to circumvent the system usually can, and the cost of the system is likely very expensive. The strength of China's Internet control apparatus is in preventing users from wanting to circumvent the system, but the Chinese authorities would be wise to worry about their ability to control those who want to beat the system. The Chinese MIIT will continue to work on ways to adapt to the changing online environment and maintain their hold on discourse. In the summer of 2009, the Chinese attempted to roll out a drastically different approach in a client-based monitoring software package called Green Dam Youth Escort. Ultimately, for a variety of reasons to be discussed, the software program was a failure, but the aborted program remains useful as an example of Chinese approaches to staying on top of the Internet problem and the limits of their power to do so.

Monitoring software is fundamentally different from packet filtering or online monitoring of posted content because it is installed on each user's machine. The software watches and tracks the individual user's every move on the computer. Monitoring software is attractive to government censors on a variety of levels. From a technical and cost perspective, such software brilliantly solves the problem of high resources required for packet filtering by distributing the computational costs of such efforts down to the

Development in China," issued March 23, 2009, http://www.cnnic.net.cn/uploadfiles/pdf/2009/3/23/131303.pdf.

individual user.[89] Packet filtering is currently suffering from the burden of extra online users, while monitoring software has no problem scaling up to meet the demands placed on the system by new users. Each individual computing unit is capable of watching over the user, and the software can be periodically updated to address current concerns of the Government. Furthermore, it potentially places new capabilities in the hands of the government. Such programs could be used to install a back door on all computers with the program installed, enabling government efforts to deter political behavior through annoyance, engage in data mining and conduct real time surveillance of Internet use.

Case Study: Green Dam Youth Escort

In June 2009, MIIT issued a directive that all new home computing units sold in China must come preinstalled with Green Dam Youth Escort Software. Green Dam, the product of a Chinese software company, was to be installed not just on computers manufactured by Chinese companies, but also by foreign companies like Dell that sell computers in China.

Green Dam was not entirely new to China. It was already installed on numerous computers in Chinese schools in early 2009.[90] The government justified the program by emphasizing that it was meant to protect children from pornography and obscenity. Teachers complained that the program was inconsistent, and had a habit of closing down

[89] Open Net Initiative, "*Internet Filtering in China,*" 15 June 2009. Accessed online 20 November 2009, http://opennet.net/research/profiles/china.

[90] Robert Faris, Hal Roberts and Stephanie Wang, "China's Green Dam: The Implications of Government Control Encroaching on the Home PC," *Open Net Initiative Bulletin*, 2009. Accessed online, 8 March 2010, http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc

all websites with pictures that contained too much of the color yellow.[91] The program works by scanning images and trying to identify pornography, in part by identifying the colors of the image. While this might use a large amount of system resources, they are resources on the individual users PC, rather than the resources of the national telecom infrastructure.

MIIT's push towards an unprecedented new strategy makes a lot of sense in the context of Chinese online demographic changes. Not only has the number of Internet users grown dramatically, but they are generating a great deal more content on social media sites and chat applications. Furthermore, as incomes grow and Internet use becomes more pervasive, more and more users are accessing broadband service from their own homes.[92] This puts the outside the reach of the extensive additional monitoring procedures in place at Internet cafes.

The reaction to this announcement was forceful and instantaneous, both inside and outside of China. Technical experts outside the country played a large role in criticizing the Green Dam software, and did so very successfully. Researchers at the University of Michigan pointed out that Green Dam is so full of security vulnerabilities that just about any site the user visited would have the capability to take control of the user's machine.[93] These problems were obvious enough that they were discovered within hours of testing and were apparent to technical experts inside and outside of China.[94]

[91] *Ibid.*

[92] Guo Liang, "China Internet Project Survey Report, 2007: Surveying Internet Usage and its Impact in Seven Chinese Cities," *Chinese Academy of Social Sciences*, 2007.

[93] Scott Wolchok, Randy Yao, and J. Alex Halderman, "Analysis of the Green Dam Censorware System," Computer Science and Engineering Division, The University of Michigan, Revision 2.4,

Technical analysis revealed that the program was not very good at its stated objective of targeting porn. The program's performance was highly random, closing programs with innocent pictures while allowing actual pornography to get through.[95] The program was highly irritating to the user, as it closed word processors and Internet browsers if users typed selected keywords or forbidden URLs. Cursory analysis showed that the program went far beyond the scope of porn and obscenity; the program interfered with a number of politically-oriented keywords and shut Internet browsers that attempted to access controversial media outlets.[96]

A U.S.-based software company alleged that the program blatantly stole software code from one of its products, and threatened to sue any U.S. company that cooperated with the government mandate in China. [97] Companies quickly began to protest as they saw that compliance with the mandate was going to be a publicity and litigation nightmare.[98] No U.S. Company wanted to be the next Yahoo to be hauled in front of Congress to testify.

Chinese reception was barely more welcoming. Green Dam Youth Escort was wildly unpopular with the Chinese public, so much so that the state mouthpiece, *The*

June 11, 2009, http://www.cse.umich.edu/~jhalderm/pub/gd/.

[94] Robert Faris, Hal Roberts and Stephanie Wang, "China's Green Dam: The Implications of Government Control Encroaching on the Home PC," *Open Net Initiative Bulletin*, 2009. Accessed online, 8 March 2010, http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc .

[95] Open Net Initiative, "*Internet Filtering in China*," 15 June 2009. Accessed online 20 November 2009, http://opennet.net/research/profiles/china.

[96] *Ibid.*

[97] Rebecca MacKinnon, "After the Green Dam Victory," *Center for Strategic and International Studies Freeman Report*, July 2009. Accessed online 15 January 2009, http://csis.org/files/pubication/fr09n0607.pdf.

[98] Rebecca MacKinnon. "The Green Dam Phenomenon," *The Wall Street Journal*, 18 June 2009

People's Daily and another prominent paper, *Caijing*, both openly criticized it.[99] Chinese bloggers called the program "crony-ware" and "corrupt-ware," and said that the program was only mandated because the Chinese software company, Jinhui, lobbied the government to mandate their ineffective program to boost sales. The very poor performance of the program, and its sometimes comic failure to perform its stated objectives, lend credence to the accusation that the program was mandated more because of corrupt backroom dealings than a drive to pursue new technology. Chinese media insiders claimed that the Green Dam software program failed because the government bureaucracy did not universally accept it and opponents quietly supported critics.[100] In the end, the government backed down from its mandate.

Green Dam's failure may serve as a reminder that Internet censorship in China is a consensus-based process, in which a variety of stakeholders including different government agencies and private sector IT companies must all cooperate.[101] It serves as a further example that the CCP and MIIT are not immune to pushback from ordinary Internet users and companies, and that their hold may not always be so absolute. The Chinese government may not be able to pursue such blatant censorship strategies without incurring the wrath of Chinese netizens and the criticism of technical experts inside and outside of China. The very nature of a software program installed on all user PCs makes it more transparent and vulnerable to outside assessment.

[99] Rebecca MacKinnon, "After the Green Dam Victory," *Center for Strategic and International Studies Freeman Report*, July 2009. Accessed online 15 January 2009, http://csis.org/files/pubication/fr09n0607.pdf.
[100] *Ibid.*
[101] *Ibid.*

It is possible that the pressures of controlling the Internet may push Chinese authorities into trying another, better designed software client. If the Green Dam experiment had been better executed, it might have been able to screen key words without being too obtrusive to the user or causing system problems. The authorities could have avoided much of the International blowback over the program by ensuring that the client worked more smoothly and did not use the stolen code from another software program.

Even if the program was not so poorly executed, however, it might still have faced insurmountable problems. Foreign hardware companies might still hesitate to cooperate so openly in government control, especially as no corporation could credibly believe the Chinese were only looking to control pornography after the Green Dam catastrophe. Moreover, the inherent nature of a software client makes it vulnerable not just to assessment by the outside world, but also to exploitation.

To understand this shortcoming in client-based monitoring software, consider the case of cheating in online computer games. Veteran game designer Raph Koster writes: "Never trust the client. Never put *anything* on the client. The client is in the hands of the enemy." [102] Koster is referencing the fact that would-be cheaters must have access to the game client software installed on their personal computers in order to be able to play the game in the first place. However, this means that the game developer cannot trust that any information recorded on the game client will remain confidential. Instead, any information that might grant an advantage to the unscrupulous player – for example, the

[102] Raph Koster, "The Laws of Online World Design," accessed online, 10 April 2010 http://www.raphkoster.com/gaming/laws.shtml

location of a hidden treasure - must be kept on the game's servers, under the developers' control.

The same issue could arise with client-based Internet filtering software in China. As with the online game, a successor to Green Dam might be more easily evaded by domestic dissidents than system-level filtering, as the dissidents could examine their own hard drives to learn what filtering algorithms and keywords were in use. Given heightened concerns about cyber warfare, the CCP would also have to carefully weigh the benefits of installing a program – which enemies could potentially obtain and reverse engineer for vulnerabilities – on computers all around the country.

Conclusions and Implications

These examinations of Chinese technical and non-technical censorship methods reveal that, while Chinese proactive strategies to shape the online experience and discourage users from seeking certain types of content are often successful, the monitoring apparatus is increasingly struggling with the amount of content Chinese users are putting online. Furthermore, users who wish to circumvent censorship technologies often easily defeat them. Increased attempts by the Chinese government to amplify their censorship strategies sometimes meet with scorn, as seen with the popularity of the Grass Mud Horse, or with outrage, as seen in the response to Green Dam software. On the other hand, Chinese success in encouraging mistrust of the Internet shows that their proactive non-technical methods of controlling Internet discourse might be most successful.

The case studies described above also show that, while much scholarly and Chinese government attention has been focused on preventing dissidents from using the Internet to promote free speech and democracy, the Internet may be most dangerous to CCP rule when it facilitates civil unrest resulting from social inequities or Government corruption. Chinese netizens gaining information from online sources may become disillusioned when they find that the government is hiding or distorting the truth. Western media tends to focus on pro-democracy activities online, like the signing of Charter 08, but the greater threat to the CCP may come in the information citizens get online about shoddy construction in Sichuan or the government role in covering up the melamine-tainted milk scandal. The government has successfully controlled perceptions of the Internet; users of the Internet trust it as a source of information much more than non-users.[103] Too many government corruption scandals could change the tide of public opinion over the most reliable source of information.

The challenges that the Chinese Government faces in dealing with Internet censorship have policy implications for both the Chinese Communist Party as well as Western governments who want to undermine their authority. New demographic shifts in Internet usage abroad may cause new weaknesses in the control apparatus of the CCP. If the Chinese government is facing a problem with scalability, they may need to consider major revisions to what is widely regarded a highly successful censorship regime. The United States, on the other hand, should take advantage of any apparent future weaknesses in focusing its free-speech efforts.

[103] Guo Liang, "China Internet Project Survey Report, 2007: Surveying Internet Usage and its Impact in Seven Chinese Cities," *Chinese Academy of Social Sciences*, 2007.

The United States opposes censorship and encourages all countries to allow for the free exchange of information and ideas. On the other hand, the current administration is overwhelmed with a domestic agenda including health care and a crippling recession, as well as the management of two ongoing conflicts. This conflict was comically apparent during President Obama's trip to China, during which he very carefully responded to a question about U.S. views on Internet controls by saying that he was a big fan of "non-censorship." The U.S. government may hold this position, and pressure from Congress forced the Administration to address the issue, but this must be delicately balanced against other policy priorities vis-à-vis China.

Following the infamous hacking of Google email accounts in early 2010, Secretary of State Hillary Clinton made a speech reaffirming U.S. commitment to the free flow of information and ideas throughout the world. The U.S. already invests some money in Internet technologies that enable free speech by supporting technologies that help citizens of foreign countries circumvent the Internet controls put in place by authoritarian governments. For example, the U.S. may fund technical research that will underpin future web proxy services that allow prominent Chinese bloggers to post content online without going through critical censorship checks.

This study, which examines how different Chinese censorship technologies will stand up to demographic shifts and changing Chinese Internet usage, might better inform the U.S. government and activists where to invest their time and energy to exploit technical weaknesses in the system. The U.S. can also continue to support the research of technical experts who expose censorship techniques and effectively limit Chinese options, as was seen with the recent Green Dam Software experiment.

Table: Summary of Chinese Censorship Methods and Scalability

	Propaganda/ Manipulating Online Environment	**Co-Opting Corporations**	**Keyword Packet Filtering**	**Terminating Access**	**Monitoring Software**
User- or System-Level	System	System	System	System	User
Technological Approach	No	No	Yes	Yes	Yes
Capital Resource Intensive	No	No	Yes	Yes	Yes, but distributed to user
Labor Resource Intensive	No for propaganda, yes for "astroturfing"	Yes, but distributed to corporations	No	No	No
Cost to CCP	Low	Low to the CCP, but moderate for the economy	High	High economic cost	Low- Cost distributed to user
Scalability	High	High	Low	High, but widespread use impractical	High, but possibly unfeasible

There are even clearer policy implications for the Chinese government. In general, Chinese Internet control is most successful when the government manages to prevent the user from wanting to seek out sensitive content on the web. In this respect, China’s non-technical censorship such as propaganda campaigns and shaping the online environment are more successful and scalable. Chinese censorship technologies like keyword filtering are particularly vulnerable to the rapid growth of content creation in

China, and the CCP will have to reevaluate their strategy. One possibility will be for the CCP to lean more heavily on censorship technologies that do not suffer from scalability problems. For example, the CCP could strengthen propaganda campaigns that encourage mistrust of the Internet. Another option would be to invest more in strengthening current technologies to better handle the increase in users.

The CCP originally allowed the Internet to flourish in China because it deemed that the economic benefit from the Internet outweighed its political risks. If certain censorship strategies, like the employment of public security personnel to monitor online content, become very expensive as the amount of content grows, the Chinese may have to reevaluate how much they are willing to spend on Internet censorship. Of course, domestic stability is the highest priority for the CCP, but if that domestic stability can be achieved through more efficient means, than the CCP may gravitate toward less labor-intensive censorship techniques.

The Green Dam Software experience presented both a solution and a limit to the CCP. Client based software programs move the computational burden of technical censorship to the user, but they expose the government to criticism and generate ill will with the online community. The CCP will continue to face the issue of visibility. As the Internet becomes more a part of everyday life in China, especially in urban environments, people may begin to recognize the heavy hand of the government in ways that they do not currently consider. The CCP is regularly shutting down social networking sites and video hosting sites that are very popular with younger Internet users. While not likely to be an insurmountable problem for the CCP, it may influence the way Chinese netizens view the government.

Domestic and international scrutiny and transparency may limit CCP options. The international scrutiny of censorship software deployed by the CCP meant that the Chinese government could not be careless in implementation. Furthermore, the domestic pushback on such programs might also indicate some practical limits on how blatant and intrusive the Chinese government can be.

China’s Internet monitoring apparatus is often hailed as the world’s most sophisticated, advanced and nuanced censorship system. That nuance and sophistication are the result of great investment and resource dedication by the CCP. If such techniques falter under the weight of explosive Chinese Internet growth, then the Chinese may have to choose between investing significantly more capital and labor in their censorship system, or accepting a system that is more blunt and heavy handed in implementation.

For those countries that wish to censor online content, China has long served as the model. Their nuanced approach allowed economic growth and fostered perceptions of an Internet that was free from the heavy hand of the government. Other countries in Southeast Asia have sought to emulate Chinese packet filtering methods. The irony may be that as China’s Internet penetration rate grows, it may move more towards the model of Iran, which uses blunter tools of Internet censorship and is more visible to the user. In the end, it may be that China’s low-tech solutions are superior to its Great Firewall.

Bibliography

Anonymous, “Guoxinban huiying ‘zhongguo xianzhi wangluo ziyou’ shuo [State Council Information Office Responds to claims that ‘China Restricts Internet Freedom’]” *Beijing Youth Daily,* 26 January 2010.

Jonathan Ansfield, “China Starts to Lift Region’s Web Blackout,” *The New York Times,* 30 December 2009.

Associated Press, "Yahoo! Settles Lawsuit by Families of Chinese Journalists," *The International Herald Tribune*, 14 November 2007. Accessed online 1 March 2010, http://www.iht.com/articles/2007/11/14/business/yahoo.php.

David Bandurski, “China’s Guerilla War for the Web, “ *Far Eastern Economic Review,* July 2008.

Dick Beveridge, “China Riot Traced to Teen’s ‘Unintentional Scream’ Xinhua Says,” *Bloomburg News,* 9 July 2009. Accessed online 4 March 2010, http://www.bloomberg.com/apps/news?pid=20601087&sid=awcbCPNKDyGQ.

Corey Boles, Don Clari and Pui-Wing Tam, “Yahoo’s Lashing Highlights Risk of China Market,” *The Wall Street Journal*, 7 November 2007.

Keith Bradsher, “China Enacting a High-Tech Plan to Track People,” *The New York Times,* 12 August 2007.

Anne-Marie Brady, “Guiding Hand: The Role of the CCP Central Propaganda Department in the Current Era,” *Westminster Working Papers in Communication and Culture,* 3.1 (2006), 58-77.

Loretta Chao and Juliet Ye. "Corndog Speaks of 'War of Internet Addiction'" *Wall Street Journal China Real Time Blog*, 19 February 2010, accessed online 2 March http://blogs.wsj.com/chinarealtime/2010/02/19/corndog-speaks-on-war-of-internet-addiction/.

Michael Chase and James Mulvenon, *You've Got Dissent: Chinese Dissident Use of the Internet and Beijing's Counter Strategies,* Santa Monica, CA: Rand, 2002.

China Internet Network Information Center, "Twenty-third Statistical Survey Report on the Internet Development in China," issued March 23, 2009, http://www.cnnic.net.cn/uploadfiles/pdf/ 2009/3/23/131303.pdf.

China Internet Network Information Center (CNNIC), "Zhongguo hulian wangluo fazhan zhuankuang tongji baogao [China's Internet Network Development Situation Statistical Report]", January 2010. Accessed online 20 February 2010, http://www.cnnic.cn/uploadfiles/pdf/2010/1/15/101600.pdf.

Richard Clayton et al. "Ignoring the Great Firewall of China." (Paper presented at the 6th Workshop on Privacy Enhancing Technologies, Cambridge, 2005).

Jeddidiah Crandall, Daniel Zinn, Michael Byrd, Earl Barr and Rich East, "Concept Doppler: A Weather Tracker for Internet Censorship," (Paper Presented at the 14th ACM Conference on Computer and Communication Security October 2007).

Wei-ping Cui. "Wo shi yi zhi caonima [I am a grass mud horse]" 19 February 2009. Accessed online 5 March 2009, http://www.hecaitou.net/?p=4723.

G. Elijah Dann and Neil Haddow, "Just Doing Business or Doing Just Business: Google, Microsoft, Yahoo! And the Business of Censoring China's Internet," *Journal of Business Ethics,* 79 (2008): 219-234.

Robert Deibert et al, *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge, MA: Harvard University Press, 2008.

Robert Faris, Hal Roberts and Stephanie Wang, "China's Green Dam: The Implications of Government Control Encroaching on the Home PC," *Open Net Initiative Bulletin*, 2009. Accessed online, 8 March 2010, http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc

Peter Ford. *"Sources in Urumqi? They Are Very Hard to Come By,"* Christian Science Monitor Blog, 6 July 2009. Accessed online 5 March 2010, http://www.csmonitor.com/World/Global-News/2009/0706/sources-in-urumqi-theyre-very-hard-to-come-by.

Howard French, "Chinese Censors and Web Users Match Wits," *The New York Times,* 4 March 2005.

Nina Hachigian, "China's Cyber Strategy," *Foreign Affairs*, 80.2 (Mar-Apr 2001): 118-133.

Eric Harwit and Duncan Clark, "Shaping the Internet in China: Evolution of Political Control over Network Infrastructure and Content," *Asian Survey* 41:3 (May-June 2001): 377-408.

Jonathan Hassid, "Controlling the Chinese Media: An Uncertain Business," *Asian Survey* 48.3 (2008): 414-430.

Muray Hierbert, “Counters to Chinese Checkers,” *Far East Economic Review*, 165.44 (7 November 2002): 24.

Lucy Hornby, “China Says Xinjiang Riot Openness a Success,” *Reuters*, 31 July 2009, accessed online 4 March 2010, http://in.reuters.com/article/worldNews/idINIndia-41464520090731?pageNumber=1&virtualBrandChannel=0

Internet Society of China, “Zhongguo hulianwang xingye zilu gongyue [Public Pledge of Self Regulation and Professional Ethics for China Internet Industry],” 24 March 2002. Accessed online 5 March 2010, http://www.isc.org.cn/20020417/ca39030.htm

Andrew Jacobs, “China Restores Text Messaging in Xinjiang,” *The New York Times*, 17 January 2010.

Liu Jun, “Qiyue hou chuchang he xiaoshou diannao jiang yuzhuang lyuse shangwang guolu ruanjian [All Computers on the Market After 1 July Will Be Pre-Installed with Green Dam Software]” *Xinhua News*, 9 June 2009, http://tech.sina.com.cn/it/2009-06-09/17073163327.shtml.

Shanthi Kalathil, “China’s Dot-Communism,” *Foreign Policy*, 122 (Jan/Feb 2001): 2001.

Shanthi Kalathil and Taylor Boas. *Open Networks, Closer Regimes: the Impact of the Internet on Authoritarian Rule*, Washington, DC: Carnegie Endowment for International Peace, 2003.

Shanthi Kalathil and Taylor C. Boas. “The Internet and State Control in Authoritarian Regmies: China, Cuba and the Counterrevolution,” *Carnegie Endowment for*

International Peace Working Papers, No. 21, July 2001. Accessed online 5 March 2010, http://www.carnegieendowment.org/files/21KalathilBoas.pdf

Raph Koster, “The Laws of Online World Design,” accessed online 10 April 2010, http://www.raphkoster.com/gaming/laws.shtml.

Nicholas Kristof, “On the Ground: Microsoft and Chinese Censorship,” *The New York Times Blogs*, 24 June 2009. Accessed online 15 February 2010, http://kristof.blogs.nytimes.com/2009/06/24/microsoft-and-chinese-censorship/?scp=4&sq=kristoff%20china%20internet&st=cse.

Nicholas Kristof, “In China It’s ****** vs. Netizens,” *The New York Times*, 20 June 2006.

Jonathan Landreth, “China Reconnects Xinjiang Province to the Web—Very Slightly,” *Christian Science Monitor*, 30 December 2009.

Michelle Lau, “Internet Development and Information Control in the People’s Republic of China,” *Congressional Research Service Report for Congress*, Washington, DC: Government Printing Office, 2005.

Guo Liang, “Approaching the Internet in Small Chinese Cities,” *Chinese Academy of Social Sciences*, 2003.

Guo Liang, “China Internet Project Survey Report, 2007: Surveying Internet Usage and its Impact in Seven Chinese Cities,” *Chinese Academy of Social Sciences*, 2007.

Jane Macartney, “Internet Addiction Made an Official Disorder in China.” *The London Times*, 11 November 2008.

Rebecca MacKinnon, “After the Green Dam Victory,” *Center for Strategic and International Studies Freeman Report*, July 2009. Accessed online 15 January 2009, http://csis.org/files/pubication/fr09n0607.pdf.

Rebecca MacKinnon, “Are China’s Demands for ‘Self-Discipline’ Spreading to the West?” *McClatchy Newspapers Syndicated Service*, 18 January 2010, Accessed online 20 February 2010, http://www.mcclatchydc.com/2010/01/18/82469/commentary-are-chinas-demands.html.

Rebecca MacKinnon, “Testimony Submitted for the Record for the Hearing ‘Google and Internet Control in China,’” Congressional-Executive Commission on China, 24 March 2010. Accessed online, 10 April 2010, http://rconversation.blogs.com/MacKinnonCECC_Mar24.pdf.

Rebecca MacKinnon. “The Green Dam Phenomenon,” *The Wall Street Journal*, 18 June 2009.

Rebecca MacKinnon, “Will the Revolution Be Blogged?” *Public Choice*, 134.2 (2008), available online, http://www.springerlink.com/content/u65456nm4j3tx7p7/.

Open Net Initiative, “*Internet Filtering in China,”* 15 June 2009. Accessed online 20 November 2009, http://opennet.net/research/profiles/china.

Xiao Qiang, “Baidu Internal Monitoring and Censorship Document Leaked,” *China Digital Times*, 30 April 2009, http://chinadigitaltimes.net/2009/04/baidus-internal-monitoring-and-censorship-document-leaked/

C. Schultz, “A Profile of Blogger Ai Weiwei,” Accessed online 3 March 2010, http://www.socialtext.net/cdt/index.cgi?blogger_profile_ai_weiwei.

Andrew Scobell, “Terrorism and Chinese Foreign Policy,” in *China Rising: Power and Motivation in Chinese Foreign Policy*, ed. Yong Deng and Fei-ling Wang, Lanham: Rowman and Littlefield, 2005.

Christine Seib, “Is There Such a Thing as Internet Addiction?” *The London Times*, 8 March 2010.

David Shambaugh, *China’s Communist Party: Atrophy and Adaption*, Ewing, NJ: University of California Press, 2008.

David Shambaugh, “China’s Propaganda System: Institutions, Processes and Efficacy,” *The China Journal*, vol. 57 (2007): 25-58.

Andrew Shapiro, “The Internet,” *Foreign Policy* 115 (1999): 14-27.

Tamara Renee Shie, “The Tangled Web: Does the Internet offer Promise or Peril for the Chinese Communist Party?” *Journal of Contemporary China*, 13.40 (2004): 523-540.

Richard Stone, “Internet Blockade in Xinjiang Puts a Strain on Science,” *Science* 326.5959 (2009): 1471.

U.S. House, Committee on Foreign Relations. *Yahoo! Inc.’s Provision of False Information to Congress*, Hearing 6 November 2007, Washington: Government Printing Office, 2007.

Choy Dick Wan, 'The Shi Tao Case: its Development in Mainland China', *Journal of Contemporary China*, 18.61 (2009), 517 -539.

Ian Weber and Lu Jia, “Internet and Self-regulation in China: the Cultural Logic of Controlled Commoditization.” *Media Culture Society,* 29.5 (2007): 772-789.

Michael Wines, “In Latest Upheaval, China Applies New Strategies to Control of Information,” *The New York Times,* 7 July 2009.

Michael Wines, “Censors Bar Mythical Creature,” *The New York Times.* 20 March 2009.

Scott Wolchok, Randy Yao and J. Alex Halderman, “Analysis of the Green Dam Censorware System” Scott Wolchok, Randy Yao, and J. Alex Halderman, "Analysis of the Green Dam Censorware System," Computer Science and Engineering Division, The University of Michigan, Revision 2.4, June 11, 2009, http://www.cse.umich.edu/~jhalderm/pub/gd/.

Gillian Wong, “China Says Recent Urumqi Unrest was Premeditated,” *The Guardian,* 20 July 2009.

Irene Wu. *From Iron Fist to Invisible Hand: The Uneven Path of Telecommunications Reform in China,* Stanford: Stanford University Press, 2009.

Xinhua News, “Zhongguo qingshaonian wangying baogao (2009) fabu [2009 Report on Chinese Internet Addiction Published]” 3 February 2010, Accessed online 15 February 2010, http://news.xinhuanet.com/internet/2010-02/03/content_12922533.htm

Guobin Yang, “The Co-Evolution of the Internet and Civil Society in China,” *Asian Survey* 43:3 (May-June 2003): 405-422.

Guobin Yang. The Power of the Internet in China: Citizen Activism Online, New York: Columbia Universiry Press, 2009.

Yu Yang. "Diaocha jieguo cheng woguo qingshaonian wangyin renshu po 2000 wan [Investigation Finds Number of Chinese Youths Addicted to the Internet Exceeds 20 Million]," *The People's Daily* 8 March 2010, Accessed online 9 March 2010, http://game.people.com.cn/GB/48644/48662/11091513.html.

Haiqing Yu, "Blogging Everyday Life in Chinese Internet Culture," *Asian Studies Review*, 31 (2007): 423-433.

Xiang Zhou. "The Political Blogosphere in China: A Content Analysis of the Blogs Regarding the Dismissal of Shanghai Leader Chen Liangyu," *New Media and Society* 11.6 (2009): 1003-1022.

Jonathan Zittrain and Benjamin G. Edelman, "Internet Filtering in China," *IEEE Internet Computing*, 7.2 (2003): 70-77.