# THE BUSINESS OF CENSORSHIP: CONTENT MANAGEMENT AND THE CHINESE ECONOMY

by

JOSHUA CLARK

B.A. (Hons.), Queen's University at Kingston, 2009

MASTER OF ARTS

in

THE FACULTY OF GRADUATE STUDIES

(Political Science)

THE UNIVERSITY OF BRITISH COLUMBIA

(Vancouver)

August 2010

## Abstract

Content control and censorship on the Internet are increasingly important topics for scholars of democratization, media and communications. Most studies have examined the relationship between the Internet, content management and various elements important to democratization such as the formation of civil society organizations. This thesis attempts to expand this discussion by examining the effects of online content management on economic systems, using the People's Republic of China as an example. China features a globally integrated economy that is increasing dependent on manufacturing and services while simultaneously maintaining one of the most extensive online content management systems in the world. This paper attempts to show how the Communist Party of China is able to reconcile the need for connectivity in order to drive their economy while maintaining political control. It also discusses the long-term implications of this strategy. The first section consists of a series of quantitative and qualitative tests to determine how various classes of websites are managed. These tests reveal that in order to maintain the flow of information necessary for a globally integrated economy, the Chinese Communist Party utilizes strategies that manage but not block the information flows related to business.  This survey is followed by a case study examining the relationship between Google and China, and the implications of Chinese regulation and control for the broader economy. The results indicate that the Chinese regulatory strategy, which is designed to meet political goals, is creating a divergent technology industry that caters to the party's needs. This development may have serious implications for the future of the Chinese globalization effort as it poses a threat to interoperability and exchange between Chinese online presences and those in the rest of the world.

# Table of Contents

## List of Tables

## Acknowledgements

Any piece of research involves the contributions, time and effort of countless individuals and acknowledging them all is a formidable task. However I would like to take a moment to extend thanks to a few notable people and groups who provided a noteworthy contribution to the production of this document. First and foremost we have Dr. Yves Tiberghien, my supervisor who helped take this research from a scattered collection of half stated ideas and form it into a cohesive piece of work through his support and guidance. I would also like to thank Dr. Maxwell Cameron for reading and reviewing the earliest proposals which formed the base of this work and agreeing to lend his insight as a second reader. Speaking more expansively I would also like to thank my colleagues and professors at the University of British Columbia for providing such a hospitable yet challenging environment for learning and growth. I would also like to thank Green College and the community there for providing a wonderful intellectual and interpersonal community.

On a more personal note, as always I would like to thank my parents and my brother for their support, input and love throughout the writing process.

## Dedication

*To my parents.*

# Chapter One: Introduction and context

## Jingjing and ChaCha

Tecent QQ is one of the most popular online communities in China. It offers a host of services, from instant messaging and virtual pets to business information and networking. At the same time, users can utilize the QQ messaging service to send questions to Jingjing and Chacha, two cartoon police officers. The characters are available over the messaging client, serve as a constant reminder of state surveillance and can answer various questions about Chinese Internet policy.[1] Drawn in a Japanese anime style with wide eyes and big smiles, their presence also informs users that the state reserves the right to monitor and control their use of the Internet and hints at penalties for disobedience. Meanwhile, in other sections of the QQ community, users exchange business information, practice English or simply waste time with entertaining games. This image sums up the contradiction of the Chinese Communist Party's (CCP) policy regarding the Internet. The party is attempting to juggle the clear economic and social benefits of a networked world while keeping control of the potentially dangerous political side effects of this global network.

China is by no means the only country attempting to censor and control the Internet, nor is it the most extreme in its filtering. The Opennet Initiative, a multi-university body dedicated to examining censorship, lists 26 countries as confirmed or suspected of filtering the Internet,

[1] Xiao Qiang, "China News: Image of Internet police: JingJing and Chacha online," *China Digital Times*, January 22, 2006, http://chinadigitaltimes.net/2006/01/image-of-internet-police-jingjing-and-chacha-online-hong-yan-o%C2%BAae%C2%A5%E2%84%A2aaio%C2%BAa/. Also see JingJing's site: http://66110.qzone.qq.com/ and ChaCha's site: http://777110.qzone.qq.com/

including China.[2] A closer examination of this data reveals an intriguing puzzle: China belongs to a select group of states engaged in "pervasive" filtering and censorship of the Internet.[3] This means that censorship is both "deep" (blocking a high promotion of potentially dangerous websites) and "broad" (the definition of dangerous website catches a large number of sites).[4] Other pervasive filterers with systems deeper or broader than China include Iran and Saudi Arabia. China is radically different from these other filtering countries for several reasons. It is by far the largest country in terms of population and economic size. Additionally, Saudi Arabia and Iran are oil rich states with economies based around the rents gained from resource extraction and processing. In contrast, China is a diverse manufacturing and export oriented market with developing telecommunications and technology industries.

This combination of an increasingly diversified and globalized production economy with strict information controls is puzzling for several reasons. First, unlike resource extraction and processing, these industries are highly dependent on information flows and transnational data exchange.[5] Therefore, while Iran can afford to limit domestic Internet speeds to a stifling 128 kilobytes per second (kb/s) in order to limit political opposition, if similar actions were taken in China, the result would immediately cripple numerous sectors of the economy.[6] This damage would stem from the fact businesses within China, both foreign and domestic, are becoming

[2] Ronald J. Deibert et al., eds., "Measuring Global Filtering," in *Access Denied: The Practice and Policy of Global Internet Filtering*, 1st ed. (The MIT Press, 2008), 6.

[3] Ibid., 8-9.

[4] ibid

[5] Amir Hartman and John Kador, *Net Ready: Strategies for Success in the E-conomy* (McGraw-Hill Professional, 2000), http://portal.acm.org/citation.cfm?id=555667.

[6] The Citizen's Lab, "Country Profile: Iran," May 9, 2007, http://opennet.net/research/profiles/iran.In comparison the average Canadian Internet speed ranges from 512kb/s to 10mb/s. Compare to broadband speeds in China China Internet Network Information Center, "The 25th Statistical Survey Report on the Internet Development in China," March 15, 2010, http://www.cnnic.net.cn/uploadfiles/pdf/2010/3/15/142705.pdf.

increasingly integrated into the world economy, especially following China's accession to the WTO.[7] This integration is highly dependent on the global flow of information, which allows actors within the market to make informed choices and adapt to new circumstances. Information control and censorship is an attempt to clamp down on very same information channels that feed the market and this presents an intriguing conundrum. How does the CCP balance its unique economic and political interests with censorship and online content management? Additionally, does the adoption of content management and intervention strategies form part of a broader, distinctive approach to globalization? Does intervention within the Internet alter the overall trajectory of the Chinese globalization project or alter what the final product might look like?

This paper answers these questions by adopting a Varieties of Capitalism style framework and re-conceptualizing the Internet as part of the broader network of institutions that facilitate cooperation between firms. First, the outline of Chinese content management strategies is revealed using quantitative testing of reactive censorship and qualitative case studies focusing on proactive techniques. This analysis reveals that the CCP depends on a strategy of management and regulation, not obstruction, to handle sections of the Internet related to business and the economy. Then the Internet is recast as a key part of inter-firm relations. The reinterpretation portrays websites and other forms of online activity as a means to facilitate deliberation, the exchange of information and other key functions that allow firms to overcome the collective action problems inherent in business. While the majority of the globe has been moving towards a mutually compatible Internet, China is diverging as the CCP seeks to project its power into the online world in order to meet political goals and quash potential opposition. This attempt to

[7] Nina Hachigian, "China's Cyber-Strategy," *Foreign Affairs* 80, no. 2 (April 2001): 118-133.

balance political and economic goals means that blocking and the obstruction of information through reactive means is ineffective because it damages the abilities of firms operating within China to coordinate through the Internet. As a result, the CCP has adopted a variety of distinct "proactive" management strategies that allow it reconcile its economic and political goals, although this process has serious repercussions for the shape and development of the Chinese economy.

## "The Internet is a series of tubes" – Key terms and definitions

Before beginning the examination, it is important to define some key terms that will appear within this discussion, and while seemingly obvious, defining the Internet as a construct is a helpful exercise. Former American Senator Ted Stevens famously defined the Internet as "a series of tubes… not a big truck," but for the purposes of this discussion, a more sophisticated definition is needed.[8] Therefore, the Internet will be defined as the global "network of networks," a transnational system designed to provide a protocol for data exchange between various electronic devices.[9] The Internet can be examined as either a broad collection of mechanisms for data transfer or a narrower network, which consumers normally associate with the idea of the "Internet." A broad definition would include cellular wireless connectivity such as 3G and EDGE, as well as unconventional mechanism of data transfer such as file sharing or online games.[10] A narrow definition focuses on the interactions conducted through a browser that

[8] Ken Belson, "Senator's Slip of the Tongue Keeps on Truckin' Over the Web," *The New York Times*, July 17, 2006, sec. Business / Media & Advertising, http://www.nytimes.com/2006/07/17/business/media/17stevens.html?_r=1.
[9] National Science Foundation, "The Internet: Changing the Way We Communicate," n.d., http://www.nsf.gov/about/history/nsf0050/internet/internet.htm.
[10] For examples of this broader perspective see: Ubonrat Siriyuvasak, "People's media and communication rights in Indonesia and the Philippines," *Inter-Asia Cultural Studies* 6, no. 2 (2005): 245. & Dmitri Williams et al., "From

involve the retrieval and display of text, images and multimedia. The majority of the literature surrounding censorship and the Internet in China focus on the Internet described by this narrower definition.[11] Therefore, the Internet will be defined using this narrower definition and this paper will focus on digital interactions mediated by browsers such as email, content retrieval and organization.

The second major term that appears frequently in this examination is content management. Otherwise known as Internet censorship or filtering, it can be defined as the intervention of states into the Internet with the explicit goal of blocking or impeding access to political sensitive information or opportunity spaces.[12] There are two routes towards this goal. Reactive censorship attempts to impose blockages between users and the banned content.[13] This is achieved by obstructing connections trying to access blocked materials, removing search results, legal sanction or self-censorship. Proactive strategies are more subtle. They involve the state utilizing the Internet to remove the impetus to seek out troublesome information. States seeking to engage in proactive censorship have a number of tools open to them. They can attempt to create a "domestic Intranet" which provides for the needs of their users while isolating sensitive materials.[14] This process can be supplemented with an e-governance strategy that makes the state more responsive to citizens, increasing domestic satisfaction and reducing the likelihood that

Tree House to Barracks: The Social Life of Guilds in World of Warcraft," *Games and Culture* 1, no. 4 (October 1, 2006): 338-361.

[11] For an example see Shanthi Kalathil, *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule* (Washington, D.C: Carnegie Endowment for International Peace, 2003).

[12] OpenNet Initiative, "About Filtering," n.d., http://opennet.net/about-filtering.

[13] Shanthi Kalathil and Taylor C Boas, "Internet and State Control in Authoritarian Regimes: China, Cuba, and the Counterrevolution," *Carnegie Papers* 1, no. 21, Carnegie Endowment for International Peace (July 21, 2001), http://www.carnegieendowment.org/publications/index.cfm?fa=view&id=728.

[14] ibid

users will engage in subversive actions when online.[15] Proactive strategies are more difficult to detect than reactive censorship because it does not actively impede connections; instead, it alters the incentive structures governing user's actions online.

It is also useful to cover the use of the term Chinese Communist Party or CCP within this examination. For the sake of simplicity, the term CCP will be used to refer to the governing party/state apparatus within China including both the governmental organization and the parallel party structure, which populates and controls it. The CCP is an incredibly diverse organization that extends across a massive and densely populated country with major variations between regions. This means that the CCP itself is also highly diversified. Officials and cadres in one region may adopt completely different policies from those of their counterparts in a different area of the country. Therefore, speaking of a monolithic “CCP” is in itself a distortion of reality. Even within the realm of Internet policy, there are numerous ministries and organizations within the party jockeying for control and enacting policy. Despite this disparity, the party has made a concerted effort to rationalize control of the Internet into one ministry at the national level, the Ministry of Industry & Information Technology (MIIT).[16] The MIIT controls the infrastructure and censorship regime within China, licensing, telecom regulation and development. This consolidation makes it possible to speak of a “Chinese Internet policy” as a coordinated entity, although it is important to recognize that implementation may vary from province to province and region to region. This paper will be concerned primarily with national level regulations and

[15] ibid
[16] OpenNet Initiative, “Country Profile- China,” June 15, 2009, http://opennet.net/research/profiles/china.

policies, so while the enforcement of specific standards may vary from locale to locale, the policies critical for this paper are relatively centralized within the MIIT.[17]

Finally, the term “business related website” refers to websites that offer information and services essential for the day-to-day conduct of economic transactions. Examples of business websites include business-to-business (B2B) transaction services, banks, stock indexes, business news and information providers and professional networking sites.

## The Internet as a tool of democratization

A constant theme throughout the debate surrounding the role of the Internet and its relationship to life in states that manage online content is the democratizing potential of online communication. While this paper will focus on the economic repercussions of content management, it is still important to summarize the democratization literature as it helps reveal the potential dangers and possibilities that the Internet poses to the CCP.

There are three broad schools of thought within the academic literature commenting on the ability of states to manage the Internet and the ability of online interaction to promote democracy. All three have their proponents and detractors and evidence can be found to support each perspective. It is important to summarize and understand these various theories as this examination will contribute to the ongoing debate.

The first and oldest perspective on the relationship between the Internet and the state can best be described as the distributed network perspective. This optimistic view argues that the Internet represents a distributed network beyond the control of any one state. Unlike television, radio or

[17] ibid

print media there is no single content source that can be controlled or co-opted.[18] Television stations can be taken over, radio transmitters broken and printing presses restricted. However, the Internet does not rest in any one country or area. Servers exist all over the world and the loss of one does not significantly damage the network. Information can be lost online, but not forgotten through preservation in online caches and archives.[19] This distributed nature of the Internet means that there are multiple sources of content and access points for savvy users which are scattered all over the world and not dependent on the largess of any one government or actor. Governments on the other hand are restricted by the shackles of geography and are unable to police content and access providers located outside their borders without serious cost.[20] Therefore, the Internet is generally resistant to state control. Crackdowns on content providers are futile when the same information can be found on websites located outside the reach of the state, and restrictions on access can be bypassed due to the distributed and flexible nature of the Internet.[21] As a result, the state is incapable of effectively enforcing its will within the online world.[22]

Standing in stark contrast with the distributed network perspective is the state capacity theory on the relationship between governments and the Internet. According to this school of thought, the Internet does not pose a challenge to non-democratic states because it facilitates the growth of state capacity and control over its population. This increase in capacity takes two forms, greater

[18] David Trend, *Reading digital culture* (Wiley-Blackwell, 2001), 262.
[19] For an example see: "Internet Archive: Free Movies, Music, Books & Wayback Machine," n.d., http://www.archive.org/.
[20] John Perry Barlow, "A Declaration of the Independence of Cyberspace.," *Humanist* 56, no. 3 (May 1996): 18-19.
[21] Jason Lacharite, "Electronic Decentralization in China: A Critical Analysis of Internet Filtering Policies in the People's Republic of China," *Australian Journal of Political Science* 37, no. 2 (2002): 344.
[22] ibid

surveillance powers and an increase in government responsiveness.[23] Both of these factors lower the likelihood of opposition to a non-democratic regime. The growth in surveillance comes from the increased opportunities offered by data mining and other forms of intelligence gathering created by the Internet. Users leave trails online that can be followed and monitored, allowing any potentially dangerous actions to be observed and countermanded.[24] Additionally, states can make use of the Internet to increase the quality of their own services, utilizing e-government techniques to create a more nimble and responsive government. According to state capacity theorists, these changes are likely because any given state has significantly more resources and motivation to utilize the Internet than the average user.[25] This advantage in funding, mobilization and willpower manifests itself as a strong control and co-optation of the Internet to serve the needs and goals of the state, making the Internet a tool of non-democratic regimes, not their downfall.

Finally, the user-based perspective adopts the view that users are the critical factor in determining the role of the Internet in non-democratic states. Accepting elements of both previous schools of thought, a user-based perspective argues that the critical element in determining the efficacy of state control over the Internet is the motivation of users. Users have several advantages over the state. They are smaller presences online and can move quickly to exploit any holes in content management, allowing for access to information that would normally be controlled by the state. These alternative forms of access are effective, but time consuming,

[23] Shanthi Kalathil and Taylor C Boas, "The Internet and state control in authoritarian regimes," text, August 6, 2001, http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/876/785.

[24] For an example see Jillian York, "ONI Affiliate Reveals Chinese Surveillance of Skype Messages," *OpenNet Initiative*, October 2, 2008, http://opennet.net/blog/2008/10/oni-affiliate-reveals-chinese-surveillance-skype-messages. Demonstrating how the introduction of Skype to China increased surveillance power.

[25] Kalathil and Boas, "The Internet and state control in authoritarian regimes."

requiring users to shield their connections or take roundabout routes to access content. However, the state has a number of distinct advantages as well. It can create barriers to access, which while are not completely successful, do create a strong disincentive for users to move beyond them.[26] Therefore, the ability of the state to control the Internet is a product of the motivation of users to seek out information and bypass controls set against the strength of the state's content management.[27] Motivation can be reduced by giving people little cause to be politically unhappy and increased through global events or specific actions undertaken by the state. As dissatisfaction increases, users become more willing to bypass state controls and seek out alternative forms of information.[28] Content management tools are not tools to restrict access but mechanisms to manage the user's motivation and willingness to strike out and gather information independently. Blocking websites and other coercive mechanisms discourage independent actions while e-governance initiatives and other more proactive strategies reduce the need for users to strike out on their own. Motivation is obviously a highly personal factor and some users will always seek to test and challenge the boundaries created by the state. However, if these users represent a small minority, their ability to organize and mount serious opposition will be limited.[29] In times of crisis, content management becomes so repressive that users are not able to fulfill their essential needs when online, which forces them to go beyond sanctioned areas. As well, management tools breakdown and this removes the costs associated with going beyond

[26] Gurdun Wacker, "The Internet and Censorship in China," in *China and the Internet : politics of the digital leap forward*, ed. Christopher R. Hughes and Gurdun Wacker (London ; New York: RoutledgeCurzon, 2003), 72.

[27] Ibid.

[28] Rebecca MacKinnon, "Flatter world and thicker walls? Blogs, censorship and civic discourse in China," *Public Choice* 134, no. 1 (January 1, 2008): 43.

[29] Jack L. Goldsmith and Tim Wu, *Who controls the Internet?: illusions of a borderless world* (Oxford University Press US, 2006), 103.

sanctioned areas. Either of these trends will cause more users to venture into previously off-limits territory, creating the population needed to mount political opposition.

## The economics of connectivity

While the debate surrounding the ability of the Internet to promote democratization is important, the economic repercussions of content management are woefully under examined. A major factor in this neglect appears to be the lack of a framework for conceptualizing the role that the Internet plays within the economy. The form that this framework assumes depends on a number of assumptions with the most important being the power of a state to influence its economy. If the state is seen as having little power then government-sponsored content management programs should not have a significant impact on firms and economic activity. Alternatively, if the state is portrayed as highly influential in affecting the economic system it presides over then the influence of content management programs will also be expanded. Therefore, in order to construct a framework that integrates the Internet with the development of an economy, key assumptions about the relationship between states and the global economy need to be made. It is prudent to summarize the literature on this field and then select a system from these debates that best reflects the relationship between the Internet and the CCP.

Some commentators generally view the state as relatively inconsequential in determining the shape of the domestic economy. The most prominent body of literature in this camp is convergence theory. Convergence theory argues that the pressures created by globalization influence the form of a domestic economy.[30] The need to stay competitive and promote growth in the increasing interconnected world economy drives decisions at all levels about policy. These demands are found all over the world, creating a push towards a standardized form of economic activity.[31] The exact mechanism that convergence theorists point towards to explain their hypothesis varies from author to author. Some argue that there is a global "race to the bottom" as the need to be competitive forces free trade and neo-liberal policies.[32] Others claim that pressure from various groups, such as powerful trading blocs and massive firms, lies behind convergence, and the list can go on. Regardless, each perspective shares the opinion that globalization is generating change in economic systems and this change can be best described as convergence.

There are many scholars who disagree with the convergence hypothesis and argue that variation and diversity exists and maybe increasing among states. The mechanisms that generate this variation have not been firmly established. Some authors point towards domestic interest groups as the critical factor. Globalization produces a number of externalities that may have positive or negative effects given the actors involved and the surrounding situation.[33] Previously competitive industries may suffer when faced with global competition while new players benefit from the increased scope and scale of business.[34] As a result, various social groups spring up in an attempt to alter or halt the process of globalization to suit their needs. As an example, workers may want greater protection for their jobs while industrialists clamor for less government intervention and

[30] Thomas L. Friedman, *The Lexus and the olive tree* (Random House of Canada, 2000), 101.

[31] ibid

[32] For a review see Daniel W. Drezner, "Globalization and Policy Convergence," *International Studies Review* 3, no. 1 (Spring 2001): 53-78.

[33] Jeffry A. Frieden and Ronald Rogowski, "The Impact of International Economy," in *Internationalization and domestic politics*, ed. Robert Owen Keohane and Helen V. Milner (Cambridge University Press, 1996), 46.

[34] Peter Alexis Gourevitch and James Shinn, *Political power and corporate control: the new global politics of corporate governance* (Princeton University Press, 2007), 10.

greater exposure to the global marketplace. Consequently, a number of social groups form, each pursuing their unique agenda. Labour unions may push for protection for chosen industries and other concessions that keep jobs within the domestic economy. Other powerful groups such as financiers or industrialists may in turn lobby for greater integration with the global market. The relative strength or weakness of these groups can be seen as a key factor in generating diversity within the global economy.[35] There are thousands of permutations on this theme of course focusing on political parties or other social groups, but they share a focus on actors within a society as the mechanisms for variation.

An alternative explanation argues that the formation of the state itself is the critical factor in creating diversity within the world economy. Different combinations of institutions, financial systems and governmental ideologies create varying degrees of willingness to intervene and shape domestic markets (the exact mechanism varies from author to author).[36] When examining these capacities, states are often labeled as strong or weak, with weaker states allowing market mechanisms to govern their economies. Stronger states may intervene more readily by fostering domestic markets, creating demand or protecting vulnerable industries from global pressure. Regardless, this state-centric perspective puts an emphasis on policy and government intervention within the economy as a key generator of international economic diversity.[37]

Another perspective on the variations within the global economy puts firms at the center of the examination. Operating under the label "Varieties of Capitalism" (VOC), this body of work

[35] Frieden and Rogowski, "The Impact of International Economy," 45.

[36] See John Zysman, *Governments, markets, and growth : financial systems and the politics of industrial change* (Ithaca N.Y.: Cornell University Press, 1983), 16. For an example

[37] Theda Skocpol and Edwin Amenta, "Did Capitalists Shape Social Security?," *American Sociological Review* 50, no. 4 (August 1985): 572-575.

argues that firms are the key actors in explaining economic activity. Firms in any economy face a number of challenges that obstruct their ability to do business. These difficulties include but are not limited to issues with employees, education and training, industrial relations, corporate governance and inter-firm relations.[38] The relationships and organizations generated by firms to overcome these issues affect the form and function of the economy in which they are situated. This leads to the separation of markets in liberal market economies (LMEs) and coordinated market economies (CMEs).[39] The former uses market-based relationships between firms to overcome the aforementioned issues while the later relies more on interaction with non-market mechanisms. The variation between these outcomes originates from the institutional backdrop, which either facilitates or hinders the spontaneous formation of relationships between firms.[40] This institutional environment includes but is not limited to trade unions, legal and regulatory systems and financial markets.[41] These actors either allow for or hinder the exchange of information, sanctioning of defectors and the monitoring of firm's behavior. This institutional surrounding is not fully controlled by firms, so they are forced to engage and work with it as opposed to bending it to suit their needs.

When comparing the various models regarding the role of the state in globalization to existing studies of content management within China, it becomes clear that the assumptions supporting the VOC literature best fit the situation. Chinese Internet policy is clear diverging from other states due to its depth and pervasiveness, making theories of convergence a poor fit.[42] Similarly,

[38] Peter A. Hall and David W. Soskice, *Varieties of capitalism: the institutional foundations of comparative advantage* (Oxford University Press, 2001), 6-7.
[39] Ibid., 8.
[40] Ibid., 14.
[41] Ibid., 10.
[42] OpenNet Initiative, “About Filtering.”

theories that argue that social groups determine the direction of policy do not seem to fit the Chinese situation. While a large section of the population supports content management for reasons of “stability”, large and important actors particularly within the critical field of business have expressed their opposition.[43] However, this does not mean that the CCP is in complete control of its Internet policy. Firms have been circumventing and bypassing restrictions by simply ignoring them or leveraging the power of international trade and regulatory bodies to press their case, as described in the section on encryption.[44] While these violations have not crippled the CPP’s ability to project power online they do demonstrate that the state is not completely dominant. This means that the VOC perspective appears to provide the most accurate theoretical toolkit as it encompasses the relational nature of the Internet for addressing the role of the Internet in China and its relation to economics.

## Conceptualizing the Internet’s role in the economy

Fitting the Internet and role of content management into the Varieties of Capitalism framework requires a re-conceptualization of the role of the Internet within the economy. As mentioned earlier, the VOC perspective argues that variation in economic systems comes from alterations in strategic actions of firms. These are generated in part by the institutions and firms operating within these systems. Institutions alter the strategic actions of firms and their ability to coordinate mutually beneficial actions with a wide variety of actors.  These institutions work to provide information, sanction defectors, monitor behavior and generate deliberation.[45] Various

[43] See lobbying against the Green Dam software: “US PC makers in 'stolen code' row,” *BBC*, June 15, 2009, sec. Technology, http://news.bbc.co.uk/2/hi/8101978.stm.
[44] Indrajit Basu, “China Forges Ahead With Homegrown WAPI Standard Instead of Wi-Fi,” *Government Technology*, September 27, 2006, http://www.govtech.com/gt/articles/101267.
[45] Hall and Soskice, *Varieties of capitalism*, 10.

combinations of institutions are mutually reinforcing leading to patterns of organization such as the liberal market economy.[46] The Internet fits into the picture as part of the institutional background that affects the strategic actions of firms. This statement is justified because the Internet fulfills all of the roles of an institution put forward by Hall and Soskice. It provides vast quantities of information for actors within any given system, allowing firms to obtain stock quotes, the latest news and other important facts.[47] Additionally, the Internet can be used to sanction defection by allowing for information about offending actions to be circulated globally and reach a wide audience.[48] The ability to distribute and consume information from a wide variety of sources also aids in deliberation and monitoring. A brief example illustrates these actions in practice; business-to-business websites (B2B) facilitate coordination between suppliers, producers and resellers in various industries.[49] These websites present a previous unheard of quantity of information to their clients. B2B websites also allow for reviews and feedback to be posted publicly, allowing defectors to be publicly identified and labeled. In addition, negotiations and status updates can be facilitated though these services allowing for monitoring and deliberation of the interaction.

By accepting the Internet as one of the institutions that affects the strategic choices of firms within a given economy, content management strategies take on new meaning. Aside from their obvious political significance, these techniques alter the information available online and therefore distort the structure that firms operate within and alter the functioning of the economy.

[46] Ibid., 18-20.
[47] For an example see http://www.tmx.com/
[48] For an example see the response to Yahoo's turnover of dissidents to the CCP which was viewed as a defection from privacy standards “Yahoo 'helped jail China writer',” *BBC*, September 7, 2005, sec. Asia-Pacific, http://news.bbc.co.uk/2/hi/4221538.stm.
[49] For an example see www.alibaba.com

In order to understand how content management affects the Chinese economy, a detailed picture of how the CCP interacts with the Internet needs to be developed.

### A brief history of content management and growth in China

Having shown how the Internet can play a role in economic development it is now time to define the form that content management and censorship takes within China. The first question facing anyone who is attempting to examine the relationship between the CCP and the Internet is; why does the party feel the need to control and manage the Internet? The CCP's desire for information control online arises from the dual nature of the Internet. Online venues provide both global information and opportunity spaces. Isolated, these two aspects do not pose an intrinsic threat to the CCP. Free information flows may highlight problems with the Communist Party and promote dissatisfaction, but if citizens cannot organize to express these complaints then the issue remains unthreatening. Similarly, opportunity spaces that allow citizens to mobilize do not pose a threat unless dissatisfaction drives citizens to make use of them. The Internet combines both of these threats into a single entity.[50] On an unrestricted connection, the average Internet user can easily access content from all around the world and utilize social networks, forums or instant messaging services to organize and act on concerns creates by this information. A perfect example of this double-sided threat is the 2009 Iranian election protest. Information about possible electoral fraud spread online and activists utilized Twitter, a social networking service,

[50] For an impassioned, if slightly old expression of these ideas see. Barlow, "A Declaration of the Independence of Cyberspace.."

to organize and carry out demonstrations.[51] Censorship and information control by the CCP therefore represents an attempt to mitigate these threats.

Along with these threats, the Internet also provides incentives that promote its adoption. Connectivity has become entrenched as a part of everyday social and economic life in developed economies with which China is attempting to trade and compete. Therefore, in order to operate with the same speed and agility as other states, widespread Internet adoption is necessary.[52] Additionally, the Internet offers the party the ability to monitor and distribute information online and increase its legitimacy in the eyes of the domestic public.[53] However, these incentives do not negate the aforementioned threats posed by the Internet, necessitating some form of content management.

This management can take many forms. According to the Opennet Initiative, China engages in "pervasive filtering" of political and conflict related information and "substantial filtering" of Internet tools and social information.[54] Filtering tends to be consistent, with blocked sites remaining inaccessible for long periods.[55] Additionally, the Chinese censorship regime is highly secretive, with information about methods and selection techniques closely guarded. Responsibility for censorship is divided between fourteen distinct ministries with each covering different aspects of the Internet. This ranges from the Ministry of Industry & Information Technology, the Ministry of Information and even the People's Liberation Army depending on

[51] Ari Berman, "Iran's Twitter Revolution," *The Nation*, June 15, 2009, http://www.thenation.com/blogs/notion/443634.
[52] Sean Xu, Kevin Zhu, and Jennifer Gibbs, "Global Technology, Local Adoption: A Cross-Country Investigation of Internet Adoption by Companies in the United States and China," *Electronic Markets* 14, no. 1 (2004): 13.
[53] Michael Chase and James C. Mulvenon, *You've got dissent!* (Rand Corporation, 2002), 87.
[54] Deibert et al., "Measuring Global Filtering." 16.
[55] OpenNet Initiative, "Country Profile- China."

the context and type of information being exchanged. Recently, this chaotic combination of regulatory bodies was streamlined with most control now resting with officials in the new MIIT wing.[56] Controls also vary based on geography, with heavy restrictions in potentially unstable regions such as Xinjiang and Tibet. Reporters covering the Uyghur riots in July of 2009 found that their connections were limited to a mere handful of sites during the riot, most of which were controlled by the party, displaying the wide variations in censorship styles and techniques within China.[57]

Censorship also extends through all levels of the Chinese Internet infrastructure, from the major international fiber optic backbones that provide the raw connectivity for the population to individual machines. At the infrastructure level, the CCP is well positioned because it owns or controls the major access points to China's Internet backbone.[58] These points allow for inspection and interdiction of potentially destabilizing material through a series of programs collectively known as the "Great Firewall of China." These programs can block sites and shape information flowing into the Chinese domestic market.[59] The party licenses access to this infrastructure to individual Internet Service Providers (ISPs) who repackage and sell the bandwidth to consumers. In order to be licensed by the state, ISPs have to commit to monitoring and shaping traffic on their networks, adding an additional layer of control.[60] Firms and websites making use of the Chinese Internet can also face restrictions, such as search providers filtering specific keywords and blocking sites or turning over information on suspected dissidents to the

[56] Ibid.
[57] "Xinjiang: an 'internet prison'," *BBC*, February 3, 2010, sec. Asia-Pacific, http://news.bbc.co.uk/2/hi/8492224.stm.
[58] Eric Harwit and Duncan Clark, "Shaping the Internet in China. Evolution of Political Control over Network Infrastructure and Content," *Asian Survey* 41, no. 3 (6, 2001): 389.
[59] OpenNet Initiative, "Country Profile- China."
[60] ibid

party.[61] At the level of the individual and their computer, the CCP has begun to introduce the "Green Dam Project" a censorship program installed on new computers that actively filters specific keywords on individual machines.[62] The CCP also makes use of self-censorship techniques such as the aforementioned Jingjing and Chacha, which produce a chilling effect among users and discourage exploration online.[63] When taken together, the Chinese censorship regime represents a frightening combination of controls, negative incentives and punishments that attempt to minimize opposition to the party.

However, while the CCP manages content online it is also a major promoter of digital connectivity. The party has been working vigorously to improve connectivity by expanding infrastructure and cracking down of price gouging by independent Internet service providers. Briefly, the history of the Internet in China begins primarily with academic usage in the 1980s with the first email exchanges sent between Chinese universities and their German counterparts.[64] This advancement was followed shortly afterward by the creation of a formal email protocol between Tsinghua University and the University of British Columbia.[65] Development accelerated with the creation of the "Golden Projects" including the "Golden Bridge" which provided funding for the creation of a national Internet backbone and the "Golden Shield," charged with the development of a censorship regime.[66]  Other golden projects were

[61] Rebecca MacKinnon, *CHINA - "Race to the Bottom" Corporate Complicity in Chinese Internet Censorship* (Human Rights Watch, 2006), 5.
[62] "China defends screening software," *BBC*, June 9, 2009, sec. Asia-Pacific, http://news.bbc.co.uk/2/hi/asia-pacific/8091044.stm.
[63] Qiang, "China News: Image of Internet police: JingJing and Chacha online."
[64] Zixue. Tai, *The Internet in China : cyberspace and civil society* (New York: Routledge,, 2006), 122.
[65] Ibid.
[66] Harwit and Clark, "Shaping the Internet in China. Evolution of Political Control over Network Infrastructure and Content."

directed towards digitizing the bureaucracy and providing e-government services.[67] The state has made promoting connectivity a major part of its long-term plan for the People's Republic of China (PRC) and as a result broadband use, Internet and adoption and website registration within China has been growing at an impressive rate since 2000.[68]

[67] Lianjie Ma, Jongpil Chung, and Stuart Thorson, "E-government in China: Bringing economic development through administrative reform," *Government Information Quarterly* 22, no. 1 (2005): 21.

[68] China Internet Network Information Center, "The 25th Statistical Survey Report on the Internet Development in China."

## Chapter Two: Testing Chinese content management

### Scaling the great firewall – Reactive blocking mechanisms

While informative, the literature surrounding content management in China that has been explored thus far does not help determine the economic implications of content management. In order to reveal how the CCP's desire to maintain control of the online world affects firms within China, a new examination is needed that focuses on the elements of Internet communication that are significant to business.

As discussed in the previous section, there are two possible forms of control the CCP can adopt to manage content on the Internet. Reactive strategies attempt to keep users away from information by obstructing access through the erection of barriers around specific sites or networks. Proactive strategies manage and distract users without completely blocking content. These two strategies are not mutually exclusive and can be used together to great effect in a “carrot and stick” type system.

Firms and the online services they use present a specific challenge because information is needed to solve the collective actions and problems that are inherent to business. Blocking access deprives them of critical resources. This means that websites related to businesses or those providing services to business will less likely be blocked than other forms of content. However, the only way to know for sure is to test this hypothesis.

Reactive censorship can be examined through penetration testing – rerouting an Internet connection from an uncensored country through a Chinese server and then comparing accessibility between the two connections. If a site is blocked from within China but accessible from other locales, it is highly likely that the CCP has chosen to restrict access to this information.

Various tools exist for automating penetration testing, but the CCP appears to have adapted their censorship protocol to restrict access from an Internet Protocol (IP) address for several minutes after a connection attempts to access blocked material, breaking automated testers.[69] Because of this adaptation, the penetration testing was done using a new method utilizing repurposed search engine optimization (SEO) tools.

First, a list of websites was compiled based on important political and economic topics such as human rights, democracy, investment and business information as well as a sampling of top sites from any category (n=1537).[70] The location and page rank (a measure of connectivity with other sites) was also gathered and factored into the examination. Half of the sites surveyed were based on search terms in Mandarin and the other half in other languages, usually English. Each site was then tested and the results interpreted through a Logistic regression. The dependent variable was whether or not the site in questions was blocked within two out of the three staggered tests conducted over the course of a week. The results are expressed as shifts from a baseline established by testing a group of randomly selected websites which function as a control group. The control group consisted of websites selected randomly from a list of the top one million websites in the world and included sites addressing a number of distinct topics ranging from social networking to pornography.

[69] Govcom, "Censorship Explorer," Digital Methods Tool, March 15, 2010, http://tools.issuecrawler.net/beta/proxies/.
[70] For details see Appendix

**Table One – Results of logistic regression**[71]

| Equation | Variables | (1)<br>Verdict |
|---|---|---|
| verdict | Page Rank | -0.00432 |
| | | (0.0388) |
| | Hosted in China | -2.438*** |
| | | (0.392) |
| | Chinese Language | 0.489*** |
| | | (0.188) |
| | Democracy | 1.777*** |
| | | (0.462) |
| | Falun Gong | 3.236*** |
| | | (0.462) |
| | Tianamen Square | 2.841*** |
| | | (0.459) |
| | Uyghur[72] | 0.103 |
| | | (0.513) |
| | Invest in China | -1.905** |
| | | (0.834) |
| | Joint Venture in China | -1.227* |
| | | (0.726) |
| | Business in China | -2.460** |
| | | (1.093) |
| | Import from China | -0.653 |
| | | (0.601) |
| | Constant | -2.576*** |
| | | (0.490) |
| | Observations | 1,537 |

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

[71] Calculated using StataCorp., "Stata Statistical Software: Release 11," 2009, http://www.stata.com/support/faqs/res/cite.html.

[72] The low values within the Uyghur category in part reflect the fact that a number of official CCP websites appeared in the search results. Since the CCP does not block its own sites this served to significantly lower the number of sites blocked related to the Uyghur population. Additionally the search gathered a number of articles related to the Uyghur detainees at Guantanamo, future revisions of this paper will aim to tighten these search criteria.

Categories of sites that exhibited a statistically significant relationship with blocking are shown above. Most sites gathered from political search terms showed a strong relationship with being reactively censored by the CCP. Meanwhile, business related websites were significantly less likely to be blocked than either their political counterparts or sites gathered through a random selection of popular domains. Domestic websites tended to be relatively free of direct restriction but sites written in Mandarin are more likely to be blocked than there English non-Mandarin counterparts. Business websites located outside of China showed a strong tendency not to be obstructed as evidenced by the projection of these coefficients into shifts in probabilities displayed in Table Two.

**Table Two – Likelihood shifts in probability of blocking by the CCP**[73]

| | Located within China, in Chinese | Located within China, not in Chinese | Located outside China, in Chinese | Located outside of China, not in Chinese |
|---|---:|---:|---:|---:|
| Democracy | 5.00% | 3.21% | 30.19% | 23.16% |
| Falun Gong | 20.62% | 14.11% | 63.93% | 58.05% |
| Tiananmen Square | 14.69% | 9.83% | 55.75% | 48.45% |
| Uyghur | 0.04% | 0.03% | 0.46% | 0.34% |
| Business | -0.83% | -0.64% | -9.86% | -6.34% |
| Joint Venture | -0.83% | -0.51% | -7.65% | -4.95% |
| Import | -0.56% | -0.35% | -4.99% | -3.27% |
| Invest | -0.98% | -0.60% | -9.22% | -5.93% |

[73] Likelihood shifts determined through Gary King, Jason Wittenberg, and Micahael Tomz, “Clarify: Software for Interpreting and Presenting Statistical Results,” *Journal of Statistical Software* 08, no. 01 (January 15, 2003), http://econpapers.repec.org/RePEc:jss:jstsof:08:i01.

Each value represents a percentage point change in the likelihood that a site would be obstructed through reactive censorship within a specific situation compared to the baseline established by the control group. So as an example a website which is in English and hosted in Canada dealing with a topic on Business in China would be 6.34% less likely to be blocked then a site from the randomly selected control list. These shifts in likelihood suggest that business websites are less likely to be blocked than their political counterparts and in some situations less likely than a site selected at random from a multi-topic list.

While these results demonstrate that business websites are  less likely to be blocked then political forms of content on the Internet, reactive techniques represent just one-half of the puzzle. Proactive strategies are more subtle, but no less important pieces of the puzzle. However, unlike reactive techniques there is no simple test to detect their presence. Therefore, a significantly smaller but more detailed examination based in case study is in order. By taking a close look at areas where the CCP intervenes and manages online content, it is possible to highlight patterns indicative of proactive strategies.

Since the primary focus of this paper is on the relationship between firms, the economy and content management, and business related websites are an area of low reactive management, these case studies will focus on proactive strategies dealing with firms and business websites operating within or dealing with China.

### The walled garden – China’s Intranet

While reactive censorship does not appear to affect significantly those websites related to business, this does not mean that this area is unmanaged. Proactive techniques can reach similar goals without obstructing the flow of information to the same degree as its reactive counterpart.

Because data is not necessarily being obstructed, penetration testing often fails to detect proactive management strategies. Therefore, a qualitative case study based approach is needed to determine if and how the CCP manages the information related to firms and economic activity on the Internet.

The structure of these case studies will follow the general process that businesses, both domestic and foreign, go through when attempting to become established both offline and online in the Chinese market. This will reveal the various content management strategies employed by the CCP at various stages throughout this process. An essential early step for entering a new market is establishing name recognition. On the Internet, this is usually done through domain name registration. Domain names, also called uniform resource locators (URLs) are text strings that identify and redirect users to a website. These tags become closely associated with a specific business and serve as a critical part of any marketing push. As an example, the popular search engine Google's URL, www.google.com, has moved into the pop culture lexicon as a verb, to Google.[74] When entering a new market, most companies attempt to set up a domestic web presence in the appropriate language. Domain name registers facilitate this process.

Registration services for domain names help groups obtain these addresses and resell them for a profit. Generally, users attempting to register a domain have to provide some basic information to the registrar such as their name and contact information. In December 2009, the CCP changed the rules for registration on .cn domain names, the extension code reserved for China. Users seeking to register a .cn domain name would have to provide a photograph and their business

[74] Geoffrey Nunberg, "As Google Goes, So Goes the Nation," *The New York Times*, May 18, 2003, sec. Week in Review, http://www.nytimes.com/2003/05/18/weekinreview/18NUNB.html?pagewanted=1..

license number.[75] This action generated protest from domain name providers. This protest accelerated when the CCP told registrars that they would have to gather this information retroactively for all previous .cn domain names and then forward this information to party controlled Internet Network Information Center for indexing and review.[76] Despite these onerous new rules only registrar, Godaddy.com, which registered a miniscule fraction all .cn domain names, continued its protest, and eventually withdrew from China. Other registrars appear to have chosen to comply with the rules and began gathering the required information.[77]

This example demonstrates the power of the CCP's national Intranet. An Intranet is the opposite of the Internet. It is a closed network, which operates for a select group of users. As an example, many businesses and academic institutions operate their own Intranets for exchanging files and data between employees.[78] While not a true Intranet, the idea of a Chinese domestic Intranet reflects the semi-closed nature of the Chinese Internet infrastructure.[79] At first glance, the Internet within China appears privatized. Independent ISPs exist and compete with each other by providing access and connectivity to corporate and individual clients. However, this veneer of competition hides the fact that the Internet is heavily nationalized within China. Each ISP does not provide access to the Internet through a private network. Instead, they lease access to the state network and its and six connections to the broader Internet.[80] All traffic entering and exiting

[75] Ellen Nakashima and Cecilia Kang, "In response to new rules, GoDaddy to stop registering domain names in China," *The Washington Post*, March 25, 2010, Online Edition , http://www.washingtonpost.com/wp-dyn/content/article/2010/03/24/AR2010032401543.html.
[76] ibid
[77] Owen Fletcher, "China Further Tightens Rules for Domain Name Owners," *PCWorld Magazine*, February 23, 2010, http://www.pcworld.com/article/190013/china_further_tightens_rules_for_domain_name_owners.html.
[78] James Callaghan, *Inside intranets and extranets* (Palgrave, 2002).
[79] Ronald J. Deibert, "Dark Guests and Great Firewalls: The Internet and Chinese Security Policy.," *Journal of Social Issues* 58, no. 1 (January 2002): 147.
[80] These connections are controlled by China Telecom, China Unicom, CST Net, CET Net, China Mobile Internet and CIER Net. Each one is either a state owned enterprise or has a majority of its stock controlled by other SOEs.

this network must pass through nodes controlled by the party and it reserves the right to deny or choke (artificially slow) connectivity as it sees fit.[81] This ability to manipulate the Internet at an infrastructure level also means that China can be selective about who can gain access to its domestic Intranet. This leaves businesses and other actors in a bind; because connectivity is essential for global commerce, they need access to the Internet, but the party controls connectivity. In order to do business within China, firms – both foreign and domestic – are forced to play by the party's rules in order to gain access.[82] When the CCP changed the rules surrounding domain name registration, they were able to back up this policy with their control over the domestic Internet infrastructure, which allows the party to convincingly threaten sanctions against those seeking, argue against or defy the new policies.[83]

This example demonstrates how physical network controls gives the CCP the ability to manage content online without resorting to reactive measures such as blocking. In order to gain access to the lucrative Chinese market and be competitive within that market, businesses need the Internet. Gaining access to the Internet within China requires playing by the rules put forward by the CCP. Actors who refuse to play by the rules can find their connectivity limited by the CCP's position of guarding all of the major incoming and outgoing routes, and protecting the semi-closed Chinese Intranet. Creating this Intranet is a classic proactive strategy. The CCP does not actually have to block potentially dangerous content after it has been created, instead it can

China Internet Network Information Center, "The 25th Statistical Survey Report on the Internet Development in China."

[81] Harwit and Clark, "Shaping the Internet in China. Evolution of Political Control over Network Infrastructure and Content," 397.

[82] Anne S.Y. Cheung, "The Business of Governance: China's Legislation on Content Regulation in Cyberspace," *New York University Journal of International Law* 38, no. 1 (2005): 18.

[83] Kathrin Hille, "China's domain name rules spur website flight," *Financial Times* (Bejing Bureau, February 1, 2010), Online edition, sec. China, http://www.ft.com/cms/s/0/7374f5ee-0f52-11df-a450-00144feabdc0,dwp_uuid=7799346e-6d6c-11da-a4df-0000779e2340,s01=1.html.

manage what actors are able to enter its domain. Businesses and other actors put up with these restrictions due to the massive incentive offered by the huge and rapidly expanding Chinese market. This allows the CCP to reconcile information controls with the need for economic growth.

## Tactical protection – Encryption and information security

Once a business is established, secrecy becomes an important concern. Whether it is internal communications, personal information, research and development or business plans, most firms rely on a degree of secrecy to function properly and conceal plans from the competition.

The most prominent method of ensuring secrecy online is encryption. Put simply, encryption is the process of taking information and transforming it into unintelligible data. Another user who has a proper "key" can then decode this data again. These keys are often quite long and practically unbreakable to third parties which lack the unlock code.[84] Encryption is widely available and used by even very small businesses to protect sensitive information both in transit (being sent from one user to another) and at rest (being stored).[85] Most companies have their own in-house encryption codes, which ensure that outside observers cannot read sensitive information.

The CCP heavily regulates encryption use within its borders despite the fact that encryption is a critical part of information secrecy for businesses of all varieties. By law, it is illegal to import

[84] Deibert, "Dark Guests and Great Firewalls," 150.
[85] David Kahn, *The Codebreakers: The Story of Secret Writing*, Reissue. (Macmillan Pub Co, 1974).

foreign encryption algorithms or devices specifically designed to encrypt data into China.[86] Specially licensed developers, many of whom are associated or part of the state apparatus, can only develop domestically developed algorithms.[87]

In effect, these restrictions mean that the CCP is holding the keys to most corporate secrets within its border. Regardless of the strength of the encryption, email, sensitive information and wireless transmissions can be decoded and read by simply applying a stored key to the information at hand.[88] Some foreign firms have lobbied successfully for the use of their own encryption software, but exceptions are only granted on a time-limited basis.[89] Because of this policy and the CCP's position, overseeing the entries and exits to the domestic Internet, a high degree of information security for businesses operating within China is eliminated.

Chinese encryption policy demonstrates another aspect of proactive management, state integration into essential online services.[90] Isolating encryption imports creates a need for the software among economic actors within China. In order to fulfill this demand, the CCP has funded the development of encryption software by promoting computer engineering and science within China.[91] The CCP has set up special zones designed to promote homegrown development and foster Internet start-ups. Additionally, the party also publicly funds the development of

[86] Ellen Messmer, "Encryption restrictions," *Network World*, March 14, 2004, http://www.networkworld.com/careers/2004/0315man.html.
[87] Ibid
[88] J. Mike Rayburn and Craig Conrad, "China's Internet Structure: Problems and Control Measures.," *International Journal of Management* 21, no. 4 (December 2004): 476.
[89] John McKenzie, Allan Marson, and Eugene Lim, "Decrypting China's Encryption Regulations" (presented at the Baker and McKenzie presentations, Palo Alto California, March 25, 2009), http://www.bakernet.com/NR/rdonlyres/BA2DDA1E-C5AB-4840-B060-BF70F64F0977/0/china_decryptingencryptionregulations_presentation_mar09.pdf.
[90] Kalathil and Boas, "Internet and State Control in Authoritarian Regimes: China, Cuba, and the Counterrevolution."
[91] Rayburn and Conrad, "China's Internet Structure," 476.

domestic software and hardware companies through subsidies and government contracts. Because these new businesses are operating within the Chinese economy, they are subject to the CCP's rules and regulations, as are the products that they choose to market. The result is an effective substitution of uncontrolled foreign products for their regulated Chinese counterparts.

Import restrictions create scarcity while party sponsorship of domestic software and encryption standards offer the only legal product to alleviate this demand. Despite the obvious economic benefits, the domestically produced substitutes are created under CCP regulations and contain the requisite backdoors which allow for monitoring and intervention should opposition or dissent spring up.

By applying the legal power of the state to market relationships, the CCP effectively inserts itself into business networks by making approved products "the only game in town." This allows the CCP to manage content without actively blocking or impeding data flows, maintaining the connectivity need for economic development while ensuring party control.

### Operation Aurora and stolen ideas – Electronic espionage and intellectual property

Encryption can be seen as tactical security, it protects specific transmissions and communications between actors. Of equal if not greater importance to business interests seeking to operate within China is strategic security, namely the protection of their intellectual property. Intellectual property is increasingly valuable in the modern knowledge-based economy and defining it can be difficult. Essentially intellectual property is proprietary information held by a business or individual via creation or acquisition that may aid their competitive success. This knowledge can range from patents to copyrighted materials and trade secrets. Theft of this property means the loss of a critical competitive edge in the increasingly cutthroat economy.

Businesses take a number of methods to secure their intellectual property, especially if it takes an online digital form. These precautions include firewalls, passwords, special servers and other barriers designed to prevent unauthorized access. However, businesses operating in China often have trouble securing these valuable assets. Cyber attacks, the theft of valuable code, blueprints and other ideas are a perennial issue within China and it generates a steady flow of valuable information out of the vaults and secure servers of firms and into the general market.[92]

A few case studies serve to demonstrate the breadth and depth of these transfers within China. During the summer of 2009, the CCP mandated the use of the "Green Dam Youth Escort" a "net-nanny" type program that blocks content while operating on a machine's hard drive, adding another layer to the already formidable Chinese content management network. This software is intended to protect children from exposure to pornography, although examination of the blacklist built into the program demonstrates that it also controls political content.[93] Shortly after the unveiling of the Green Dam software, an American firm, Solid Oak Software, alleged that it contained significant sections of code copied from their own "Cyber-sitter" software, leading to a $2.2-billion lawsuit against Chinese authorities and the company contracted to create the Green Dam software.[94]

Another, more recent example of code theft can be seen in early 2010 when Google announced that it, along other companies such as Dow Chemicals and Yahoo, had been the victim of

[92] Robert McMillan, "Google attack part of widespread spying effort - Computerworld," 13T05:37-05:00 1, 2010, http://www.computerworld.com/s/article/9144221/Google_attack_part_of_widespread_spying_effort. ""China is likely using its maturing computer network exploitation capability to support intelligence collection against the U.S. government and industry by conducting a long term, sophisticated computer network exploitation campaign."

[93] Robert Faris, Hal Roberts, and Stephanie Wang, *China's Green Dam: The Implications of Government Control Encroaching on the Home PC*, Executive Summary, Opennet Initiative Reports (University of Toronto, n.d.), http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc.

[94] "China sued by US software company," *BBC*, January 6, 2010, sec. Technology, http://news.bbc.co.uk/2/hi/technology/8442771.stm.

"Operation Aurora." The attackers exploited a previously unknown flaw in Microsoft's Internet Explorer browser (otherwise known as a "zero-day" attack) to break into numerous corporate servers.[95] Once inside, the perpetrators targeted and accessed sensitive databases including source-code repositories, the raw code which makes online services function.[96] The attackers also targeted the Google email (Gmail) accounts of Tibetan activists in an attempt to steal information from them.

The source code stolen from Google was revealed the be the "Gaia" system, a universal login that allows the holder to access any account hosted by Google, essentially the keys to any data which individuals or firms have entrusted to the search provider.[97] Google detected the attack the locked down the Gaia system but with access to the source code, the perpetrators may be able to find undiscovered vulnerabilities and break into the system once again.[98]

The theft of data and intellectual property has not been limited to computer code. As an example, a recent American trade delegation to China discovered that valuable information had been copied from secure laptops.[99] This information turned up again in meetings with party officials who displayed a surprising knowledge of the delegation's goals, objectives and what they were willing to concede, giving Chinese negotiators an advantage in the meeting. Data from the

[95] David Drummond, "A new approach to China: an update," *Official Google Blog*, March 22, 2010, http://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html.

[96] Kim Zetter, "Google Hack Attack Was Ultra Sophisticated, New Details Show | Threat Level | Wired.com," *Wired Magazine- Threat Level Blog*, January 14, 2010, http://www.wired.com/threatlevel/2010/01/operation-aurora/.

[97] John Markoff, "Cyberattack on Google Said to Hit Password System," *The New York Times*, April 19, 2010, sec. Technology, http://www.nytimes.com/2010/04/20/technology/20google.html.

[98] ibid

[99] Tom Leonard, "Chinese spies stole US trade secretary data," *Telegraph.co.uk*, May 30, 2008, http://www.telegraph.co.uk/news/worldnews/asia/china/2054874/Chinese-spies-stole-data-from-US-trade-secretarys-laptop.html.

laptops was used in an attempt to access secure databases in the United States.[100] Similarly, handheld personal data assistants have been hacked during meetings with party officials, resulting in information theft.[101] As a result, the Commerce Department in the United States has started advising the adoption of "sanitized" laptops with no valuable information on by executives and other businesses operating within China.[102]

Assigning responsibility for these incidents is notoriously difficult. It is impossible to say who within China is responsible for any one of the attacks described above due to the complexities of the Internet. However, the generally agreed upon trend is that intellectual property within China can be quite insecure.[103] Some analysts argue that the CCP is directly involved in these attacks based on the targets, the information obtained and the sophistication of various efforts, however it is impossible to establish firm culpability at this moment aside from determining that the attacks originated from China.[104] The generally lax standards surrounding intellectual property within China can be attributed to the Communist Party.

As part of its accession to the World Trade Organization (WTO) China agreed to enforce global standards surrounding patents, copyright and intellectual property within its border but simply because standards are in place it does mean that they are being enforced.[105] The CCP has shown a profound unwillingness to crack down on issues such as piracy and theft of firm's intellectual

[100] Shane Harris, "China's Cyber-Militia," *National Journal*, May 31, 2008, http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php.
[101] Ibid.
[102] Sky Canvaves, "U.S. Investigates Laptop Spying Suspicions," *Wall Street Journal* (New York, NY, May 30, 2008), Online edition, sec. China, http://blogs.wsj.com/chinarealtime/2008/05/30/us-investigates-laptop-spying-suspicions/tab/article/.
[103] Ernest J., III Wilson and Adam Segal, "Trends in China's Transition toward a Knowledge Economy," *Asian Survey* 45, no. 6 (12, 2005): 899.
[104] Nart Villeneuve, "The Aurora Mess," *Internet Censorship Explorer*, March 4, 2010, http://www.nartv.org/2010/03/04/the-aurora-mess/.
[105] Wilson and Segal, "Trends in China's Transition toward a Knowledge Economy," 899.

property, especially when it takes place over the Internet, letting cases stagnate and delay in the labyrinthine party/state bureaucracy.[106]

While this foot-dragging can be partially attributed to the inability of the party to comprehensively tackle the issue of intellectual property, it is also important to remember that these thefts also supplement a larger proactive strategy of bolstering state capacity using the Internet. The Green Dam example mentioned earlier demonstrates this principle in action. While it is unlikely that the CCP directly stole the code from Solid Oak Software, it is clear that they benefited from it. Instead of paying a significantly higher fee to import technology and having to negotiate with a foreign firm over the politically dangerous issue of content restrictions, the same product could be offered by a Chinese firm without any of these problems, and at a lower price.

Intellectual property theft, whether it is trade secrets, Google’s universal password or raw code from the Cyber-sitter application, gives the CCP access to these commodities within the infinitely more pliable domestic market. The CCP can simply amalgamate and repurpose these technologies to suit their needs while saving time and money on research and development. This in turn boosts state capacity and provides new powers such as the ability to disaggregate censorship to user’s hard drives through the Green Dam software. In addition to this boost in state capacity, the free flow of trade secrets within China makes corporate surveillance significantly easier.[107] When a company’s strategic plans or newest product are leaked and distributed on the Internet, obtaining information about them becomes more accessible, allowing the CCP to keep closer tabs on firms operating within its jurisdiction.

[106] ibid

[107] For an example of this surveillance see “Germany accuses China of industrial espionage | World news | The Guardian,” July 22, 2009, http://www.guardian.co.uk/world/2009/jul/22/germany-china-industrial-espionage.

All of these factors demonstrate that while the CCP may not be directly behind the various thefts and cyber attacks that have been taking place with disturbing regularity over the past few years, it does benefit from them through the increase in state capacity and surveillance, which results from having such sensitive information circulating in the public realm. The key to the successful implementation of this proactive strategy is the free flow of information that allows data to enter China freely, demonstrating how the CCP reconciles the need for free information and the desire to maintain control.

## Chapter Three: The effects of content management in action

### China and Google – The troubled relationship

These case studies clearly demonstrate the creation and implementation of proactive content management strategies within China by the CCP. However, establishing the presence of these techniques still does not answer the second question posed at the start of this examination; how does content management effect the development of the Chinese economy? In order to answer the question the various strategies and techniques previously outlined need to be examined when acting together in a situation with implications for the development of the Chinese economy. The 2009-2010 dispute involving Google and the CCP provides an excellent case study.

The Google situation is informative for several reasons. First, it is a recent series of events, allowing for an up-to-date picture of the CCP's Internet strategy in action. Additionally, the fate of Google has profound implications for the broader Chinese economy and Internet.

Google operates as an information broker, facilitating the retrieval, storage and generation of data for individuals and firms. Beyond its famous search capabilities, Google offers a suite of productivity, communication and research.[108] This critical role makes Google a lynchpin in many firms' online strategies. This means that Google's fate within China has profound implications not just for Google, but also for the thousands for firms and small businesses that depend on its services. All of these factors mean that examining the dispute between Google and the CCP regarding the implementation of content management strategies offers a chance to observe how the political need for control on the Internet is influencing business.

[108] Clive Thompson, "Google's China Problem (and China's Google Problem)," *The New York Times Magazine*, April 23, 2006, http://courses.washington.edu/imt551/content/NYT_Magazine_Googles_China_Problem.pdf.

Google first entered the Chinese market indirectly in 2000 when its engineers managed to establish a search protocol that recognized simplified Chinese characters.[109] Users with IP addresses located within China were simply redirected from the standard Google homepage to a sub domain that handled Chinese language requests. All of the servers and the technology that facilitated this transition were located in California, outside the regulation of the CCP. Google's presence within China grew steadily, especially among the business and upper middle classes within Chinese society.[110] In 2002, the CCP responded by placing a block on Google that rendered it relatively inaccessible. While users could circumvent these measures, the vast majority lacked the motivation and time to response and instead simply migrated to competing services such as Baidu, a domestic competitor of Google, which benefited tremendously from the measures.[111] A few weeks later access was restored but connections were slow and downtime was frequent. Meanwhile Baidu proceeded to dominate the local search market. In 2006, Google finally entered the Chinese market with Google.cn, a Chinese language service that complied with state policy by removing blacklisted sites from search results.[112]

Google took a significant public relations hit within the United States and other areas which do not extensively manage content online, however it did  recapture some of its Chinese market share, although still dwarfed by the now massive Baidu service. It continued to operate without significant incident until late 2009 and early 2010. At this point Google announced the existence

[109] "Google China History: Google's Biggest China Controversies," *Huffington Post*, March 8, 2010, http://www.huffingtonpost.com/2010/01/13/google-china-history-time_n_422488.html.
[110] Clive Thompson, "Google's China Problem (and China's Google Problem)," *The New York Times Magazine*, April 23, 2006, http://courses.washington.edu/imt551/content/NYT_Magazine_Googles_China_Problem.pdf.
[111] ibid
[112] ibid

of Operation Aurora and the breach of its servers.[113] In response, Google stopped censoring search results, displaying blocked sites in search results (although access to these sites was still limited by reactive blocking by the CCP). In order to facilitate this new policy, Google also shifted its servers to Hong Kong, taking advantage of the less restrictive controls on the island.[114] This uneasy situation persisted until late June 2010 when Google shifted it stance again. Google.cn no long automatically redirected users to the Hong Kong version of the site. Instead, users were forced to click through and physically choose to access unrestricted services.[115]

Underlying this narrative is the constant presence of content management strategies and their role in shaping the strategic actions of Google and its competitors such as Baidu. Each one of the strategies outlined in the previous section has affected the choices and movements of Google and its rivals within the Chinese market. The VOC literature points toward five areas that require coordination between firms using institutions such as the Internet; industrial relations, skills and education, corporate governance, inter-firm relations and employees.[116]

## The implications of control

The primary economic effect of Chinese content management strategies appears to be the selective disruption of coordination between firms, which in turn distorts the market within China and alters the process of globalization. As demonstrated in the first half of this paper, reactive censorship is not a significant factor for corporate information, but proactive

[113] David Drummond, “A new approach to China,” *Official Google Blog*, January 12, 2010, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.
[114] Ibid.
[115] “Google in 'new approach' on China,” *BBC*, June 30, 2010, sec. Business, http://news.bbc.co.uk/2/hi/business/10443648.stm.
[116] Hall and Soskice, *Varieties of capitalism*, 6-7.

management strategies appear disrupt and alter deliberation and information exchange between firms in a distinct manner. Each of the three proactive mechanisms, including the domestic Intranet, technology-use policy and information gathering techniques, affect the ability of firms to relate with their suppliers, competitors and possible allies, and thus coordinate their actions.

Arguably, the most important element of the CCP's proactive Internet strategy is the maintenance of a domestic Intranet. This allows the CCP to control who enters its domestic Internet and impose regulations upon them. Theoretically, the presence of a domestic Intranet would not be a problem for most companies; they could simply host their data in a more accommodating jurisdiction and then access it when doing business within China. However, the existence of a reactive censorship regime makes this option less attractive.

While the examination at the start of this paper demonstrated that economic sites are not as extensively controlled as other varieties of online content, the CCP is notoriously fickle when choosing what sites to block. Since the criteria and timing of blocks is completely unpublished, firms can often find their own sites or those belonging to critical partners and services unavailable when they need them for seemingly arbitrary reasons. A simple example demonstrates this danger; Ars Technica is a popular technology industry blog, which rarely if ever comments on China.[117] However, the advertisements on the site occasionally link to blacklisted URLs causing Ars Technica to become unavailable at times from within China. The solution to this problem is to operate inside the Great Firewall of China and set up a presence on the Chinese Internet.  This process requires firms to register of a license with the MIIT, which must then be periodically renewed in order to maintain a commercial web presence within

[117] "Ars Technica," Technology Blog, n.d., http://arstechnica.com/.

China.[118] However, due to the domestic Intranet, this requirement means conforming to Chinese content management policy. Essentially, the combination of an unstable reactive censorship apparatus, and the ability of the CCP to leverage the power of its domestic Intranet to foist regulations on site owners, leads to the commoditization of secure access. In exchange for providing their compliance and conformation to regulations, firms receive secure connections. Putting this idea in an alternative frame, the CCP is exploiting the needs of firms to have secure reliable institutions for information exchange and deliberation in order to secure compliance with domestic regulations. Without consistent and reliable Internet access, firms lose the ability to coordinate access within their company and with suppliers and consumers, crippling their ability to solve the collective action problems facing all businesses.

An example of this process can be seen in the case of Google between 2002 and 2006. As mentioned earlier, Google entered the Chinese market in 2000 with a translated search page hosted in California. In 2002, the Chinese government began to block intermittently Google, occasionally restricting access to the site. While Google remained accessible for the vast majority of time, these actions by the CCP made it unreliable. This damaged the inter-firm relations between Google, its advertisers and its audience, making effective business significantly more difficult. In order to bypass these restrictions, Google was forced to "purchase" reliable access to the Chinese Intranet by agreeing to conform to content management strategies.[119] This ability to force a tradeoff between regulation and access means that the CCP is able to introduce extensive regulation into the Internet, an area considered

[118] Jason Dean and Peppi Kiviniemi, "China Is Still Reviewing Google's License," *The Wall Street Journal* (New York, July 8, 2010), Online  edition, sec. Technology, http://online.wsj.com/article/SB10001424052748703636404575352363052493380.html?mod=googlenews_wsj.
[119] Thompson, "Google's China Problem (and China's Google Problem)."

difficult to control. By exploiting firm's need for secure flows of information into order to solve the coordination problems inherent in business transactions, the CCP is able to generate a more closely regulated online environment than other states by making regulation a condition for access to the institutions that can help solve these issues.

Of course, as the most recent financial crisis has taught the world, regulation does not always equal compliance. Firms have a great deal of autonomy and power, and can sometimes bypass regulations through a combination of persuasion, coercion and inducement.[120] The most strictly worded regulations in the world are often defeated by the dexterity and skill of the entities they are attempting to control. This issue of information scarcity regarding the internal operations of firms is bypassed by the presence of rampant intellectual property theft within China. These actions release large quantities of information, moving it from corporate servers onto the Internet. This movement makes this data more accessible to regulators by shifting it from isolated corporate servers into general circulation. An example of this policy in action can be seen with the Aurora attacks against Google that prompted the company's withdrawal from China. The attacks targeted emails belonging to dissidents, mainly those held by Tibetan exiles. However, the secondary objective was access to Google's source code repositories, some of the most secure data hosted by Google. More specifically, the attackers accessed Google's Gaia system, which as described earlier is a universal login that provides access to any Google account, making every user, firm or entity utilizing Google's products vulnerable.[121] Since the attack was detected, Google has chosen to add an extra layer of security to the Gaia system but

[120] China's first attempt to introduce domestic encryption was slowed by corporate lobbying but it returned in 2009., see: Sumner Lemon, "China's WAPI will not go down without a fight," May 30, 2006, http://www.networkworld.com/news/2006/053006-chinas-wapi-protocol.html. and "Made-in-China WAPI standard resubmitted for global use," *APA*, June 2, 2009, http://en.apa.az/news.php?id=104668.
[121] Markoff, "Cyberattack on Google Said to Hit Password System."

the theft of the source code makes future attacks much easier.[122] The movement of this information from Google's secure servers, through hackers and into the market makes gathering information about Google significantly easier.

In addition, it is important to remember that the Aurora attacks were not just targeting Google. Most firms refuse to acknowledge that their servers were broken into but more than twenty major firms experienced break-ins. Source code, financial statements, corporate memos, long-term strategies and confidential communiqués are just some of the information that was or has been accessed through cyber attacks on businesses operating within and outside of China. This information flows back into the PRC where it benefits domestic firms (which are easier to control than their foreign counterparts are) or ends up in the hands of the CCP. Either way, this valuable information suddenly becomes infinitely more accessible for the CCP making data gathering and effective

Because of this increased regulatory advantage, the CCP is able to put its second proactive strategy into effect, the restriction on specific technologies within China. The CCP blocked the importation and implementation of numerous technologies and services within China. The classic example is encryption, as described earlier of this examination. One can also see this technique at work in the ongoing battle between Google and the CCP. Using its regulatory power, which springs from the existence of a domestic Intranet, the CCP has instituted a complex series of licenses and controls on essential technologies.[123] Without acknowledgment from the party, a firm cannot import or implement these technologies within China. As an

[122] ibid
[123] Dean and Kiviniemi, "China Is Still Reviewing Google's License."

example, geo-location and mapping technologies are currently not implemented in China.[124] The CCP held a licensing competition for firms to receive the ability to bring this technology to China and Google put forward with its Google Maps tool. Despite being a well-established leader in the field, Google lost the competition to domestic sites, namely the large web portals such as Sohu and Sino.[125] The control of these technologies has political repercussions (geo-location and mapping software has been used in the past as a form of citizen surveillance and for planning protests) these limitations also affect the Chinese economy. Mapping services and geo-location are essential parts of the modern supply chain allowing for coordination between firms on issues such as deliveries, cross national transactions and meetings.[126] Similarly, encryption protocols also play a role in both business and politics and have been used to secure communication regarding high-level corporate transactions and protest movements.

This elimination of specific technologies for political reasons cripples the ability of the Internet to act as an effective forum of deliberation and coordination between firms. Without these and other technologies restricted by the CCP, firms lose the ability to communicate securely and perform other essential tasks while making use of the power of the Internet to bridge time and space. Instead of forcing firms to do without these products and crippling their ability to coordinate with each other, the CCP has engaged in what is essentially a politicized version of import substitution industrialization by funding the development of Chinese equivalents to these existing services while barring the introduction of foreign competitors. While the rationale

[124] Mike Clendenin, “China Snubs Google Maps -- China-Google -- InformationWeek,” *Information Week*, n.d., http://www.informationweek.com/news/infrastructure/management/showArticle.jhtml?articleID=225702048&cid=RSSfeed_IWK_News.

[125] Ibid.

[126] For an example see Andrew Nusca, “Foursquare lands Starbucks as partner; geolocation meets lattes,” *ZDNet*, March 12, 2010, http://www.zdnet.com/blog/gadgetreviews/foursquare-lands-starbucks-as-partner-geolocation-meets-lattes/13199.

behind this policy appears to be generally political, aiming to neutralize the political threats posed by online communication, the economic side effects results in the creation of a parallel Chinese technology industry. Once again, the case study of Google illustrates the point. When examining the global share of the search and information retrieval industry, most users and firms appear to have settled on a few predominantly American services (Google, Yahoo, and Microsoft). These services are available in a multitude of languages and have generally succeeding in invading and dominating unrestricted foreign markets.[127] However, China is a special case; it has its own national search service (Baidu) as well as other developing domestic technology firms specializing in restricted areas such as encryption.[128] While most of the world appears to be converging around universal standards for online information location, exchange and security, the PRC is charting its own path, fostering the growth of domestic alternatives and local standards that conform to the party's political needs.

Firms operating within China are forced to make use of these domestic services because they lack access to the technologies that they normally utilize to secure, coordinate and facilitate information exchange. However, firms are constrained by the need to appease the CCP to maintain connectivity and lack of alternative services due to party regulation, forcing them to make use of local copies, further fueling the growth of various domestic industries while providing the party with the ability to maintain surveillance within its borders.

[127] Net Market Share, "Search engine market share," n.d., http://marketshare.hitslink.com/search-engine-market-share.aspx?qprid=4.

[128] "Made-in-China WAPI standard resubmitted for global use."

## Chapter Four: Conclusion

In summary, the cumulative economic side effects of content control are as follows.

1) The creation of a domestic Intranet means that the CCP can impose a higher quantity of regulation over firms' activities online than most other states by exploiting the need for secure and reliable connections and trading access for compliance.

2) This regulation is effective due to the constant flow of information out of corporate servers into the Chinese marketplace, making data mining and information gathering much easier for the CCP.

3) Once firms are operating within China, the party blocks specific technologies that make the Internet an effective venue for communication and deliberation. Without access to these technologies, firms cannot solve the collective action problems inherent to business activities, forcing them to rely on vulnerable domestic equivalents in order to maintain communication.

The effects of these strategies can be seen in the case study of Google's trials and tribulations within the Chinese market. While many firms may not directly experience the problems that Google has, its fate is still significant. Google provides critical services to firms operating within China, and changes in its status within the PRC will have a profound impact on the way firms operate within the country.

Contemplating the fate of Google brings this paper back to the opening questions: How does China reconcile the need for economic growth and control? Is content management and intervention into the Internet part of a broader, distinctive approach to globalization? Does intervention within the Internet alter the overall trajectory of the Chinese globalization project or alter what the final product might look like? Between the penetration testing of the "Great Firewall of China" to determine the accessibility of hundreds of different websites, the in-depth examination of proactive strategies and their application within China, and the examination of the Internet's role in economics, answers to all three questions are available to some extent.

With respect to the first question, it appears clear that the CCP does not apply reactive censorship as heavily to those websites deemed essential for economic growth. Instead, it applies a series of more subtle proactive strategies, which aim to shape and alter the priorities of firms in order to make coincide with the party's own preferences. These strategies include the creation of a domestic Intranet, the control of strategic technologies, and the facilitation of unwilling information exchange from firms into the Chinese marketplace. Each one of these strategies allows the CCP to manipulate, regulate and survey firms operating within its borders while maintaining the connectivity needed for business.

These strategies also affect the way the Chinese economy operates; shifting the form globalization within China takes. The combination of increased regulation, the chance for property theft and usage restrictions all serve to deter foreign technology and Internet service firms from operating within China. This deterrence springs from the fact that they often feel the brunt of Chinese regulation and can even be restricted from entering the Chinese market. In addition, these firms are highly dependent on knowledge and ideas as well as highly transportable products such as computer code, making them particularly susceptible to intellectual property theft.  Because of this aversion or rejection from the Chinese market, there seems to be a move towards the rapid development of powerful domestic firms to fill the void. China is the only country in the world to have a powerful "national" search engine (Baidu) catering to users within its borders. The rest of the globe makes use of regional variations of Google, Yahoo and Microsoft’s Bing service. Additionally, China has highly developed encryption, domain name and content control services well beyond those found in other parts of the world, especially in developing economies.[129] These variations are the result of content management strategies that exclude or penalize competing foreign products and facilitate the transfer of expertise and information to Chinese firms.  As a result, information technology within China is diverging from the rest of the world and embracing alternative standards and rules.

### The future of the Internet within China

This trend has repercussions for the entire Chinese economy because firms operating within China need to utilize the Internet in order to collaborate and facilitate inter-firm communications. The Internet depends on interoperability. In order to remain global, the protocols used by a firm in China need to be the same as the one it uses in Europe or the United States or else interoperability breaks down, destroying the global reach of the Internet which makes it so attractive. The divergent Chinese tech industry caters first to the needs of the CCP (whose policies allow it to succeed) and then to its users. As a result, Chinese standards have diverged from their global counterparts. Chinese search engines are more likely to turn over data, encryption protocols work only within the PRC and other unique quirks set the domestic marketplace apart from the globe.

While the long-term results of these divergent standards generated by the CCP’s need to maintain some form of control and surveillance are hard to predict, it seems clear that they are

[129] Wilson and Segal, “Trends in China's Transition toward a Knowledge Economy.”

running contrary to global trends. As the rest of the world moves towards interoperability in order to facilitate communications between firms and transactions over borders, China is remaining stubbornly resilient.[130] For the time being, firms appear to be willing to accept this divergence, most likely because the Chinese market offers other incentives such as low labor costs and a vast unchecked pool of domestic demand. Nevertheless, as these advantages are tapped and exploited, the contradictions and disadvantages generated by the CCP's management strategies may become more and more grinding, opening up the possibility for pressure and reform somewhere in the future.

Pressure for change is most likely to arise from the breakdown of the incentives that make doing business within China attractive for foreign firms. These organizations, as opposed to their domestic Chinese counterparts, are more likely to press for change for three reasons:

1) Foreign firms generally have experience with different and more liberalized regulatory structures, making them more aware of the costs imposed by the CCP's strategy.

2) Foreign firms are likely to experience political pressure in their home countries because of their dealings with China. This is obviously not an issue for Chinese businesses.

3) Foreign firms are able to utilize the threat of exit and voice due to their legal autonomy in their dealings with the CCP, whereas their Chinese counterparts often lack this protection.

[130] For an example see the divergence between the WPA and WAPI standards of Wifi encryption: Basu, "China Forges Ahead With Homegrown WAPI Standard Instead of Wi-Fi."

The reduction of incentives to accept divergent Internet standards is ongoing and seems to be driven by two interrelated factors; the growing public awareness of Chinese Internet controls, and the gradually emergence of clearly dominant players within sections of the Chinese domestic market. These trends highlight the costs imposed by divergent Chinese technologies standards by damaging a firm's public image and reducing the probability of profit within the Chinese market in addition to the direct costs of accommodating the CCP's push for divergent standards.

The first major factor in reducing the incentives to comply with the CCP's management strategies is the increasing recognition of Chinese censorship and Internet policy among governments and the public. Several events have contributed to this development, most notably the Ghostnet attacks on Tibetan dissidents and the recent spat between Google and the CCP. Ghostnet refers to a network of Trojan horse programs that were discovered in the computers of various embassies and Tibetan dissidents around the world.[131] This program gave its handlers access to emails and secure information as well as enabling them covertly to activate microphones and web cameras on infected computers in order to gather information not input into the machine.[132] Although culpability for this attack has not been firmly established, there is strong evidence linking it to CCP servers.[133] Regardless of who was responsible for the Ghostnet attacks, the media adopted the frame of a state-sponsored cyber attack and the event was

[131] Ronald J. Deibert et al., "Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor,* March 29, 2009, 42-43, http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network..

[132] Malcolm Moore, "China's global cyber-espionage network GhostNet penetrates 103 countries," *Telegraph.co.uk*, March 29, 2009, http://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-global-cyber-espionage-network-GhostNet-penetrates-103-countries.html.

[133] Shishir Nagaraja, *The snooping dragon: social-malware surveillance of the Tibet movement*, Cambridge Computer Laboratory Technical Reports (Cambridge, UK: Cambridge University, March 2009), http://scholar.google.ca/scholar?cluster=8308699034073564142&hl=en&as_sdt=2000.

publicized as such.[134] A few months afterward, Google released the details of the Operation Aurora attacks, the details of which have already been discussed. When taken together, these events generated a significant increase in interest about the Internet and China, and this public scrutiny is directed towards businesses that operate within China.[135] Compounding this pressure is a series of government investigations, most notably an inquiry by Congress in United States, into technology transfers and collaboration between firms and the Chinese government.[136]

These pressures generate extremely negative public relations for firms seen to be collaborating with the CCP and its spying or repressive activities. Although it is true that public opinion is not as important to businesses as to political actors, this steady increase in pressure increases the likelihood that consumers will utilize their "voice" to express displeasure with the current state of affairs or simply "exit" and avoid purchasing altogether.[137] While the percentage that will actually go through with this process will most likely remain small, the extreme negative perception of Chinese Internet strategy still provides an important factor in party/business relations.

Another important element increasing opposition to the CCP's Internet strategy is the increasingly solidified nature of the Chinese market. China contains a vast quantity of potential customers. However, some areas of this developing market have stabilized around a few key players. Newcomers or late arrivals often find themselves frozen out of a potentially lucrative

[134] Moore, "China's global cyber-espionage network GhostNet penetrates 103 countries."

[135] Searches for Censorship and China have tripled since the start of 2010. "China Censorship," *Google Trends*, April 14, 2010, http://www.google.com/trends?q=China+Censorship.

[136] Anjai Bhat, "U.S. Senate Subcommittee Examines American Companies' Compliance With Censorship Abroad," 2010/03/08, *The Columbia Science and Technology Review*, n.d., http://www.stlr.org/2010/03/u-s-senate-subcommittee-examines-american-companies%E2%80%99-compliance-with-censorship-abroad/.

[137] Albert O. Hirschman, *Exit, voice, and loyalty* (Harvard University Press, 1970).

situation. The example of GoDaddy, the DNS service that was discussed earlier in this examination is a perfect example of this trend. By most accounts, GoDaddy failed to crack the Chinese market, losing out to other DNS service providers.[138] Similarly, Google was also having trouble in China and facing stiff competition from the homegrown alternative search engine Baidu.[139] Companies that are losing within the Chinese market no longer have the promise of profit and riches to add incentive to their compliance, making the perceived costs of compliance with Chinese regulation and commands more acute. This facilitates the use of exit or voice by the corporation itself in an attempt to bring pressure to bear on the CCP to alter its policy and alleviate some costs. This reform would theoretically make competition freer and grant losing companies a respite. As the Chinese market continues to develop and solidify, the potential number of losing firms will only grow, increasing pressure on the CCP.

If foreign firms are successful at winning concessions from the CCP, their victories are likely to benefit Chinese businesses as well. The loosening of regulation for foreign businesses but not their Chinese counterparts would put Chinese entrepreneurs at a disadvantage and generate political pressure within the PRC from an important constituency. Any victories won due to pressure from outside China are likely to spread and affect actors within it.[140] Ideally, these changes would lead to greater social pressure for Internet reform within China, as managers and businesspeople compare the access which they have at work to that in their personal life. However, if twenty years of engagement between the CCP and the Internet has demonstrated anything it is that the party remains surprising and adaptable to new situations.

[138] Ryan Singel, "Go Daddy Says China Refusal Is No PR Stunt," *Wired Magizine- Epicenter Blog*, March 25, 2010, http://www.wired.com/epicenter/2010/03/go-daddy-china-stunt/.
[139] "Google loses China market share," *BBC*, August 30, 2005, sec. Business, http://news.bbc.co.uk/2/hi/business/4197834.stm.
[140] Deibert, "Dark Guests and Great Firewalls," 152.

## Bibliography

"Alexa the Web Information Company," n.d. http://www.alexa.com/.

"Ars Technica." Technology Blog, n.d. http://arstechnica.com/.

Barlow, John Perry. "A Declaration of the Independence of Cyberspace.." *Humanist* 56, no. 3 (May 1996): 18-19.

Basu, Indrajit. "China Forges Ahead With Homegrown WAPI Standard Instead of Wi-Fi." *Government Technology,* September 27, 2006. http://www.govtech.com/gt/articles/101267.

Belson, Ken. "Senator's Slip of the Tongue Keeps on Truckin' Over the Web." *The New York Times*, July 17, 2006, sec. Business / Media & Advertising. http://www.nytimes.com/2006/07/17/business/media/17stevens.html?_r=1.

Berman, Ari. "Iran's Twitter Revolution." *The Nation*, June 15, 2009. http://www.thenation.com/blogs/notion/443634.

Bhat, Anjai. "U.S. Senate Subcommittee Examines American Companies' Compliance With Censorship Abroad." 2010/03/08. *The Columbia Science and Technology Review,* n.d. http://www.stlr.org/2010/03/u-s-senate-subcommittee-examines-american-companies%E2%80%99-compliance-with-censorship-abroad/.

Callaghan, James. *Inside intranets and extranets*. Palgrave, 2002.

Canvaves, Sky. "U.S. Investigates Laptop Spying Suspicions." *Wall Street Journal*. New York, NY, May 30, 2008, Online edition, sec. China. http://blogs.wsj.com/chinarealtime/2008/05/30/us-investigates-laptop-spying-suspicions/tab/article/.

Chase, Michael, and James C. Mulvenon. *You've got dissent!* Rand Corporation, 2002.

Cheung, Anne S.Y. "The Business of Governance: China's Legislation on Content Regulation in Cyberspace." *New York University Journal of International Law* 38, no. 1 (2005).

"China Censorship." *Google Trends*, April 14, 2010. http://www.google.com/trends?q=China+Censorship.

"China defends screening software." *BBC*, June 9, 2009, sec. Asia-Pacific. http://news.bbc.co.uk/2/hi/asia-pacific/8091044.stm.

China Internet Network Information Center. "The 25th Statistical Survey Report on the Internet Development in China," March 15, 2010. http://www.cnnic.net.cn/uploadfiles/pdf/2010/3/15/142705.pdf.

"China sued by US software company." *BBC*, January 6, 2010, sec. Technology. http://news.bbc.co.uk/2/hi/technology/8442771.stm.

Clendenin, Mike. "China Snubs Google Maps -- China-Google -- InformationWeek." *Information Week,* n.d. http://www.informationweek.com/news/infrastructure/management/showArticle.jhtml?articleID=225702048&cid=RSSfeed_IWK_News.

Dean, Jason, and Peppi Kiviniemi. "China Is Still Reviewing Google's License." *The Wall Street Journal*. New York, July 8, 2010, Online edition, sec. Technology. http://online.wsj.com/article/SB10001424052748703636404575352363052493380.html?mod=googlenews_wsj.

Deibert, Ronald J. "Dark Guests and Great Firewalls: The Internet and Chinese Security Policy.." *Journal of Social Issues* 58, no. 1 (January 2002): 143.

Deibert, Ronald J., Arnav Manchanda, Rafal Rohozinski, Nart Villeneuve, and Greg Walton.

"Tracking GhostNet: Investigating a Cyber Espionage Network." *Information Warfare Monitor*, March 29, 2009. http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network.

Deibert, Ronald J., John G. Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds. "Measuring Global Filtering." In *Access Denied: The Practice and Policy of Global Internet Filtering*. 1st ed. The MIT Press, 2008.

Drezner, Daniel W. "Globalization and Policy Convergence." *International Studies Review* 3, no. 1 (Spring 2001): 53-78.

Drummond, David. "A new approach to China." *Official Google Blog*, January 12, 2010. http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

———. "A new approach to China: an update." *Official Google Blog*, March 22, 2010. http://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html.

Faris, Robert, Hal Roberts, and Stephanie Wang. *China's Green Dam: The Implications of Government Control Encroaching on the Home PC*. Executive Summary. Opennet Initiative Reports. University of Toronto, n.d. http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc.

Fletcher, Owen. "China Further Tightens Rules for Domain Name Owners." *PCWorld Magazine*, February 23, 2010. http://www.pcworld.com/article/190013/china_further_tightens_rules_for_domain_name_owners.html.

Frieden, Jeffry A., and Ronald Rogowski. "The Impact of International Economy." In *Internationalization and domestic politics*, edited by Robert Owen Keohane and Helen V. Milner. Cambridge University Press, 1996.

Friedman, Thomas L. *The Lexus and the olive tree*. Random House of Canada, 2000.

"Germany accuses China of industrial espionage | World news | The Guardian," July 22, 2009. http://www.guardian.co.uk/world/2009/jul/22/germany-china-industrial-espionage.

Goldsmith, Jack L., and Tim Wu. *Who controls the Internet?: illusions of a borderless world*. Oxford University Press US, 2006.

"Google China History: Google's Biggest China Controversies." *Huffington Post*, March 8, 2010. http://www.huffingtonpost.com/2010/01/13/google-china-history-time_n_422488.html.

"Google in 'new approach' on China." *BBC*, June 30, 2010, sec. Business. http://news.bbc.co.uk/2/hi/business/10443648.stm.

"Google loses China market share." *BBC*, August 30, 2005, sec. Business. http://news.bbc.co.uk/2/hi/business/4197834.stm.

Gourevitch, Peter Alexis, and James Shinn. *Political power and corporate control: the new global politics of corporate governance*. Princeton University Press, 2007.

Govcom. "Censorship Explorer." Digital Methods Tool, March 15, 2010. http://tools.issuecrawler.net/beta/proxies/.

———. "Google Scraper," n.d. http://tools.issuecrawler.net/beta/scrapeGoogle/.

Hachigian, Nina. "China's Cyber-Strategy." *Foreign Affairs* 80, no. 2 (April 2001): 118-133.

Hall, Peter A., and David W. Soskice. *Varieties of capitalism: the institutional foundations of comparative advantage*. Oxford University Press, 2001.

Harris, Shane. "China's Cyber-Militia." *National Journal*, May 31, 2008. http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php.

Hartman, Amir, and John Kador. *Net Ready: Strategies for Success in the E-conomy*. McGraw-Hill Professional, 2000. http://portal.acm.org/citation.cfm?id=555667.

Harwit, Eric, and Duncan Clark. “Shaping the Internet in China. Evolution of Political Control over Network Infrastructure and Content.” *Asian Survey* 41, no. 3 (6, 2001): 377-408.

Hille, Kathrin. “China’s domain name rules spur website flight.” *Financial Times*. Bejing Bureau, February 1, 2010, Online edition, sec. China. http://www.ft.com/cms/s/0/7374f5ee-0f52-11df-a450-00144feabdc0,dwp_uuid=7799346e-6d6c-11da-a4df-0000779e2340,s01=1.html.

Hirschman, Albert O. *Exit, voice, and loyalty*. Harvard University Press, 1970.

“Internet Archive: Free Movies, Music, Books & Wayback Machine,” n.d. http://www.archive.org/.

Kahn, David. *The Codebreakers: The Story of Secret Writing*. Reissue. Macmillan Pub Co, 1974.

Kalathil, Shanthi. *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule*. Washington, D.C: Carnegie Endowment for International Peace, 2003.

Kalathil, Shanthi, and Taylor C Boas. “Internet and State Control in Authoritarian Regimes: China, Cuba, and the Counterrevolution.” *Carnegie Papers* 1, no. 21. Carnegie Endowment for International Peace (July 21, 2001). http://www.carnegieendowment.org/publications/index.cfm?fa=view&id=728.

———. “The Internet and state control in authoritarian regimes.” Text, August 6, 2001. http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/876/785.

King, Gary, Jason Wittenberg, and Micahael Tomz. “Clarify: Software for Interpreting and Presenting Statistical Results.” *Journal of Statistical Software* 08, no. 01 (January 15, 2003). http://econpapers.repec.org/RePEc:jss:jstsof:08:i01.

Lacharite, Jason. “Electronic Decentralization in China: A Critical Analysis of Internet Filtering Policies in the People's Republic of China.” *Australian Journal of Political Science* 37, no. 2 (2002): 333.

Leonard, Tom. “Chinese spies stole US trade secretary data.” *Telegraph.co.uk*, May 30, 2008. http://www.telegraph.co.uk/news/worldnews/asia/china/2054874/Chinese-spies-stole-data-from-US-trade-secretarys-laptop.html.

Ma, Lianjie, Jongpil Chung, and Stuart Thorson. “E-government in China: Bringing economic development through administrative reform.” *Government Information Quarterly* 22, no. 1 (2005): 20-37.

MacKinnon, Rebecca. *CHINA - "Race to the Bottom" Corporate Complicity in Chinese Internet Censorship*. Human Rights Watch, 2006.

———. “Flatter world and thicker walls? Blogs, censorship and civic discourse in China.” *Public Choice* 134, no. 1 (January 1, 2008): 31-46.

“Made-in-China WAPI standard resubmitted for global use.” *APA*, June 2, 2009. http://en.apa.az/news.php?id=104668.

Markoff, John. “Cyberattack on Google Said to Hit Password System.” *The New York Times*, April 19, 2010, sec. Technology. http://www.nytimes.com/2010/04/20/technology/20google.html.

McKenzie, John, Allan Marson, and Eugene Lim. “Decrpyting China's Encryption Regulations” presented at the Baker and McKenzie presentations, Palo Alto California, March 25, 2009. http://www.bakernet.com/NR/rdonlyres/BA2DDA1E-C5AB-4840-B060-BF70F64F0977/0/china_decryptingencryptionregulations_presentation_mar09.pdf.

Messmer, Ellen. “Encryption restrictions.” *Network World*, March 14, 2004. http://www.networkworld.com/careers/2004/0315man.html.

Moore, Malcolm. “China's global cyber-espionage network GhostNet penetrates 103 countries.”

*Telegraph.co.uk*, March 29, 2009. http://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-global-cyber-espionage-network-GhostNet-penetrates-103-countries.html.

Nagaraja, Shishir. *The snooping dragon: social-malware surveillance of the Tibet movement*. Cambridge Computer Laboratory Technical Reports. Cambridge, UK: Cambridge University, March 2009. http://scholar.google.ca/scholar?cluster=8308699034073564142&hl=en&as_sdt=2000.

Nakashima, Ellen, and Cecilia Kang. "In response to new rules, GoDaddy to stop registering domain names in China." *The Washington Post*, March 25, 2010, Online Edition  edition. http://www.washingtonpost.com/wp-dyn/content/article/2010/03/24/AR2010032401543.html.

National Science Foundation. "The Internet: Changing the Way We Communicate," n.d. http://www.nsf.gov/about/history/nsf0050/internet/internet.htm.

Net Market Share. "Search engine market share," n.d. http://marketshare.hitslink.com/search-engine-market-share.aspx?qprid=4.

Nunberg, Geoffrey. "As Google Goes, So Goes the Nation." *The New York Times*, May 18, 2003, sec. Week in Review. http://www.nytimes.com/2003/05/18/weekinreview/18NUNB.html?pagewanted=1.

Nusca, Andrew. "Foursquare lands Starbucks as partner; geolocation meets lattes." *ZDNet*, March 12, 2010. http://www.zdnet.com/blog/gadgetreviews/foursquare-lands-starbucks-as-partner-geolocation-meets-lattes/13199.

OpenNet Initiative. "About Filtering," n.d. http://opennet.net/about-filtering.

———. "Country Profile- China," June 15, 2009. http://opennet.net/research/profiles/china.

Qiang, Xiao. "China News: Image of Internet police: JingJing and Chacha online." *China Digital Times*, January 22, 2006. http://chinadigitaltimes.net/2006/01/image-of-internet-police-jingjing-and-chacha-online-hong-yan-o%C2%BAae%C2%A5%E2%84%A2aaio%C2%BAa/.

Rayburn, J. Mike, and Craig Conrad. "China's Internet Structure: Problems and Control Measures.." *International Journal of Management* 21, no. 4 (December 2004): 471-480.

Robert McMillan. "Google attack part of widespread spying effort - Computerworld," 13T05:37-05:00 1, 2010. http://www.computerworld.com/s/article/9144221/Google_attack_part_of_widespread_spying_effort.

"ScrapeBox – Harvest, Check, Ping, Post," n.d. http://www.scrapebox.com/.

Shirky, Clay. "Power Laws, Weblogs, and Inequality." *Clay Shirky's Writings About the Internet*, February 8, 2003. http://www.shirky.com/writings/powerlaw_weblog.html.

Singel, Ryan. "Go Daddy Says China Refusal Is No PR Stunt." *Wired Magizine- Epicenter Blog*, March 25, 2010. http://www.wired.com/epicenter/2010/03/go-daddy-china-stunt/.

Siriyuvasak, Ubonrat. "People's media and communication rights in Indonesia and the Philippines." *Inter-Asia Cultural Studies* 6, no. 2 (2005): 245.

Skocpol, Theda, and Edwin Amenta. "Did Capitalists Shape Social Security?." *American Sociological Review* 50, no. 4 (August 1985): 572-575.

StataCorp. "Stata Statistical Software: Release 11," 2009. http://www.stata.com/support/faqs/res/cite.html.

Sumner Lemon. "China's WAPI will not go down without a fight," May 30, 2006. http://www.networkworld.com/news/2006/053006-chinas-wapi-protocol.html.

Tai, Zixue. *The Internet in China : cyberspace and civil society*. New York: Routledge,, 2006.

The Citizen's Lab. “Country  Profile: Iran,” May 9, 2007. http://opennet.net/research/profiles/iran.

Thompson, Clive. “Google's China Problem (and China's Google Problem).” *The New York Times Magazine*, April 23, 2006. http://courses.washington.edu/imt551/content/NYT_Magazine_Googles_China_Problem.pdf.

———. “Google's China Problem (and China's Google Problem).” *The New York Times Magazine*, April 23, 2006. http://courses.washington.edu/imt551/content/NYT_Magazine_Googles_China_Problem.pdf.

Trend, David. *Reading digital culture*. Wiley-Blackwell, 2001.

“US PC makers in 'stolen code' row.” *BBC*, June 15, 2009, sec. Technology. http://news.bbc.co.uk/2/hi/8101978.stm.

Villeneuve, Nart. “The Aurora Mess.” *Internet Censorship Explorer*, March 4, 2010. http://www.nartv.org/2010/03/04/the-aurora-mess/.

Wacker, Gurdun. “The Internet and Censorship in China.” In *China and the Internet : politics of the digital leap forward*, edited by Christopher R. Hughes and Gurdun Wacker, xiii, 178 p. : ill. ; 24 cm. London ; New York: Routledge Curzon, 2003.

Williams, Dmitri, Nicolas Ducheneaut, Li Xiong, Yuanyuan Zhang, Nick Yee, and Eric Nickell. “From Tree House to Barracks: The Social Life of Guilds in World of Warcraft.” *Games and Culture* 1, no. 4 (October 1, 2006): 338-361.

Wilson, Ernest J., III, and Adam Segal. “Trends in China's Transition toward a Knowledge Economy.” *Asian Survey* 45, no. 6 (12, 2005): 886-906.

“Xinjiang: an 'internet prison'.” *BBC*, February 3, 2010, sec. Asia-Pacific. http://news.bbc.co.uk/2/hi/8492224.stm.

“XROXY.COM - more than just proxy,” n.d. http://www.xroxy.com/.

Xu, Sean, Kevin Zhu, and Jennifer Gibbs. “Global Technology, Local Adoption: A Cross-Country Investigation of Internet Adoption by Companies in the United States and China.” *Electronic Markets* 14, no. 1 (2004): 13.

“Yahoo 'helped jail China writer'.” *BBC*, September 7, 2005, sec. Asia-Pacific. http://news.bbc.co.uk/2/hi/4221538.stm.

York, Jillian. “ONI Affiliate Reveals Chinese Surveillance of Skype Messages.” *OpenNet Initiative*, October 2, 2008. http://opennet.net/blog/2008/10/oni-affiliate-reveals-chinese-surveillance-skype-messages.

Zetter, Kim. “Google Hack Attack Was Ultra Sophisticated, New Details Show | Threat Level | Wired.com.” *Wired Magizine- Threat Level Blog*, January 14, 2010. http://www.wired.com/threatlevel/2010/01/operation-aurora/.

Zysman, John. *Governments, markets, and growth : financial systems and the politics of industrial change*. Ithaca N.Y.: Cornell University Press, 1983.

## Appendix: Methodology and sample selection

This section will address the selection and sampling of websites used for the section on reactive controls. Three specific elements of the methodology used to gather the data presented within this examination will be elaborated in more detail; the selection of websites to test, the actual testing process and the interpretation of the results

The goal of these test was to determine what websites are reactively blocked by the Chinese Communist Party. Reactive blocking refers to the obstruction of access to a website for a user attempting to access it within China. This does not affect the server hosting the website and it generally still available for users from other jurisdictions. Since the criteria used by China to determine which websites are selected for blocking are a closely guarded secret examinations such as the one conducted in this paper provide valuable insights into the CCP's policy as well as furthering the arguments made in this examination.

The first step in the process of testing blocking within China is to generate a list of websites to be examined. For the purposes of this examination the websites selected were chosen in an attempt to mimic the behavior of actual users. That is to say websites were selected by "scraping" the results of search criteria and selecting the top sites returned by a search string. With only finite resources these searches could be either broad or deep. Broad searches would gather a smaller number of the top URLs from a wide range of search terms (i.e. 10 search terms 100 URLs each). Deep searches focus on fewer search terms and gather more URLs (i.e. 2 search terms, 500 URLs each). A relatively broad approach was selected for this examination for several reasons. First a broad approach allowed for a greater variety of search terms, ensuring that the results presented were less likely to be susceptible to quirks within the CCPs blocking protocol.

Additionally a broad approach is a better approximation of the search habits of users. The distribution of visits to websites tends to follow a "Power Law" type distribution. This means that 20% of the websites within a given field generally gather 80% of the visits, with the remainder squabbling over the left over users.[141] An easy example of this trend can be seen in the field of social networking sites. A few powerful sites such as Facebook and MySpace gather the majority of visits, with a large quantity of more obscure sites splitting the remainder. By adopting a broad search protocol the top and most popular sites from each search term can be gathered, providing the URLS which gather the vast majority of visitors within each specific area.

The search terms used to gather URLs are as follows

**Table I – Search terms utilized for URL collection**

| **Search Terms** | |
|---|---|
| **English** | **Simplified Chinese characters** |
| Democracy in China | 民主中国 |
| Falun Gong | 法轮功 |
| Uyghur | 维吾尔 |
| Tiananmen Square Protest | 六四事件 (June 4th Incident, Chinese name for the protests) |
| Business in China | 在中国的业务 |
| Investment in China | 投资中国 |
| Joint Venture in China | 合资企业在中国 |
| Import from China | 从中国进口 |

[141] Clay Shirky, “Power Laws, Weblogs, and Inequality,” *Clay Shirky's Writings About the Internet*, February 8, 2003, http://www.shirky.com/writings/powerlaw_weblog.html.

All of these search terms were gathered using Google.[142] Although Baidu is more popular within China it is unsuitable as a search engine for this brand of research because inputting specific terms will trigger a response and block the search and any future queries for several minutes. This makes gathering URLs for controversial search strings such as "Falun Gong" impossible.

The top 100 results from each search term were gathered, with some omissions and additions for broken links or strongly related websites detected by the search tool. In addition a random selection of websites was gathered from a list of the top one million websites in the world published by the website ranking service Alexa which serves as a control group drawn from a non-specific list websites with a similar level of popularity.[143]

In some cases there were duplicate domains between the various search terms. As an example the popular video sharing website Youtube or the online encyclopedia Wikipedia appeared in the results of multiple search strings. In these cases the specific URL which was returned was tested, so the specific video or article on Wikipedia as opposed to the general domain name.

Testing to see if the gathered websites were blocked within the PRC required the development of a new testing protocol. The current system employed by the CCP blocks access to blacklisted websites not only at the moment of access, but also for up to ten minutes afterwards. This means that testing protocols which relied on a single connection within China were either crushingly slow or simply did not function.

[142] Govcom, “Google Scraper,” n.d., http://tools.issuecrawler.net/beta/scrapeGoogle/.
[143] “Alexa the Web Information Company,” n.d., http://www.alexa.com/.

To bypass these problems a new protocol was developed, centering around a repurposed Search Engine Optimization (SEO) tool called Scrapebox.[144] SEO tools are used by individuals to increase a website's placement on a search engine, moving it up towards the top of reported results. This can be done by generating links, hits and posting comments on websites to attract visitors. SEO tools automate this process and utilize proxies (computers which provide an alternative connection) to make it appear that a website is drawing visitors from a wide and diverse audience. For the purposes of this examination Scrapebox was repurposed to become an automated censorship explorer. This was done through the combination of two functions, a "ping mode" and a rotating proxy list.[145] Pinging is a way to test if a website is accessible. Instead of loading the entire site and all its content a computer can send a small packet a data called a ping to the server hosting a website in question. If the website is available it will respond to the ping giving its status. Essentially each website gathered through search engine scraping was inputted into Scrapebox. The program was also instructed to use a list of Chinese proxy servers which simulated having a Chinese Internet connection. The list of websites was then pinged to determine their availability. This technique bypassed Chinese controls because Scrapebox was programmed to shuffle randomly between proxies and discard ones which had been blocked, ensuring a functioning connection to the website being tested. Each website was tested three times over the course of two weeks in order to ensure that any downtime was not due to a temporary server failure or other technical trouble. If a website was reported to be inaccessible at least two times out of three in these tests it was labeled as being blocked by the CCP. In order to

[144] “ScrapeBox – Harvest, Check, Ping, Post,” n.d., http://www.scrapebox.com/.

[145] Proxies drawn from “XROXY.COM - more than just proxy,” n.d., http://www.xroxy.com/.

ensure accuracy a sampling of those websites reported to be blocked were also checked by hand through a browser to determine if they were actually being blocked.

The results of these tests were collated into a dataset. The variables used as outlined below

**Table II – Description of independent and dependent variables**

| **Dependent variable** | |
|---|---|
| Name | Description |
| Blocked | Accessibility within China (0-Accessible, 1-Blocked) |
| **Independent variables** | |
| Keyword related variables. *(Democracy, Falun Gong, Tiananmen Square, Uyghur, Business, Joint Venture, Import, Invest)* | Website appeared within the search related to the given keyword in English or Chinese. (0-Did not appear, 1- Appeared) |
| Domestic | Website was hosted within China (0-Hosted outside of China, 1- Hosted within) |
| Language | Website appeared in Chinese language during the keyword search (0-Did not appear, 1-Appeared) |
| Page Rank | Measure of how many links the URL has, higher page rank means the site is more interconnected and popular |
| Popular Random Sample | Websites randomly selected from the Alexa top one million |

These variables were then examined through logistic regression with a bivariate dependent variable representing whether a term was blocked or not via the STATA software package. Translation of the coefficients into shifts in likelihood was undertaken using CLARIFY add-on by Gary King.