INTERNET CENSORSHIP IN CHINA

By

Joseph House

Submitted to the Faculty of the School of International Service

of American University

in Partial Fulfillment of

the Requirements for the Degree of

Master of Arts

in

International Politics

Chair:

Professor Amitav Acharya, PhD

Professor Eric Novotny, PhD

Dean of School of International Service

2011

American University

Washington, DC 20016

INTERNET CENSORSHIP IN CHINA

BY

Joseph House

ABSTRACT

Internet censorship in China is considered to be the most sophisticated in the world. However, it is also misunderstood. Many authors view the internet as a quick fix for democratization in the country. This thesis will study the history, tactics, and actors within the Chinese government's information control systems, showing that the Chinese government runs a nuanced system of information control used to maintain its authoritarian regime. Further, the Chinese government has proven to be quite adept at utilizing the internet, suggesting caution and restraint should be the proper responses to the use of the internet for democratization in China.

Acknowledgements

There are many people I have to thank for helping to get me through the arduous task of writing and preparing this thesis. Chief amongst these people is my wife, Lysette, who never stopped believing that, yes, I could do this. Day after day, she provided me with tireless (and often thankless) strength in completing this thesis. The same can be said for my friends and family who constantly pushed me to make this thesis my priority, even when I did not want to listen to them. In truth, any major project is a group effort, a collaboration between the writer and the support network he puts around him. I also need to thank Professors Amitav Acharya and Eric Novotny for providing solid, constructive criticism and helping me to achieve this goal. In that same vein, I must also thank the staff at SIS graduate advising who handled all my administrative questions with care, precision, and depth.

Table of Contents

Chapter

List of Tables and Figures

List of Figures

Chapter 1: Introduction and Methodology

The internet has often been referred to as a defense against closed and authoritarian societies. Thus, the censorship of the internet would be an affront to a free society, allowing for an authoritarian government to stay in power. However, many authors have chosen to focus on a more vague and general discussion of the democratizing power of the internet. Few have gone the route prescribed by Evgeny Morozov, who urges a path of cyber realism, where discussions of the power of the internet focus on the internet in a single country, focusing on the political context within that country and the pros and cons of the use of the internet, both within that context and in general.[1] This thesis will seek to follow Morozov's framework, looking at the overall picture of Chinese internet censorship (as well as the political history and context in modern China, particularly as it relates to speech) in an effort to discuss the topic of internet censorship in China. The censorship of the internet in China has often been referred to as the most sophisticated censorship system in use today. This censorship is conducted in a manner that seeks to bolster regime stability, though it is often portrayed as actions undertaken to promote the security of China. This paper will argue that China's internet censorship is undertaken by the Chinese government to maintain legitimacy and stability through the suppression of communication and coordination of opposition groups. It will be argued that the censorship of the internet is both a direct and indirect affront to human rights in China. Further, it will be argued that this censorship is part of the historical political context in China, where censorship and government intervention have a long history.

The argument regarding how China conducts internet censorship will be tied to the direct abuse of human rights perpetrated by internet censorship. This discussion will be carried out by

[1] Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom*, (New York, PublicAffairs, 2011), xvii.

discussing the history of China’s internet censorship and their policies and procedures. This will include discussions of China’s relations with multinational corporations. This discussion will largely take place in chapters 2, 3 and 4. The argument regarding why China conducts internet censorship will focus on both China as a specific case study and overarching theoretical perspectives on internet censorship. These discussions will mainly occur in chapters 4, 5, and 6. These chapters will explore, in specific, the ideas of authoritarian resilience and the use or restriction of coordination goods by dictatorial and authoritarian states to maintain their rule. In an effort to present a complete argument, these chapters will also reference legitimate concerns that may be held by the Chinese government when discussing internet censorship. However, this thesis will also attempt to debunk aspects of these concerns as reactionary, given the state of China’s relationship with the internet and the vague nature of many terms regarding cybersecurity.

This paper will follow a theoretical framework brought up by Evgeny Morozov, that of cyber realism. Cyber realism, according to Morozov, is a way of thinking about the internet and technology that views them as pieces within a political structure that can be used by both citizens and the government. It stands in direct opposition to cyber utopianism, which always gives citizens the upper hand in technology issues. Further, it also stands against those who argue that the internet is inherently apolitical and not a part of the overall political context in a country. Morozov says that much of the policy prescriptions since the inception of the internet and its rise to prominence have come from those who ascribe to cyber utopianism. This paper will seek to view Chinese censorship through a lens of cyber realism, presenting policy solutions that are clear and based in the social, political, and cultural context of present-day China. Much of the modern discussions of censorship, both in China and elsewhere, have been plagued by cyber-utopianism. Cyber-utopianism, according to Morozov, is “a naïve belief in the emancipator nature of online communication that rests on a stubborn refusal to acknowledge its downside.”[2] Such thoughts, as per Morozov, have led to an increased desire to enlist technology start-ups in quests for democracy around the world, something he refers to as the “Google Doctrine.”[3] Given that much of the discussion has focused on the internet in general, focusing very little on the political and cultural context of China, a reliance on these utopian views and the Google Doctrine could be catastrophic in the case of China. This thesis will urge restraint and further study. Policy prescriptions for this problem would be premature, given the lack of knowledge of the local context. In China, a free communications system may have to follow democratization, not lead to it.

When literature has not focused on the internet in general, it has focused only on certain aspects of this topic. Much of the literature has focused on the actions taken by the Chinese government to censor the internet or the media. Other authors have focused on the technical aspects of the censorship in China. Also, much of the literature has focused on comparing the Chinese government to other regimes that have censored the internet and the media. Only a few studies have decided to look at the overall picture of internet censorship in China. Many of these authors have chosen to examine the topic within the context of other aspects of international politics (moving them dangerously close to the idea of cyber utopianism). One author which provides an extremely informative and in depth discussion of censorship is Yuezhi Zhao, in his book, *Communications in China: Political Economy, Power, and Conflict.* In the book, Zhao looked at the issue of internet censorship (along with other aspects of media control in China)

[2] Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom*, (New York: PublicAffairs, 2011), xiii.
[3] Ibid.

within the context of political economy.[4] Specifically, Zhao looked at the level of censorship relative to the amount of exposure that a particular medium received. He noted that television got the most censorship, since it was the most widespread, followed by print media, and, then, the internet. He also noted that the fringes of the internet were where dissident groups and others were often quarantined. This was done as a means of silencing them through poor connectivity and an unstable section of network while they were able to evade censorship. He refers to this as "multiple layers of censorship."[5] Zhao talks about China's reliance on "passive censorship." Passive censorship, according to Zhao, is an attempt to limit the impact of an offending story by ensuring that the story is isolated to a small group of elites but restricted from the masses.[6] Zhao argues that such measures are more practical and that the Chinese government has "given up on the political indoctrination of the population.[7] Overall, Zhao says that the government is looking to decentralize its efforts at media control to 1) be more effective in their censorship and 2) limit political cost.[8] All of this, according to Zhao, is in support of the Chinese Communist Party (CCP)'s new goal of "effective domination" of communication in China as opposed to "total control of media matters."[9] Zhao's argument is bolstered by numerous authors in the field which have noted that the revolutionary power of the internet may be undermined by effective measures to dominate communications, rather than control all messaging. Robert Peters argued, "China has made an internet community largely antithetical to the West."[10] Taylor C. Boas argued as far back as 2000 that China had a strategy for the diffusion of the internet and how to control the

[4] Yuezhi Zhao, *Communication in China: Political Economy, Power, and Conflict*, (Lanham, MD: Rowan & Littlefield Publishers, 2008).
[5] Ibid, 36.
[6] Ibid, 34.
[7] Ibid.
[8] Ibid.
[9] Ibid, 35.
[10] Robert Peters, "China, Democracy, and the Internet," in *Information Technology and World Politics,* ed. Michael J. Mazaar, (New York: Palgrave MacMillan, 2002), 109.

system.[11] Many other authors have used an argument similar to Zhao's to argue that the revolutionary presence of the internet is an illusion. Peters sums this up nicely by noting that the internet is nothing more than a tool.[12]

Zhao's overarching argument that the Chinese are investigating ways to pursue effective domination of communication while still promoting technological development reveals a time shift in the discussion on this topic. Many of the early writers on the censorship of the internet, or even the presence of the internet, in China, were discussing the nature of the internet as a revolutionary tool. Politicians and public figures had been, for years, touting the nature of the internet as something that could destroy an authoritarian regime. As China began developing the internet, many authors began either touting the internet as the death knell for the Chinese government or arguing that there were ways that the Chinese government could still promote internet development and be an authoritarian state. Zhao effectively gives an account of Chinese censorship that relies on the political and social context within the country. His portrayal of the Chinese government is not one of evil bureaucrats looking for every way to limit communications or of a naïve and scared government running from the proposition of the internet. Instead, his view is nuanced and focuses on the actions of the Chinese. As such, it stands as an example of how authors should approach this topic.

Much of the remaining literature focused on specific aspects of the history of China's internet censorship. Much of this writing is vital to creating the historical context of internet censorship in China. Jack Linchuan Qiu looked at the discussion through a dichotomy of the

[11] Taylor C. Boas, "Weaving the Authoritarian Web: The Control of Internet Use in Non-Democratic Regimes," in *How Revolutionary was the Digital Revolution,* ed. Zysman and Newman, (Stanford, CA: Stanford Business Books, 2000), 371.
[12] Robert Peters, "China, Democracy, and the Internet," in *Information Technology and World Politics,* ed. Michael J. Mazaar, (New York: Palgrave MacMillan, 2002), 111.

upper classes in the cities and the lower class (often migrant) segments of the cities.[13] Qiu argues that lower class groups (labor groups, etc.) are blocked from the internet and that much of Chinese regulation has come about from their regulations on internet cafes, where the initial resurgence of the Chinese government's presence online began with its late 1990s assault on the Falun Gong.[14] Obviously, these two approaches are linked. The assumption would be that lower class groups are isolated from the internet so that they can be prevented from sharing their stories while also being kept in the dark about the plight of other groups with different sets of problems. Zhao makes an important note that the Chinese government is especially interested in preventing the spread of information to the masses, willing to let it pass amongst a small group of elites and go no further.[15]

Jens Damm and Simona Thomas compiled a book that looked at the issue in terms of technological changes and political effects.[16] Articles within the book, like Eric Harwit and Duncan Clark's, viewed the issue in terms of creation and control, examining who created and controls the overall network in China and who creates and controls the content.[17] However, while this approach seems to be radically different, it still harbors some of the same approach as that of Qiu, who makes a big deal out of internet cafes and the role of the government in shaping their technology to maneuver.[18] These arguments are just a basic argument of that discussion, laying a

[13] Jack Linchaun Qiu, *Working-Class Network Society: Communications and the Information Have-Nots in Urban China,* (Cambridge, MA: The MIT Press, 2009).

[14] Ibid, 122 and 33-35.

[15] Yuezhi Zhao, *Communication in China: Political Economy, Power, and Conflict*, (Lanham, MD: Rowan & Littlefield Publishers, 2008), 57-58.

[16] Jens Damm and Simona Thomas, ed., *Chinese Cyberspaces: Technological Changes and Political Effects*, (New York: Routlege, 2006).

[17] Eric Harwit and Duncan Clark, "Government Policy and Political Control over China's Internet," in *Chinese Cyberspaces: Technological Changes and Political Effects*, Jens Damm and Simona Thomas, ed., (New York: Routlege, 2006), 12.

[18] Jack Linchaun Qiu, *Working-Class Network Society: Communications and the Information Have-Nots in Urban China,* (Cambridge, MA: The MIT Press, 2009), 33-35.

technological framework for the discussion. This technological framework is vital and the fact that it is missing from so much of the literature in favor of slews of case studies is troubling. This thesis will seek to tell less stories about the Chinese censors (of which there are many) in favor of including a technical explanation and a solid backing in arguments of human rights and cybersecurity. This will be done as an effort to provide a truly multi-disciplinary and original work that gives this topic the synthesis it so desperately needs.

While all of these approaches are necessary to getting a good overall view of Chinese internet censorship practices, none of these individual approaches are able to fully explain the intricacies of the Chinese censorship regime. Arguably, Zhao comes closest; providing excellent historical context, through his focus on all media, including the internet, and China's censorship measures. The main reason none of these arguments effectively tackle the issue of internet censorship is because they fail to combine their arguments into an overall narrative that describes the Chinese censorship regime in a linear fashion. While many of the studies discuss the history and development of Chinese censorship, few discuss the possibilities of the continuation of Chinese censorship in its current form. Studies often look at what would happen if the internet was to become a freer medium in China. However, few studies discuss the possibility that the Chinese censorship regime will be maintained or will increase its efforts, especially with a higher number of internet users than ever. This study will seek to combine the human rights, political economy, and political development arguments, along with other arguments, to determine a rationale for the Chinese censorship regime that takes into account its history and development, its technological nuances, and its implications for human rights and political development in China.

Outside of the authors focusing specifically on China or specifically on internet censorship, there are a few important theories that will help to drive this thesis. One of these theories is the theory of “strategic coordination” and authoritarian leaders, which is articulated by Bruce Bueno de Mesquina and George Downs. This argument, which uses China’s internet censorship as an example, discusses how authoritarian leaders can stifle “coordination goods” that are intended for political and social rivals.[19] Downs and Mesquina define these goods as “those public goods that critically affect the ability of political opponents to coordinate but that have relatively little impact on economic growth.”[20] While this theory mainly deals with the pitfalls of those who link development with democracy, it also shows how a government that is willing to engage in behaviors such as internet censorship can hope to maintain control over its citizenry. This, it will be argued, is a major part of the justification of China’s internet censorship.

Another theory which tangentially touches on this topic is that of “authoritarian resilience,” which was coined by Andrew Nathan in his article of the same name from January 2003. Nathan’s theory specifically discusses China’s ability to maintain its regime, despite the after effects of Tiananmen Square in the international market. While it focuses on China’s overall political system, the discussion does at times, look at communications in China and the differentiating of institutions within the Chinese government.[21] Given that some of this institutional differentiation has to do with certain aspects of the government controlling information and propaganda, one can see the tangential link to the issue of internet censorship.

[19] Bruce Bueno de Mesquina and George Downs, “Development and Democracy,” *Foreign Policy,* 84, 5 (September-October 2005): 81-82.
[20] Ibid, 82.
[21] Andrew J. Nathan, “China’s Changing of the Guard: Authoritarian Resilience,” *Journal of Democracy,* 14, 1 (January 2003): 11-12.

Methodology and Outline

This thesis will examine these theories by combining theories and information from the previous literature with interviews with members of the international NGO community, academia, and government. The project will begin with an overall introduction to the topic of censorship of the internet in China. The second chapter will discuss the history of the network in China and the methods used by the government in censoring the internet. This history would include a discussion of the increasing importance of cyberwarfare in general, with special discussions related to China. This history would also include who created and controls the network. It will also examine the technical aspects of the Chinese censorship regime. Cyberwarfare needs to be discussed as a topic given the legitimate importance that can be placed on the topic by the Chinese government. As a means of debunking any legitimate claims the government may have for censoring the internet, this is important. As a method of understanding the discussion of internet censorship, the chapter will also discuss some specific efforts of the Chinese government related to internet censorship.

This discussion will be continued in the third chapter, which will discuss the increasing role of multinational corporations in China’s internet censorship regime. Here, the project will also seek to show the increasing role of multinational corporations in the censorship of the internet in China, providing a detailed timeline of the actions of MNCs in the recent history of the internet in China. Companies discussed include Microsoft, Cisco, Yahoo, and Google. The discussion of Google pays special attention to the actions of the past few years, in which the Chinese and Google sparred over the hacking of many Google e-mail addresses and Google’s contention to remove its search engine from behind the Chinese “Great Firewall.” This discussion will not merely end with a discussion of the companies that have aided or have a mixed record toward the Chinese censorship regime. It will also discuss the work of Bill Xia's Dynamic Internet Technologies and other companies that have worked against the Chinese internet censorship regime. Here, there will be some discussion of hacktivism and network activism, a discussion that will be completed while discussing cybersecurity later in the project.

Once this discussion is completed, the project will examine the censorship of the internet as an indirect abuse of human rights, citing both the ability of the Chinese government to cover up abuses of human rights and the inability of dissident and democracy groups to gain effective traction, based on the repression of coordination goods. The fourth chapter will detail human rights abuses committed by the Chinese government and show how such offenses were kept out of the mainstream media, including high traffic areas of the internet. This chapter will also discuss the notion that human rights are universal, discounting the "Asian values" debates that are often pointed to as reasoning for not only China's censorship regime but also for their human rights record. Also, this chapter will discuss coordination goods in depth. The definition of coordination goods comes from a paper on political development by Bruce Bueno de Mesquina and George Downs. The basic idea is that certain goods are necessary for a group to succeed in gaining political power and traction within a society. Downs and Mesquina directly reference the idea of communication amongst members as coordination goods.[22] Thus, any internet censorship which limits this communication, either through direct means (disruption of sites) or other means (by placing such sites and groups within poorly maintained and vulnerable sections of the Chinese network) reduces the ability of these groups to effectively become a part of the community, which limits their right to self-determination.

[22] Bruce Bueno de Mesquina and George Downs, "Development and Democracy," *Foreign Policy,* 84, 5 (September-October 2005): 82.

The fifth chapter will follow this discussion with a discussion of authoritarian resilience, describing the methods in which the Chinese government has been able to maintain stability, in spite of the beliefs of many experts on the stability and longevity of the Chinese regime, especially in the aftermath of the Tiananmen Square incident and with the precedent of the USSR and several Eastern European countries.[23] The contention that will be posited in this thesis is that the censorship of the internet, combined with the censorship of the media, helps to improve the stability of the Chinese regime. This chapter will posit that the Chinese government is engaged in its actions to censor and control the internet to prevent dissident groups and others from gaining an effective foothold through cyberconflict. These dissidents will be discussed in the terms of cyberconflict, such as hacktivism, electronic civil disobedience, and network activism. These terms will be defined and placed in the Chinese context, thus outlining the message that the Chinese government is not interested in sitting by while reformers and revolutionaries begin to act within their country. As such, they view the censorship of the internet as vital to controlling their state and improving the resiliency of their regime.

The final chapter will serve as a conclusion of the thesis. The conclusion will issue a warning that policymakers should use restraint when engaging the idea of the use of internet to attack the Chinese regime. The Chinese system is simply too nuanced and broad to expect the use of the internet to have massive impact. This chapter will note the overall point of this thesis – that the Chinese government has sought to engage the internet in ways to defend its governmental actions and in ways to carry out is governmental actions This argument is important as many have seen the internet as a magical democratizing force and not merely a tool for coordination and communication (which can be used by governments as well as citizens and

[23] Andrew J. Nathan, “China’s Changing of the Guard: Authoritarian Resilience,” *Journal of Democracy,* 14, 1 (January 2003).

activists). While this paper argues that the censorship of the internet is a direct and indirect human rights abuse, largely because of its clashes with free association and self-determination through association, it is important to realize that a free internet does not magically produce association and new governments. It is important to realize that there are methods beyond censorship that can control speech on the internet and that the political, social, and cultural context of a country is important when determining the power of internet censorship within a country, as well as the policy prescriptions for that country.

Chapter 2: The History of the Internet and Control in China: A Multidimensional Issue

In understanding China's censorship and attempts to control the internet, we must look at the history of the internet in China and the government's efforts to control the medium as a means of social control. As such, this chapter will investigate a series of aspects of the internet in China. First, it will investigate the dispersion of the physical networks of the internet in China. Then, it will discuss the history of internet service providers (ISPs) in China. Then, the chapter will turn to a discussion of China's efforts to control the medium. Further, this chapter will end with a discussion of the methods that the Chinese government has implemented that would be considered part of a cyberwarfare or cyberconflict paradigm. In short, this chapter will investigate the changing role and infrastructure of the internet in China. Further, this chapter will discuss how these changes have impacted the Chinese government's efforts to censor and control the internet. This chapter will argue that, as the internet has become more engrained in China; the overall strategy of the Chinese government has altered, allowing for a multifaceted strategy that seeks to effectively control communications in China, as opposed to an outright domination of communications in the country. This change in strategy has been affected by the presence of cybersecurity concerns and the nature of the Chinese government to rely on information warfare as a tactic.

Part I: The History of the Physical Internet Infrastructure in China

China's internet use began in earnest in the mid-1990s, originally being used for universities in the country.[24] The original network, China Education and Research Network (CERNET), leased its lines from the Ministry of Posts and Telecommunications (MPT), which,

[24] Eric Harwit and Duncan Clark, "Government Policy and Political Control over China's Internet," in *Chinese Cyberspaces: Technological Changes and Political Effects*, Jens Damm and Simona Thomas, ed., (New York: Routledge, 2006), 15.

in 1998, became the Ministry of Information Industry (MII).[25] CERNET had some competition from Ministry of Electronics Industry (MEI) and China Netcom, which was part of State Administration of Radio, Film, and Television (SARFT) and the Ministry of Railways.[26] With the internet still in its infancy in the late 1990s, something marked by the multiple ministries vying for control of the network, access was somewhat constrained. As such, the internet café was extremely important in China. Jack Linchuan Qiu notes that, from 1998 to 2001, the internet café was the greatest venue for internet access in China.[27] (Qiu, 33-34).

By the year 2000, there were three more networks in China.[28] The wireless industry in China was largely controlled by the Chinese government.[29] However, the network in China was starting to grow. This was expedited by the entrance of companies from the United States into the Chinese market. In the early 2000s, US companies entered the Chinese internet market. Many of these help with the "biggest state censorship campaign ever." Some of the companies that became involved in the market include internet and technology giants like Google, Microsoft, Yahoo, Cisco, and Skype. Other companies, like Skype, entered the Chinese market later. In 2002, Yahoo decided to sign on to a law that led to the later release of private information about users.[30] Many of the decisions made by United States companies upon entrance into the Chinese market have led to greater control of the medium by the Chinese

[25] Eric Harwit and Duncan Clark, "Government Policy and Political Control over China's Internet," in *Chinese Cyberspaces: Technological Changes and Political Effects*, Jens Damm and Simona Thomas, ed., (New York: Routlege, 2006), 16.
[26] Ibid, 16-17.
[27] Jack Linchaun Qiu, *Working-Class Network Society: Communications and the Information Have-Nots in Urban China,* (Cambridge, MA: The MIT Press, 2009), 33-34.
[28] Eric Harwit and Duncan Clark, "Government Policy and Political Control over China's Internet," in *Chinese Cyberspaces: Technological Changes and Political Effects*, Jens Damm and Simona Thomas, ed., (New York: Routlege, 2006), 16-17.
[29] Jack Linchaun Qiu, *Working-Class Network Society: Communications and the Information Have-Nots in Urban China,* (Cambridge, MA: The MIT Press, 2009), 71.
[30] Jonathan Mirsky, "US Companies are Abetting Internet Censorship in China," in *Censorship: Opposing Viewpoints,* ed. Scott Barbour, (Farmington Hills, MI: Greenhaven Press, 2010), 129.

government. These issues will be more fully discussed in Chapter 3, which will discuss the impact of multinational corporations on China's internet.

By 2003, there were no less than 10 networks in China.[31] By this time, the main player was ChinaNet.[32] Also, by this time, the MII had consolidated control over the network and had emerged as the major ministry for internet issues.[33] James Fallows notes that the physical infrastructure of the Chinese internet became set as a system that came with a series of "choke points."[34] (Fallows, 114-15) These "choke points," according to Fallows, included the presence of only three fiber optic entrances into the network in China, which existed in Beijing-Qingdao-Tianjin for the north region, Shanghai for the central region, and Guangzhou for the south region of the country.[35] Fallows notes the lack of entrances into the Chinese network, which makes it easier to physically monitor foreign information on the web.[36] Further, he notes that information in forced to China's censors through technology. Routers force the information to China's "Golden Shield" computers.[37] As such, one can see how the physical development of the internet infrastructure in China has aided the ability of the Chinese government to control the information presented on the network and engage in effective control of the system. Next, we will investigate the history of ISPs in the Chinese market, again looking for areas in which the Chinese government has instituted controls that could lead to the effective manipulation of the internet in China.

[31] Eric Harwit and Duncan Clark, "Government Policy and Political Control over China's Internet," in *Chinese Cyberspaces: Technological Changes and Political Effects*, Jens Damm and Simona Thomas, ed., (New York: Routlege, 2006), 16-17.
[32] Ibid.
[33] Ibid, 19.
[34] James Fallows, "China's Internet Censorship is Effective," in *Censorship: Opposing Viewpoints,* ed. Scott Barbour, (Farmington Hills, MI: Greenhaven Press, 2010), 114-15.
[35] Ibid, 115.
[36] Ibid.
[37] Ibid.

Part II: The History of Internet Service Providers in China

An overview of the history of internet service providers (ISPs) in China requires far less detail than a discussion of the physical network in the country. The reason for this is simple. The efforts put in place to control ISPs in China were simple and effective. Early ISPs in the country suffered losses from high fees and operating costs and low profits.[38] It is important to note that, early on, many of the ISPs were private or members of cooperatives and were outside of the purview of the MII. As such they were regulated by the State Council and top CCP officials.[39] However, by the early 2000s, with the consolidation of network control in China, ISPs were forced to engage in numerous actions that limited their ability to independent and objective providers of information to the Chinese populace. They were required to engage in actions that kept them directly identified by the Chinese government, which, when combined with the government's control of the physical networks in China, served to create an environment of self-censorship. This included the requirement that ISPs apply for licenses from the Chinese government and store all user data.[40]

The storage of user information and application for licenses, coupled with other aspects of Chinese internet control, leads to a system that regulates the promulgation of information on multiple levels. For one, it encourages nervous ISPs to remove content that would offend the government for fear of losing access to the market based on the loss of a license. Further, the storage of information may make it more likely that individual users and groups of users would be less likely to publish information that would be considered dangerous or offensive, given that

[38] Eric Harwit and Duncan Clark, "Government Policy and Political Control over China's Internet," in *Chinese Cyberspaces: Technological Changes and Political Effects*, Jens Damm and Simona Thomas, ed., (New York: Routlege, 2006), 21.
[39] Ibid, 24.
[40] Gudrun Wacker, "The Internet and Censorship in China," in *China and the Internet: Politics of the Digital Leap Forward,* ed. Christopher R. Hughes and Gudrun Wacker, (London: Routlege, 2003), 63-64.

there information is readily accessible, making them prime targets for arrest and other coercive measures delivered by the government. This makes up some of what has been referred to as China's engagement in self-censorship. This will be discussed further as we examine the history of internet usage and control in China in the next part of this chapter.

Part III: The History of Internet Control and Usage in China

Internet censorship is not a new phenomenon for the Chinese. From the late 1990s to 2001, there were 150,000 blocked sites. This included most major American newspapers.[41] However, in 2002, many of these restrictions regarding wholesale web blocking were removed. However, self-censorship and other efforts have remained.[42] Much of this early government crackdown was due to actions of Falun Gong in 1999.[43] Much of this crackdown, which was largely aimed at internet cafés in China, was seen as the government reasserting its control over communications.[44] Qiu notes that three directives were issued about internet cafés between 1998 and 2002.[45] Much of this was centered on the notion that internet cafes could no longer be an anonymous location for their users, considering that many of these internet cafes had used programs to hide the identity of those using their systems. Further, these restrictions required internet café cooperation with the government and put severe penalties on the table for non-

[41] Martin Woesler, "Internet Censorship Focus: Human Rights Not Found," in *China's Digital Divide: The Impact of the Internet on Chinese Society,* ed. Zhang Junhua and Martin Woesler, (Berlin: European University Press, 2004), 290.

[42] Ibid.

[43] Jack Linchaun Qiu, *Working-Class Network Society: Communications and the Information Have-Nots in Urban China,* (Cambridge, MA: The MIT Press, 2009), 33-34.

[44] Ibid.

[45] Ibid, 35.

compliance.[46] However, regardless of the fact that restrictions on foreign news outlets were eased in 2002, China still maintained control over the information that was put onto the internet.

In the early 2000s, the government still maintained a hefty list of content that was forbidden on the internet. A complete list of forbidden content guidelines from the early 2000s is shown below in Table 1.[47]

Table 4. Content Forbidden by the Chinese Government

1. Contradicts PRC principles defined in the Constitution
2. Endangers national security, discloses state secrets, subverts the government, destroys the unity of the state
3. Damages state honor and interests
4. Instigates ethnic hatred or discrimination, destroys the unity of Chinese nationalities
5. Negative effects on state policies on religion; propagates evil cults or feudal religions
6. Disseminates rumors, disturbs social order, undermines social stability
7. Lewdness, pornography, gambling, violence, murder, terror, or instigates crime
8. Offends or defames others, infringes on the rights and intents of others
9. Other content forbidden by law or administrative regulation.

It is important to remember in the discussion of the internet in China that, in the words of Lawrence Lessig, effective control of the internet may be possible even in the absence of

[46] Jack Linchaun Qiu, *Working-Class Network Society: Communications and the Information Have-Nots in Urban China,* (Cambridge, MA: The MIT Press, 2009), 35.

[47] List taken from Gudrun Wacker, "The Internet and Censorship in China," in *China and the Internet: Politics of the Digital Leap Forward,* ed. Christopher R. Hughes and Gudrun Wacker, (London: Routlege, 2003), 62.

complete control.[48] Indeed, it is important to not write off the ability of the state to control the internet.[49] Much of the Chinese government's control of the internet comes from trials of those who have violated their laws regarding content. One of the earliest cases of a crime against the state concerning the internet was Huang Qi, who posted info on the Tiananmen victims in the early 2000s.[50] Huang Qi went on trial for "subverting state power" in 2001 although, because his site was based outside of China, it continued to report on his trial until 2003.[51] Eric Harwit and Duncan Clark refer to the tactics used in the case Huang Qi as "killing the chicken to scare the monkeys."[52] In other words, China's trials regarding dissidents and their online postings served to show others that they indeed could find them and arrest them. Thus, these actions add credence to the actions of the government in regulating and licensing both ISPs and internet cafes.

Government control of foreign websites, according to Harwit and Clark, has been erratic, something that can be seen from the government's inability to shut down Huang Qi's site while he was on trial and their 2002 change in tactics, when they stopped blocking many Western newspapers.[53] Also, several sites existed that allowed a user to skirt the restrictions on foreign sites. Sites such as Rewebber and the various proxy servers aided users in protecting their identity while searching controversial content.[54] As such, control was far more likely to be

[48] Gudrun Wacker, "The Internet and Censorship in China," in *China and the Internet: Politics of the Digital Leap Forward,* ed. Christopher R. Hughes and Gudrun Wacker, (London: Routlege, 2003), 60.
[49] Ibid, 61.
[50] Eric Harwit and Duncan Clark, "Government Policy and Political Control over China's Internet," in *Chinese Cyberspaces: Technological Changes and Political Effects*, Jens Damm and Simona Thomas, ed., (New York: Routlege, 2006), 25.
[51] Ibid.
[52] Ibid.
[53] Ibid, 27.
[54] Ibid, 27-28.

exercised on the domestic user end.[55] As early as 1996, users were forced to register with the government to open an account with an ISP.[56] In short, based on the exponential growth of the foreign internet and the inability of any government to control the entire flow of information on the internet, Chinese users have actually seemed to have had an easier time accessing foreign controversial information that controversial information that originates in China.

However, simply because much of the controversial information that exists on the internet is from foreign servers does not mean that information on Chinese servers is always benign. Some chat rooms in China have expressed frustration with the government. Such information has included debates regarding the NATO bombing of the Chinese embassy in Belgrade in the 1990s and other hot topics in Chinese politics. Sometimes, these debates would even influence Chinese policy.[57] Also, even more controversial information has been spread via e-mail in the country.[58] It is important to remember that the control of the Chinese network is not the same as the control of the content on the Chinese network.[59]

Given that the Chinese government could not completely control all of the content on the internet, the government has also engaged in other actions to limit the effectiveness of dissident movements in the country. Much of this has come in the form of greater transparency by the government through the use of the internet. Government online was released in 1999.[60] This allowed the Chinese government to provide services to the public through the use of the internet,

[55] Eric Harwit and Duncan Clark, "Government Policy and Political Control over China's Internet," in *Chinese Cyberspaces: Technological Changes and Political Effects*, Jens Damm and Simona Thomas, ed., (New York: Routlege, 2006), 27.
[56] Ibid.
[57] Ibid, 34.
[58] Ibid.
[59] Ibid, 36.
[60] Gudrun Wacker, "The Internet and Censorship in China," in *China and the Internet: Politics of the Digital Leap Forward,* ed. Christopher R. Hughes and Gudrun Wacker, (London: Routlege, 2003), 58.

furthering Chinese efforts at a propaganda message that showed the Chinese government as modern and benevolent regarding its usage of the internet. Further, the Chinese government also began working with businesses regarding the regulations of the internet. This is largely explained by the vast importance of business to the internet in China. By 2002, .com addresses were the most common addresses in China.[61] According to Gudrun Wacker, this has caused many to doubt the democratizing effects of the internet in China, given the vast commercialization of the medium.[62] Such thoughts have been reinforced given the fact that many of the early internet content providers were supported by the Chinese government, thus making them more reluctant to engage in controversial behavior and more apt to support self-censorship methods.[63] Wacker even talks about an "authoritarian-capitalist coalition," in which internet providers have gone so far as to come to the government with drafted regulations that are not even in force.[64]

China has managed for many years to walk a technological tight rope when it comes to internet censorship and control. Now, as James Fallows puts it, "China is frequently cited as one of the most censorious countries in the world."[65] Further, he notes that the Western conception of the "Great Firewall" is only part of a larger and more complex system of censorship.[66] He notes that there are technical ways to get around the censorship system in China, namely through the use of a virtual private network (VPN) or a proxy server, which initiates a second, hidden path to

[61] See figure 2.2 in Eric Harwit and Duncan Clark, "Government Policy and Political Control over China's Internet," in *Chinese Cyberspaces: Technological Changes and Political Effects*, Jens Damm and Simona Thomas, ed., (New York: Routlege, 2006), 23.

[62] Gudrun Wacker, "The Internet and Censorship in China," in *China and the Internet: Politics of the Digital Leap Forward,* ed. Christopher R. Hughes and Gudrun Wacker, (London: Routlege, 2003), 59.

[63] Eric Harwit and Duncan Clark, "Government Policy and Political Control over China's Internet," in *Chinese Cyberspaces: Technological Changes and Political Effects*, Jens Damm and Simona Thomas, ed., (New York: Routlege, 2006), 26.

[64] Gudrun Wacker, "The Internet and Censorship in China," in *China and the Internet: Politics of the Digital Leap Forward,* ed. Christopher R. Hughes and Gudrun Wacker, (London: Routlege, 2003), 68-69.

[65] James Fallows, "China's Internet Censorship is Effective," in *Censorship: Opposing Viewpoints,* ed. Scott Barbour, (Farmington Hills, MI: Greenhaven Press, 2010), 113.

[66] Ibid, 114.

a blocked website. This is because, if the Chinese government cracked down completely on the internet, they would harm business.[67] As such, we begin to see some of the nuance of the Chinese censorship regime. Qiu notes that labor rights are often limited under the censorship regime but only for those who are considered the "Have-nots" or the "Have-less." Further, he argues that this seems to follow the rural/urban and urban/migrant divides present in Chinese society, with urban elites enjoying greater access to information on the internet.[68]

It is important to remember regarding Chinese efforts to control the internet that they are not looking to completely control the entire network. Instead, China wants the search to be just difficult enough to make a user quit, something Fallows refers to as a mental firewall and is more commonly called self censorship.[69] This is not to say that the Chinese do not make vast efforts to regulate online content. Fallows notes that blogs can only be read if they are based in China and that teams of censors delete offending content.[70] Yet, despite this vigorous effort at censorship, blogs still pose a problem for the Chinese government.[71] April Gu notes that Wang Keqin posted an entire censored news story to a blog in 2007 an that Gao Yao Jie blogged about his house arrest.[72] Even Fallows notes that there is room for discussion.[73] The Chinese government seems to be installing a bend-don't-break mentality regarding the presence of controversial information through blogging. They have accomplished this through the intermittent blocking of MSN

[67] James Fallows, "China's Internet Censorship is Effective," in *Censorship: Opposing Viewpoints,* ed. Scott Barbour, (Farmington Hills, MI: Greenhaven Press, 2010), 116-17.

[68] Jack Linchaun Qiu, *Working-Class Network Society: Communications and the Information Have-Nots in Urban China,* (Cambridge, MA: The MIT Press, 2009), 122.

[69] James Fallows, "China's Internet Censorship is Effective," in *Censorship: Opposing Viewpoints,* ed. Scott Barbour, (Farmington Hills, MI: Greenhaven Press, 2010), 118.

[70] Ibid, 119.

[71] April Gu, "China's Internet Censorship can be Circumvented," in *Censorship: Opposing Viewpoints,* ed. Scott Barbour, (Farmington Hills, MI: Greenhaven Press, 2010), 126.

[72] Ibid, 123.

[73] James Fallows, "China's Internet Censorship is Effective," in *Censorship: Opposing Viewpoints,* ed. Scott Barbour, (Farmington Hills, MI: Greenhaven Press, 2010), 121.

Spaces and other blogging platforms and a reliance on self-censorship.[74] Yet, it is also possible that the blocking instigated by the Chinese government, which must, at times, seem random in nature, is akin to Fallows's discussion of a mental firewall, a system in which the Chinese government keeps users confused to the point of keeping them for searching for information of a controversial nature. Perhaps Yuezhi Zhao puts it best when he says, "The party (CCP) now aims for effective domination rather than total control of media messages."[75] This is further discussed by Zhao in his noting that the Chinese have "given up" on political indoctrination[76] and that they now are focusing on "passive censorship" in which oppositional ideas are neglected and driven to a small elite circle.[77] Such ideas mesh well with Qiu's contention that urban elites tend to have greater access to the internet in China.[68] Zhao, who focuses on the overall communications strategy of the Chinese government, notes that different types of media receive different levels of control. TV, according to Zhao, receives the highest levels of control, given that it receives the highest numbers of viewers. This is followed by print sources and then the internet, which has the smallest viewing base in China.[78] Zhao especially notes that elite websites have received an "expanded space under more refined control."[79]

China has installed a nuanced and evolving system of censorship and control over the internet. In 2009, China proposed the idea of putting software, known as Green Dam, on all the computers in China. However, after a massive international outcry, the Chinese backed off of

[74] April Gu, "China's Internet Censorship can be Circumvented," in *Censorship: Opposing Viewpoints,* ed. Scott Barbour, (Farmington Hills, MI: Greenhaven Press, 2010), 125.
[75] Yuezhi Zhao, *Communication in China: Political Economy, Power, and Conflict*, (Lanham, MD: Rowan & Littlefield Publishers, 2008), 35.
[76] Ibid.
[77] Ibid, 34.
[78] Ibid, 36.
[79] Ibid.

such a requirement, instead making the software optional.[80] In short, the goal of the Chinese information control systems with regard to the internet is not only to block information but to create an effective political narrative. Clay Shirky puts this well when he says:

> "The Chinese system has evolved from a relatively simple filter of incoming Internet traffic in the mid-1990s to a sophisticated operation that not only limits outside information but also uses arguments about nationalism and public morals to encourage operators of Chinese Web services to censor their users and users to censor themselves. Because its goal is to prevent information from having politically synchronizing effects, the state does not need to censor the Internet comprehensively; rather, it just needs to minimize access to information."[81]

This is the history and evolution of the Chinese censorship regime. It has left wholesale blocking, as evidenced by its moves regarding Western newspapers in 2002 and the presence of controversial information on the Chinese internet. Instead, they have engaged in a campaign to control information, leaving the Chinese citizen at odds with not only a censorship regime, but also with a propaganda apparatus that is pushing the Chinese view of the world. As such, we can begin to see the Chinese reliance on tactics that would be more appropriate in a cyberconflict or cyberwarfare setting, something we will go into more detail about in the next section. While it appears that Chinese blocking of the internet is a relatively small portion of the overall Chinese communications strategy, one has to question whether or not this will change as more and more Chinese citizens enter into the internet. Thus, we can see the problem of development that faces the Chinese government. As they gain the technological and economic development they desire, they open the door for ever larger numbers of users to engage in the internet, which could well force them to either increase their censorship measures, something that has been noted as potentially harmful to business in the country, or liberalize their policies. Only time will tell if

[80] Ronald Deibert, "China's Cyberspace Control Strategy: An Overview and Consideration of Issues for Canadian Policy," *Canadian International Council China Papers* 7 (2010): 4.
[81] Clay Shirky, "The Political Power of Social Media," *Foreign Affairs* 90, 1 (2011): 28-41.

the internet is truly able to be a foothold for communications and dissent in China. However, history shows a regime that has been effective in managing, maintaining, and controlling a status quo that is in their favor.

Part IV: The History of Cyberconflict and Cyberwarfare in Chinese Policy

Information warfare has, by some, been traced back to the Chinese strategist Sun Zi, who suggested "deception, knowing the enemy and gathering intelligence" to fight wars.[82] In more modern Chinese history, Deng Xiaoping developed the idea of the "smokeless war" in which the infiltration of American values and culture in China undermined socialism through peaceful evolution.[83] Further, China was worried that technologically advanced states could take advantage of China through these means, something Christopher Hughes refers to as "virtual realism."[84] Many authors note that China has appropriated Western knowledge directly for cyberconflict.[85] Ronald Deibert brings up GhostNet, a secret espionage program which infiltrated 1,295 computers in 103 countries.[86] GhostNet, according to the Information Warfare Monitor, was shown by "documented evidence" to be a cyber espionage network, infecting at least 1,295 computers in 103 countries, "of which close to 30% can be considered as high-value diplomatic,

[82] Christopher Hughes, "Fighting the Smokeless War: ICTs and International Security," in LSE Research Online, http://eprints.lse.ac.uk/9641/, 215. Note: This same piece was published in *China and the Internet: Politics of the Digital Leap Forward, ed. Christopher R. Hughes and Gudrun Wacker, (London: Routlege, 2003),* 139-161. However, this piece has some differences from the final version that was published in the book. As such, this paper uses both this piece and the one published in the book. Further references will denote whether or not the piece comes from the book.

[83] Christopher Hughes, "Fighting the Smokeless War: ICTs and International Security," *China and the Internet: Politics of the Digital Leap Forward,* ed. Christopher R. Hughes and Gudrun Wacker, (London: Routlege, 2003), 141.

[84] Christopher Hughes, "Fighting the Smokeless War: ICTs and International Security," in LSE Research Online, http://eprints.lse.ac.uk/9641/, 218.

[85] For examples of this discussion, see Christopher Hughes, "Fighting the Smokeless War: ICTs and International Security," *China and the Internet: Politics of the Digital Leap Forward,* ed. Christopher R. Hughes and Gudrun Wacker, (London: Routlege, 2003), 150, or Ronald Deibert, "China's Cyberspace Control Strategy: An Overview and Consideration of Issues for Canadian Policy," *Canadian International Council China Papers* 7 (2010)*:* 5.

[86] Ronald Deibert, "China's Cyberspace Control Strategy: An Overview and Consideration of Issues for Canadian Policy," *Canadian International Council China Papers* 7 (2010)*:* 5.

political, economic, and military targets." [87] This included the private offices of the Dalai Lama and other Tibetan targets.[88] Further, the study into GhostNet, called it "a covert, difficult-to-detect and elaborate cyber-espionage system capable of taking full control of affected systems."[89] Royce Priem, the Director of Information Technology for the International Campaign for Tibet, an organization that was targeted by GhostNet, notes that the full effect of the attack is yet to be known, especially given the nature of the program to bury into systems. Priem mentioned that, when he came on board at the International Campaign for Tibet, the systems were already compromised, making it difficult to tell the impact of a singular attack.[90]

While it is difficult to pinpoint the Chinese as the source of the GhostNet cyber espionage program (However, the report on GhostNet acknowledges that, even if the Chinese government was not directly behind the attacks, they probably viewed those who were as effective and useful extensions of the country's power.[91]), certain clues indicate that the Chinese government may have directly been behind the attack. As Ronald Deibert notes, many of the signals came from a known People's Liberation Army base:

> "Many of the target computers were based inside high value political and economic targets of strategic significance to China's defense and foreign policy, such as diplomatic ministries and organizations related to Taiwan, Hong Kong, Tibet, Pakistan and others. The Indian Embassy in Washington, DC was thoroughly infected by GhostNet. The system enabled the attackers to take complete control of infected computers, including access to all files, remote desktop viewing, keystroke logging and audio and video controls. Some of the IPs used in the attack were traced

[87] Information Warfare Monitor, "Tracking GhostNet: Investigating a Cyber Espionage Network," Information Warfare Monitor (2009): 6.
[88] Ibid.
[89] Ibid.
[90] Royce Priem, Interview by Joseph House, Washington, DC, 9 March 2011.
[91] Information Warfare Monitor, "Tracking GhostNet: Investigating a Cyber Espionage Network," Information Warfare Monitor (2009): 12.

> back to Hainan Island, home of the People's Liberation Army's Signals Intelligence Facility."[92]

Further, some other stories indicate a more direct role by the government. According to the report on GhostNet:

> "During the course of our research, we were informed of the following incident. A member of Drewla, a young woman, decided to return to her family village in Tibet after working for two years for Drewla. She was arrested at the Nepalese-Tibetan border and taken to a detention facility, where she was held incommunicado for two months. She was interrogated by Chinese intelligence personnel about her employment in Dharamsala. She denied having been politically active and insisted that she had gone to Dharamsala for studies. In response to this, the intelligence officers pulled out a dossier on her activities and presented her with full transcripts of her Internet chats over the years. They indicated that they were fully aware of, and were monitoring, the Drewla outreach initiative and that her colleagues were not welcome to return to Tibet. They then released her and she returned to her village."[93]

It is important to note that it is still impossible to fully determine who is controlling GhostNet.

The report on the topic notes this, saying:

> "Who is ultimately in control of the *GhostNet* system? While our analysis reveals that numerous politically sensitive and high-value computer systems were compromised, we do not know the motivation or the identity of the attacker(s) or how to accurately characterize this network of infections as a whole. We have not been able to ascertain the type of data that has been obtained by the attacker(s), apart from the basic system information and file listings of the documents located on the target computers. Without this data we are unable to deduce with any certainty what kind of data the attacker(s) were after. There are thus several possibilities for attribution."[94]

The report notes that circumstantial evidence points to the Chinese government. However, it also concedes that it could be a group or individual with no political agenda and high level

[92] Ronald Deibert, "China's Cyberspace Control Strategy: An Overview and Consideration of Issues for Canadian Policy," *Canadian International Council China Papers* 7 (2010)*:* 5.

[93] Information Warfare Monitor, "Tracking GhostNet: Investigating a Cyber Espionage Network," Information Warfare Monitor (2009): 28.

[94] Information Warfare Monitor, "Tracking GhostNet: Investigating a Cyber Espionage Network," Information Warfare Monitor (2009): 48.

targets just happened to be included.[95] They noted that this could be an individual or group targeting these systems for profit or it could even have been another country using Chinese (and, in one instance, US) servers for the attacks.[96] However, given this circumstantial evidence and the fact that the Chinese opened their first public cyber operations base in 2010[97], we can see the history of cyberwarfare and cyberconflict in Chinese communications control strategies. Regardless of whether or not the Chinese were responsible for the GhostNet attack, the Chinese have certainly shown an affinity for cyberwarfare activities and have certainly framed the discussion of the internet in a security context. We will address this viewpoint in Chapter 5 and Chapter 6, which will touch on cyberterrorism and China's security justifications for its internet censorship regime.

Conclusion

China has continually expanded its physical infrastructure and has implemented numerous methods of both direct and indirect control on that infrastructure. China has evolved its censorship and regulation structures over the years from basic filtering to a structure which controls the system in a general sense and prevents information from becoming politically damaging. This is done both through the blocking of information and the discrediting of information through propaganda and other measures. Further, the government has become more reliant on self-censorship to accomplish its goals. Also, the Chinese government has placed most ISPs in a precarious position, with demands for licensing and acquiescence to Chinese laws regarding content control. The Chinese have also shown an increased interest in offensive

[95] Information Warfare Monitor, "Tracking GhostNet: Investigating a Cyber Espionage Network," Information Warfare Monitor (2009): 48.
[96] Ibid.
[97] "PLA sets up cyber base, assures it's not for war," *The Times of India*, July 23, 2010. Also see Russell Hisao, "China's Cyber Command?" *China Brief* 10, 15 (July 22, 2010). The story was originally published in the People's Liberation Army (PLA Daily).

cyberwar capabilities. These capabilities could be potentially dangerous (and may have already been) for both foreign governments and dissident groups within the country. These systems would serve as a nice addition to China's control structures, further illustrating how China's internet control measures are not merely based on internet censorship. As such, any discussion of this topic that solely focuses on internet censorship in China, without talking about other efforts of the government to control the narrative of political and sensitive information on the internet is flawed. In short, China's efforts regarding the internet are not merely a matter of blocking the internet. Instead, their efforts indicate a concerted effort to control, and not merely, deny information.

Chapter 3: The Internet and Multinational Corporations in China

The last chapter discussed the history of the internet in China, including the infrastructure, ISPs, censorship efforts, and cyberwarfare and cyberconflict aspects. The chapter also touched quickly on the issue of multinational corporations (MNCs) in China and their impact on the censorship regime. It is important to note that the MNCs within China are service organizations that rely on advertising for revenue, given Chinese regulations on ownership within the technology sector. Even still, many of these companies must maintain a Chinese partner at some level. This chapter will go into more detail on the history of MNCs in the Chinese internet market. In specific, it will touch on the actions of two companies, Yahoo! and Google. In touching on Yahoo!, it will discuss issues of the confidentiality of personal information, specifically information on the identity of users. In discussing Google, the questions touched on will be those related to issues of censorship. Yahoo! and Google will be presented as case studies and conclusions will be presented at the end given the specific details surrounding each company. This chapter will, in short, examine the debate between whether or not these companies should consistently obey all local laws or whether they should not compromise, based on principle. It is unwise to assume that these relationships only lead to more internet censorship or information control. Indeed, in certain instances, these relationships have shown conflict between the two sides, similar to the conflict exposed in 2010, when Google stopped censoring its search results in the aftermath of a string of Chinese hacking incidents.

In the early 2000s, US companies entered the Chinese internet market. Many of these have helped with what Jonathan Mirsky called the “biggest state censorship campaign ever.”[98]

[98] Jonathan Mirsky, “US Companies are Abetting Internet Censorship in China,” in *Censorship: Opposing Viewpoints,* ed. Scott Barbour (Farmington Hills, MI: Greenhaven Press, 2010), 129.

Companies involved in the market included Google, Microsoft, Yahoo!, Cisco, Sun, and Skype (which entered the market later in the 2000s).[99] Surya Deva singles out four companies as major players in the Chinese market - Google, Yahoo!, Microsoft, and Cisco.[100] Of these four companies, this chapter will focus on Yahoo! and Google. The reasons for this are simple enough. First, Yahoo! serves as an excellent example of issues of user confidentiality, while Google serves as a great example of censorship issues. Second, the two companies show vastly different relationships with the Chinese government. Google shows a more tenuous relationship, arguing in 2010 to stop censoring their internet search results after discovering a string of cyber attacks that they blamed on the Chinese government. Yahoo! shows a relationship that is more homogenous, given their partnership with Alibaba for in-China activities (especially given their lack of control over Alibaba's actions in China because they have kept themselves out of the majority of their own company in China).

MNC involvement in China was described as follows by Representative Christopher Smith of New Jersey:

> "U.S. technology companies today are engaged in a similar sickening collaboration, decapitating the voice of the dissidents. In 2005, Yahoo!'s cooperation with Chinese secret police led to the imprisonment of cyber-dissident Shi Tao. And this was not the first time. According to Reporters Without Borders, Yahoo! also handed over data to Chinese authorities on another of its users, Li Zhi. Li Zhi was sentenced on December 10, 2003, to 8 years in prison for inciting subversion. His ''crime'' was criticizing in online discussion groups and articles the well-known corruption of local officials."[101]

[99] Jonathan Mirsky, "US Companies are Abetting Internet Censorship in China," in *Censorship: Opposing Viewpoints,* ed. Scott Barbour (Farmington Hills, MI: Greenhaven Press, 2010), 129.

[100] Surya Deva, "Corporate Complicity in Internet Censorship in China: Who Cares for the Global Compact or the Global Online Freedom Act?" *George Washington Law Review* 39, 2 (2007): 257.

[101] Congress, House of Representatives, Committee on International Relations, "The Internet in China: A Tool for Freedom or Suppression?" 109th Congress, 2nd Session, 15 February 2006, 2.

Smith further compared the actions these companies in China to the strategic alliance that IBM held with the Nazis up until WWII.[102] Smith also said:

> "Yet for the sake of market share and profits, leading U.S. companies, like Google, Yahoo!, Cisco, and Microsoft, have compromised both the integrity of their product and their duties as responsible corporate citizens. They have, indeed, aided and abetted the Chinese regime to prop up both of these pillars, secret police and propaganda, propagating the message of the dictatorship unabated and supporting the secret police in a myriad of ways, including surveillance and invasion of privacy, in order to effectuate the massive crackdown on its citizens."[103]

In the hearing, Smith notes the censorship inherent in Google.cn.[104] It is important to realize that the relationship of Google and the Chinese government has changed sharply from the time of this hearing. Yet, it is also important to note that Google entered the Chinese market knowing the restrictions of the Chinese government. Yet, regardless of these restrictions, Google still began doing business in the Chinese market, something that, regardless of the changes in this relationship, is important. The relationship of Google and China will delved into in depth as this chapter continues. This chapter will also delve into other corporate relations with the Chinese government, many of which have led to issues for dissidents throughout the country.

Part I: Yahoo! and the Chinese Government

Yahoo has been one of the most controversial companies in China. Much of this stems from cases such as the Shi Tao case. According to Representative Tom Lantos:

> "On the eve of the 15th anniversary of the Tiananmen Square massacre 3 years ago, the Chinese Government issued the directive forbidding journalists from covering anything related to this anniversary.
>
> In a brief second that would have a momentous impact on the rest of his life, Shi Tao

[102] Congress, House of Representatives, Committee on International Relations, "The Internet in China: A Tool for Freedom or Suppression?" 109th Congress, 2nd Session, 15 February 2006, 2.
[103] Ibid.
[104] Ibid, 3.

> hit the Forward button on his the Yahoo! e-mail account and sent the government's message to an NGO overseas advocating for democratic change in China.
>
> When the Chinese Government set out to unlock the mystery of who had publicly disclosed this document, they went to the offices of Yahoo! China to provide the key."[105]

Lantos continued:

> "The flagship American company… complied with the request from the Chinese political suppression apparatus and provided the necessary identifying information to track down Shi Tao."[106]

Yahoo's defense regarding the Shi Tao case was that the company's China operations were merged with Chinese company Alibaba in the mid 2000s and that the American company no longer has day to day operational control over the Chinese company. However, they did say that they expressed concern to Alibaba.[107] This relationship with Alibaba underscores a far more cozy relationship with the Chinese government than the relationship had by many other companies. Google, which is discussed below, entered into the Chinese market later and does not have such relations with any Chinese company.[109] The case of Yahoo! and Shi Tao led to calls for a stronger regulatory framework on MNCs dealing with the internet in China. This included the proposal of the Global Online Freedom Act in 2006. The Global Online Freedom Act will be discussed as part of the proposed regulatory framework on MNCs in the conclusion of this chapter. As such, Lantos's comments were made at a hearing indicating that Yahoo! had provided false information to Congress. Lantos notes:

[105] Congress, House of Representatives, Committee on Foreign Affairs, "Yahoo! Inc.'s Provision of False Information to Congress," 110th Congress, 1st Session, 6 November 2007, 1.

[106] Ibid.

[107] Congress, House of Representatives, Committee on International Relations, "The Internet in China: A Tool for Freedom or Suppression?" 109th Congress, 2nd Session, 15 February 2006, 56-57.

> "In an effort to convince this committee that Yahoo! was not a knowing agent of the Chinese Government repression, Mr. Callahan testified that Yahoo! had no knowledge of the facts surrounding the Shi Tao case at the time the company provided information to the Chinese authorities. Let me quote from what Mr. Callahan said:
>
>> "'When Yahoo! China in Beijing was prepared to provide information about the user who we later learned was Shi Tao, we had no information about the nature of the investigation. Indeed, we were unaware of the particular facts surrounding the case until the news story emerged.'"[108]

Part II: Google and the Chinese Government

Google set up Google.cn in 2006.[109] The company, which has tended to boast an ethical record counter to that of the Chinese internet censorship regime, has had a tenuous relationship with the Chinese government. According to Jonathan Watts:

> "Since then it has been typically creative in trying to find solutions to the problems it faced in China. Recognizing the ethical wrong of censorship, it insisted on telling users that their search terms had been filtered. To avoid having to hand over emails to police, it did not set up a gmail service in China. Recognizing that rampant music piracy was a competitive advantage for its main rival, Baidu, it bought up the rights of tens of thousands of songs and offered them free to Chinese users. That the authorities let them not only do, but announce, these things suggests there was a degree of flexibility on both sides."[110]

Over time, however, Google made only relatively pedestrian profits and censorship increased in China. According to Watts, 2009 was a particularly bad year, with the blocking of Twitter, Facebook, and other sites. Google also experienced service disruptions and restrictions on their applications. The state even criticized the company for "promoting pornography." When this combined with the increased hacking, according to Watts, it certainly seemed like a series of

[108] Congress, House of Representatives, Committee on Foreign Affairs, "Yahoo! Inc.'s Provision of False Information to Congress," 110th Congress, 1st Session, 6 November 2007,.

[109] Jonathan Watts, "How Internet Giant Google Turned on Gatekeepers of China's Great Firewall," *The Guardian,* 14 January 2010.

[110] Ibid.

trends in the wrong direction.[111] In January 2010 and again in March 2010, Google released blog posts regarding these issues. In these posts, Google claimed to have been targeted by cyber attacks which had the primary goal of gathering information on human rights activists.[112] As a result, Google decided to review its business operations in China.[113] In March 2010, they started rerouting their search engines through Google.com.hk – which is uncensored.[114] As of March 2011, the google.cn page still has a link to Google.com.hk.[115]Blocking of the site appears incomplete and sporadic. China blocked a question page for the site in August 2010, but seems to have refused to block the site outright.[116] This dispute sparked global outcry. Hillary Clinton made a speech on the subject in which, as Evgeny Morozov noted, she worked in a lot of Cold War rhetoric.[117] According to Morozov, the language that was used by Clinton represents "an anachronistic view of authoritarianism."[118] The sixth chapter will more fully discuss the issue of whether or not the internet can be a democratizing force and the policy goals of Western liberal nations. However, what is important in this particular instance is the large outcry regarding this one case and the reliance on Cold War rhetoric by high level United States officials.

In truth, the eventual resolution to this dilemma was surprising. Morozov, in January 2010, said:

[111] Jonathan Watts, "How Internet Giant Google Turned on Gatekeepers of China's Great Firewall," *The Guardian,* 14 January 2010.

[112] "A New Approach to China," (12 January 2010), *The Official Google Blog,* *http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.*

[113] Ibid.

[114] "A New Approach to China – An Update," (22 March 2010), *The Official Google Blog,* *http://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html.*

[115] This is based on the author's own observation of the Google Chinese search engine. It is important to note that a link of this nature could easily be blocked. Also, Google.cn could be blocked as well. Further, since Hong Kong is related to the People's Republic of China, the Chinese government could potentially censor those results as well, if it felt so inclined.

[116] "Google's Hong Kong Question Page Blocked in China," *Reuters*, 3 August 2010: http://www.reuters.com/article/2010/08/03/us-google-china-idUSTRE6720HN20100803.

[117] Evgeny Morozov (21 January 2010), "Is Hillary Clinton Launching a Cyber Cold War?" *Foreign Policy*, 21 January 2010: http://neteffect.foreignpolicy.com/posts/2010/01/21/cyber_cold_war.

[118] Ibid.

> "By pulling out of China — a prospect that now looks inevitable, as Chinese authorities are not likely to change their laws to acquiesce a foreign company — Google would not make itself any safer from future cyberattacks."[119]

Yet, Google did not end up pulling out of China and (admittedly) is still in danger of cyberattacks. Cyberattacks were probably never the entire reasoning for Google's actions. Indeed, they were probably a small part of the discussion, which, mixed with Google's low market share and the continued censorship and antics on behalf of the Chinese government, made for a situation in which Google felt it could push a harder line with the Chinese government. However, it is an open question as to whether or not Google is in a better situation, given that it is still operating in China and is only routing through a Hong Kong server, which has only marginally less control from the Chinese government. It is a good possibility that, if searches were rerouted to Google.com, that this situation would be playing out differently. At the bare minimum, in such a situation, the Google.com link on the Google.cn page would be blocked from the Chinese net surfer.

Part III: Other Corporate Entities in China that Have Had an Impact

Other companies have had an impact in the relations between the Chinese government and dissidents within the country. Dr. Eric Novotny points out that Narus, an American company, has worked extensively with the Chinese government. Narus has developed software that, according to Novotny, helps governments track dissidents. This is also pointed out by Timothy Karr in his article for The Huffington Post.[120] Narus even discusses its work in China on its own website.[121] The presence of companies like Narus further complicates the relations of the United States and China regarding the internet. This is because Narus is actually staffed by

[119] Evgeny Morozov, "Try Different Keywords," *The New York Times*, 16 January 2010.
[120] Timothy Karr, "One U.S. Corporation's Role in Egypt's Brutal Crackdown," *The Huffington Post*, 29 January 2011.
[121] "Government – Intelligence," Narus, http://www.narus.com/index.php/industries/government-intelligence.

former NSA members.[122] This makes the US position of this topic tough to defend, given the hypocrisy inherent in an overly moralistic tone, given the presence of former government officials in a company that is helping the Chinese government.

The Lacking Nature of Policy Prescriptions

China is still a vast market, with 384 million internet users in 2010.[123] As such, it is likely MNCs will not leave the country. Until US and other governments put some restrictions on the actions of MNCs in foreign countries with regards to internet censorship and privacy, there will likely be little change in the uneven policy exhibited by MNCs. However, much of the legislation or actions lack enforcement mechanisms or political will to be able to get passed. As such, we can continue to expect long term uneven policy regarding MNCs in China and the internet.

The Global Compact

One of the bodies put in place to control the behavior of multinational corporations is the Global Compact. The Global Compact is "…the world's largest and most embraced corporate citizenship imitative."[124] Further, it is described as "a multi-stakeholder initiative involving diverse actors such as governments, companies, labor and civil society organizations, and the United Nations."[125] Deva notes that it was originally 9 principles and that, in 2004, an anti-corruption principle was added.[126] These principles, according to Surya Deva, were derived from

[122] Dr. Eric Novotny, interview with Joseph House, Washington, DC, 11 February 2011.

[123] "China Internet Population Hits 384 Million," *Reuters*, 15 January 2010.

[124] Quote taken from Surya Deva, "Corporate Complicity in Internet Censorship in China: Who Cares for the Global Compact or the Global Online Freedom Act?" *George Washington Law Review* 39, 2 (2007): 291.

[125] Ibid.

[126] Ibid.

Universal Declaration of Human Rights.[127] A full enumeration of the principles of the Global Compact can be found in Table 2, below.[128]

Table 2. The Principles of the Global Compact

Principle 1: Businesses should support and respect the protection of internationally proclaimed human rights; and

Principle 2: make sure that they are not complicit in human rights abuses.

Principle 3: Businesses should uphold the freedom of association and the effective recognition of the right to collective bargaining;

Principle 4: the elimination of all forms of forced and compulsory labour;

Principle 5: the effective abolition of child labour; and

Principle 6: the elimination of discrimination in respect of employment and occupation.

Principle 7: Businesses should support a precautionary approach to environmental challenges;

Principle 8: undertake initiatives to promote greater environmental responsibility; and

Principle 9: encourage the development and diffusion of environmentally friendly technologies.

Principle 10: Businesses should work against corruption in all its forms, including extortion and bribery.

The goals of the Global Compact, as stated by Deva, are to internalize its principles as business strategy and facilitate "cooperation and collective problem solving" between the actors under it.[129] However, the Global Compact is not regulatory in nature.[130] Instead, it tends to rely on unconventional means and actors that are "enlightened" to achieve the goals it has set out.[131]

[127] Surya Deva, "Corporate Complicity in Internet Censorship in China: Who Cares for the Global Compact or the Global Online Freedom Act?" *George Washington Law Review* 39, 2 (2007): 291-92.

[128] "The 10 Principles," *The United Nations Global Compact,* *http://www.unglobalcompact.org/AboutTheGC/TheTenPrinciples/index.html*.

[129] "Surya Deva, "Corporate Complicity in Internet Censorship in China: Who Cares for the Global Compact or the Global Online Freedom Act?" *George Washington Law Review* 39, 2 (2007): 292.

[130] Ibid, 293.

[131] Ibid.

This is a huge problem. The lack of enforcement makes profit more powerful than principle. As such, so long as unethical actions are not damaging to company's bottom line, they will continue.

The Global Online Freedom Act

Another option on the global regulatory front is the Global Online Freedom Act. However, The Global Online Freedom Act (Deva 309 – 317) has yet to be passed. The act was originally proposed in 2006. The act definitely shows more of a regulatory nature, imposing heavy guidelines and restrictions on companies. However, as it has not passed in five full years of being proposed, it appears to be dead in the water and thus, ineffective. Unless there is a drastic change in political will, something that might have been expected in 2010, given the actions between China and Google, it is highly unlikely that the Global Online Freedom Act will ever amount to much of a solution to the problems posed by the Chinese internet censorship regime and its relations with MNCs.

Conclusion

The presence of a large number of MNCs in the Chinese market makes the issues of censorship in China difficult to untangle. The Shi Tao case and others like it show the situations that MNCs are often put in when they enter the Chinese market, given the rules and regulations that Yahoo! was required to sign onto, along with the need for the company to join with Alibaba. The Google case further shows these issues, showing the tense relationship that can develop between company and government, especially in the case of a company that has a low market share and is the target of numerous incidents of government harassment (perceived or otherwise). These cases are all further complicated by the presence of companies like Narus, which are staffed by former government officials. All of these dilemmas make it difficult to promote an effective legal or norm based regime from the international community. Current solutions and proposed solutions have been shown to suffer from two major problems. In the case of the Global Compact, we are able to see that one of the problems is that a more generalized regime that is based on corporate citizenship is too vague and hard to enforce. In the case of the Global Online Freedom Act, the other problem readily emerges. That problem is the fact that more specific and ranging laws on the subject are difficult to get passed as the political will for such issues seems to be lacking. The Global Online Freedom Act has been stuck in committee since its initial introduction in 2006. As such, it is likely the law will not pass, at least not in its current or previous forms.

Chapter 4: Censorship Activities in China and Coordination Goods

So far, this thesis has discussed the censorship of the internet in China. Included in this discussion is a discussion of the history of the internet in China and the regulatory measures used by the Chinese government in blocking the internet. Also, this thesis has discussed the role of multiple actors involved in this discussion. Now, this thesis will turn its discussion to the human rights aspects of China's censorship. China has a well documented history of abusing human rights, including the torture and forced imprisonment of dissidents, including those from Tibet.[132] Also, the mere violation of freedom of expression, as shown in the censorship of the internet, is a bona fide violation of the human rights of the Chinese people. While some in China would seek to argue that freedoms like freedom of expression can lead to chaos, the lack of a unified chorus of such thoughts serves to weaken these claims. This chapter will detail the Chinese abuses of human rights and then tie them to the censorship of the internet. This will be done two ways. One, it will be done by arguing that the censorship of the internet is a measure to hide abuses from the mainstream public in China. Second, it will be argued that the censorship of the internet, or any media, is a violation of the freedom of expression and, thus, a human rights violation. After tying these aspects together, this chapter will touch on the issue of "Asian Values," which, as argued by proponents, place Asian countries in a different context from the countries in the West. However, this paper will argue that Asian values are not even a wholly accepted principle within Asia and, as such, are merely a smoke screen for bad behavior on the part of Asian governments, including the Chinese. Given that Asian Values are not wholly accepted by all members of the Asian societies, one must question whether or not a unified version of "Asian Values" can even be proposed. While some may still argue that the freedoms given by unfettered access and use of mediums like the internet may lead to chaos, it would be

[132] Ben Carrdus and Royce Priem, interview with Joseph House, Washington, DC, March 9, 2011.

disingenuous to say that such rationale exists only within the Asian context. Thus, while the individual values may exist for some, when a government claims that “Asian Values” are the reason for their actions, such claims must be taken with a grain of salt. From there, this chapter will discuss the relationship of the internet, human rights, and coordination goods, arguing that the restriction of communication and planning capabilities, often through censorship, is an effective method of circumventing dissidents and others in authoritarian regimes. In total, this chapter will argue that the internet is used to both undermine human rights and hide instances where human rights are abused, in violation of international standards. Further, it will argue that attempts by the Chinese and others to justify their actions of philosophical or values-based grounds should be discounted. Lastly, it will argue that these violations of rights are aimed at a general desire to limit to coordinating power of dissident groups, to maintain the power of the Chinese state.

Part I: China and Human Rights

China has long shown a willingness to abuse the rights of groups that oppose the state. The Tibetan minority, for example, has endured many actions that violate their rights at the hands of the Chinese government.[133] Further, China has shown a willingness throughout its recent history to give the illusion of human rights. This is noted by Ying Ma, who writes:

[133] Ben Carrdus and Royce Priem, interview with Joseph House, Washington, DC, March 9, 2011.

> "Though millions of villagers throughout China have now experienced elections firsthand, such elections are deeply flawed. Many are uncompetitive; many others provide little or no choice over the slate of candidates; fraud is rampant; and those elected, fairly or not, often wield little decision-making power. Furthermore, the government shows little interest in expanding the elections to the national level. On the rule of law, though China now eagerly participates in rule-of-law exchanges with the United States, it has permitted legal reforms for the purpose of facilitating economic development and making its governance more efficacious, not more democratic. As such, Beijing has limited legal reform only to politically safe areas, such as commercial and administrative law, and has barred legal reform from politically sensitive areas such as political dissent, labor unrest, and religious freedom."[134]

Further, some have noted that any efforts towards liberalization may be a way to move political reform up the agenda without engaging in higher stakes activities, such as actual elections or more consequential steps. [135] Again, Ma points out:

> "Of course, regime institutionalization alone cannot quell political discontent, dissent, or opposition, but this is where the effective suppression and cooptation of rival political groups come in. Beijing has brutally suppressed the spiritual group Falun Gong, a Buddhist sect that surprised and alarmed the regime by massing outside of its walled leadership compound in Beijing in a 10,000-strong silent protest on April 25, 1999. Similarly, the CCP has effectively cracked down on the China Democracy Party, which democracy activists in 1998 attempted to organize as the first national opposition party under communist rule."[136]

Others have brought this point home. Joshua Kurlantzick warned against the nature of the Chinese government, which would give small concessions to some groups while cracking down on others, making oppression easier by only going after a few cases in a very harsh way. According to Kurlantzick:

[134] Ying Ma, "China's Stubborn Anti-Democracy," *Policy Review* (February and March 2007): 6.

[135] Joseph Fewsmith, "Feedback without Pushback? "Innovations in Local Governance," statement to Congressional-Executive Commission on China, "Political Change in China? Public Participation and Local Governance Reforms," May 15, 2006, 8.

[136] Ying Ma, "China's Stubborn Anti-Democracy," *Policy Review* (February and March 2007): 8.

> "Instead of publicly suppressing all religious organizations, political dissidents, or ethnic minorities, Beijing has begun playing groups off each other, sanctioning a few mainstream organizations while quietly but harshly repressing those that challenge state authority."[137]

What has never ceased to be important is the presence of threat to the Chinese government. If there is a threat present to the government, the government will not hesitate to crack down on the source. Hence, movements that seek tangible goals, like autonomy or separation are cracked down on while less aggressive groups (like the Catholic Church) are allowed to flourish.[138] According to Ma:

> "In short, the Chinese regime has not sat haplessly by when confronted with challenges to its rule but has instead aggressively fought to maintain power. Its tactics may have differed with each political challenge, but the result — continuation of CCP rule — has remained the same."[139]

Further, Kurlantzick argues that Beijing wants to be seen as a country that is tolerant while viciously striking down those who disagree. This, he argues is the country's "two-pronged strategy."[140] Kurlantzick even goes so far as to write:

> "Indeed, Beijing seems to want it both ways: to appear to be more tolerant even while relentlessly suppressing dissent. China's current leaders, most of whom would be more accurately described as technocrats than as revolutionaries, are more cautious than their immediate predecessors about managing China's international image. President Jiang and like-minded members of China's leadership tended to avoid blatant methods of control, preferring a mix of carrots and sticks and more subtle forms of repression."[141]

More threatening organizations would likely include the Falun Gong, Tibetan groups, and democracy dissidents. Less threatening groups would likely be major international religions.

[137] Joshua Kurlantzick, "The Dragon Still Has Teeth: How the West Winks at Chinese Repression," *World Policy Journal* XX, 1 (Spring 2003).

[138] Ibid.

[139] Ying Ma, "China's Stubborn Anti-Democracy," *Policy Review* (February and March 2007): *9.*

[140] Joshua Kurlantzick, "The Dragon Still Has Teeth: How the West Winks at Chinese Repression," *World Policy Journal* XX, 1 (Spring 2003).

[141] Ibid.

Looked especially kindly upon by the Chinese government are business groups, many of which push for economic growth – which China likes. Beyond business, many major religions have been co-opted and persuaded to denounce the Falun Gong. In the wake of friendly overtures to business and mainstream churches, the Falun Gong, called an "evil cult" in China has been the target of several Strike Hard Campaigns. Similar campaigns have been carried out against Uighurs and Tibetans. [142] Further, Kurlantzick argues that this two pronged strategy has also been used against labor movements and peasants' rights groups.[143] This is not surprising, given the government's insistence on economic growth without political growth. Peasants groups and labor groups provide little economic incentive. Indeed, they provide possibly economic disincentive, removing labor conditions that are more favorable for business, as cheaper labor may equal a higher profit margin.

Such issues have not gone unnoticed by the international community. China made certain promises on human rights in the run up to getting the 2008 Olympic Games.[144] Indeed, the Secretary General of the Beijing Olympics Bid Committee, said, ''We are confident that the Games coming to China not only promotes our economy, but also enhances all social conditions, including education, health, and human rights.''[145] Yet, as was pointed out by Representative Sander Levin, the Chairman of the Congressional-Executive Committee on China (CEC), at a hearing six months before the Olympic Games in Beijing:

[142] Joshua Kurlantzick, "The Dragon Still Has Teeth: How the West Winks at Chinese Repression," *World Policy Journal* XX, 1 (Spring 2003).

[143] Ibid.

[144] Congressional-Executive Commission on China, "The Impact of the 2008 Olympics on Human Rights and the Rule of Law in China," 110th Congress, 2nd Session, 27 February 2008, 1.

[145] Ibid, 2.

> “These same authorities assert that raising concern over human rights in the context of the 2008 Games violates the Olympic spirit. Nothing could be further from the truth. Fairness on the field of play, fair judgments, and the opportunity to witness human potential unleashed to the fullest extent are the very essence of the Olympic spirit. They are also the essence of freedom and fundamental human rights.”[146]

Senator Byron Dorgan, the committee’s co-chair, noted some of the injustices committed by the Chinese government, saying:

> “Just last week (Feb 2008), Yang Chunlin, an unemployed factory worker, went on trial for subversion in northeast China. He was arrested last year for reportedly helping nearby villagers seek compensation for lost land. He had collected 10,000 signatures from local farmers. The signatures were for a letter that read in part: ‘‘We Want Human Rights, Not the Olympics.’’ Prosecutors said that that letter stained China’s international image, and that it amounted to subversion, so this unemployed factory worker went on trial.”[147]

Also, Table 3 shows a sample of political prisoners in China. This list was entered into the record by Senator Dorgan at the hearing.[148]

[146] Congressional-Executive Commission on China, “The Impact of the 2008 Olympics on Human Rights and the Rule of Law in China,” 110th Congress, 2nd Session, 27 February 2008, 3.

[147] Ibid, 4.

[148] Ibid, 64. Note: The figure is shown on page 47.

Table 3. Cases of Political Imprisonment in China

LIST OF POLITICAL PRISONERS SUBMITTED BY SENATOR BYRON DORGAN

1. **Hu Jia:** A prominent activist who has advocated on behalf of HIV/AIDS patients, environmental issues, and other rights defenders, Hu was detained by Chinese authorities on December 27, 2007, on suspicion of ‘‘inciting subversion of state power.’’ Hu’s detention may be linked to comments he made at a European Parliament hearing that were critical of China’s hosting of the Olympics.

2. **Yang Chunlin:** As a land rights activist, Yang reportedly collected more than10,000 signatures from farmer for a letter titled ‘‘We Want Human Rights, Not the Olympics,’’ protesting the farmers’ loss of land. Yang was detained in July 2007, and stood trial on charges of ‘‘inciting subversion of state power,’’ on February 19.

3. **Wu Lihong:** An environmental activist from Jiangsu province, Wu spent more than a decade documenting pollution in Lake Tai, including providing environmental information to the government and the media. Shortly after Wu was detained in April 2007, Lake Tai experienced one of the worst blue-algae blooms, with millions of area residents without water for a few days. Wu was sentenced in August 2007 to three years in prison on the pretext of extortion and fraud.

4. **Guo Feixiong:** Guo is a prominent lawyer who was active in helping ordinary Chinese citizens defend their rights. In November 2007, Guo was sentenced to five years in prison for ‘‘illegal operation of a business,’’ for allegedly distributing a publication without the necessary government license. The publication, which concerned a political scandal, reportedly angered local officials.

5. **Ronggyal Adrag:** A Tibetan nomad, Adrag was detained in August 2007 after he walked onto the speakers’ stage at a horse-racing festival and called for the Dalai Lama’s return to Tibet, the release of the Panchen Lama identified by the Dalai Lama, and Tibetan independence. In October, a court sentenced him to eight years in prison on the charge of ‘‘inciting splittism.’’

6. **Adrug Lupoe:** A nephew of Ronggyal Adrag, Adrug Lupoe is a monk who was sentenced by the same court to 10 years’ imprisonment on charges of splittism and espionage. He allegedly helped two other men attempt to send digital photos out of China of the local security crackdown.

7. **Nurmemet Yasin:** He is an ethnic Uighur writer from Xinjiang who wrote a short story in 2004 about a caged bird who chooses suicide over living without freedom. Chinese authorities viewed the story as an attack on government policy in Xinjiang, and sentenced him in 2005 to 10 years in prison for ‘‘inciting splittism.’’

What can be seen by these examples is that China has a robust tradition of political imprisonment and behavior that violates the rights of many of its citizens, especially those who have presented a threat to their government. These actions have often been paired with hollow gestures towards less dangerous groups or actions that have been used as an attempt to hide

China's human rights record. However, this is only the beginning of the tangled web woven by the Chinese on human rights. This chapter will now discuss the relationship of the internet to human rights and the Chinese efforts to stifle and use the internet at the same time to benefit their particular position on human rights and political liberalism.

Part II: The Internet and Human Rights

There is a long standing belief that the right to information and to impart information has been central to human rights. This can be seen in the ideas of freedom speech, freedom of expression, freedom of redress, and freedom of association. According to Brian W. Esler, "The right to impart and receive information freely has long been a cornerstone of human rights law."[149] Many argue that the internet is part and parcel of this freedom of information, serving as a tool for speech. Esler argues that internet access opens up speech.[150] He says that the very ordering of content online could affect perception and that one way to control this order is through content filtering – censoring objectionable material.[151]

Beyond this, other authors have that the internet is a vital aspect in the rise of civil society actors and others. According to Ronald Deibert and Nart Villeneuve, "The internet has been a central force in facilitating the rise of civil society actors, dissidents, and transnational social movements of all stripes."[152] However, it is important to note that the technology is 1) still under the purview of the state; and… this technology is still not beyond the control of the state and 2) that too proactive a view of the rights based potential of the internet could pose serious

[149] Brian W. Esler, "Filtering, Blocking and Rating: Chaperones or Censorship," in *Human Rights in the Digital Age*, ed. Mathias Klang and Andrew Murray, (New York: Routledge Cavendish, 2005), 99.
[150] Ibid.
[151] Ibid, 100.
[152] Ronald Deibert and Nart Villeneueve, "Firewalls and Power: An Overview of Global State Censorship of the Internet," in *Human Rights in the Digital Age*, ed. Mathias Klang and Andrew Murray, (New York: Routledge Cavendish, 2005), 111.

implementation problems.[153] Such warnings about the internet and human rights abound. David Weinberger notes:

> "There are at least two ways to take the call to claim Net access as a human right…. The first is the stronger claim: People have the right to Internet access, just as they have a right to food and shelter. The second expresses qualities of the Internet to which people should have access."[154]

Weinberger notes that Secretary Clinton, in her January 2010 speech on the internet, seemed to be talking about the second sense of Internet human rights. He notes that the first four of her five proposed rights connected to the internet apply existing human rights to the more technological domain of the internet. The fifth, as he points out, is her discussion of the right to connect, of which she said, "… governments should not prevent people from connecting to the internet, to websites, or to each other." Weinberger argued that she was, "analogizing it to freedom of assembly." He continued, "I like those five freedoms, but the analogy doesn't quite work."[155] The first sense of the internet being a human right is a difficult course to navigate because of the inability for all governments to provide access to the net. The second sense is easier because it merely asks that governments do not stand in the way of free use of the internet. However, Weinberger still finds some problems with the second view as well. Namely, he is concerned with the procedures that would need to be implemented in the various situations that could be discussed regarding internet human rights abuses. He questions what could be or would be done regarding German restrictions on Nazi EBay sales or on restrictions to the adult section

[153] Ronald Deibert and Nart Villeneueve, "Firewalls and Power: An Overview of Global State Censorship of the Internet," in *Human Rights in the Digital Age*, ed. Mathias Klang and Andrew Murray, (New York: Routledge Cavendish, 2005), 111.

[154] David Weinberger, "The Internet as a Human Right," *Joho the Blog,* Published 19 September 2010, accessed 24 September 2010, http://www.hyperorg.com/blogger/2010/09/19/the-internet-as-a-human-right/.

[155] Ibid.

of Craigslist.[156] His main concern is the degree to which the international community could become involved in the policing of content violations. There seems to be a definite question of enforceability, which harkens back to our discussion of the Global Compact and, to a lesser extent, the Global Online Freedom Act in Chapter 3.

However, Weinberger makes the point that freedom of speech has some similar issues attached to it and we still attempt to promote free speech.[157] The bigger issue seems to be the insistence that countries engage in positive steps to provide the internet to their people, something that many human rights don't call for.[158]

The viewing of the internet as part of the international human rights discussion has led to different groups promoting ventures to quantify internet rights. Ling Cangzhou and others have called for an internet human rights doctrine, which is shown in Table 4, below[159]:

[156] David Weinberger, "The Internet as a Human Right," *Joho the Blog,* Published 19 September 2010, accessed 24 September 2010, http://www.hyperorg.com/blogger/2010/09/19/the-internet-as-a-human-right/.
[157] Ibid.
[158] Ibid.
[159] C.A. Yeung, "Internet Human Rights Declaration," *Under the Jacada Tree Blog*, Published 08 October 2009, accessed May 30, 2010, http://underthejacaranda.wordpress.com/2009/10/08/internet-human-rights-declaration/. The original source is listed as Canyu and the original authors are listed as 15 Chinese intellectuals, including Ling Canzhou. The declaration was also published at the Global Voices Blog and other locations on the internet. Note: the figure is shown on page 51.

Table 4. Principles of the Internet Human Rights Declaration

“We therefore pledge for the following principles to be endorsed:

1. Freedom of speech on the Internet is a part of citizens’ rights to freedom of speech. It is the most basic human rights and the most fundamental value that should be pursued, treasured and protected.

2. Netizens who express their opinions on the Internet using words, sounds, pictures or videos, should be protected and encouraged, as long as such conduct is in accord with the constitution and local statutes.

3. The right to publish opinion is the most basic rights for netizens. This includes the right to publish through weblogs and podcasts, as well as online discussion forums. Netizens’ rights to publish should not be subjected to unlawful investigation and interference. They should be allowed freedom to hold and to express their views without feeling intimidated.

4. Netizens’ editorial rights should be respected. When they are exercising those rights, they should not be subjected to harassment by authorities who act outside of law.

5. It is the right of Netizens to conduct interviews and to report their findings. This right is protected as a part of their constitutional rights to freedom of speech. Netizens who exercise this right should endeavor to report the truth, and to avoid distortions, fabrications and malicious slander.

6. It is the right of netizens to make comments and to exchange opinion. This includes the right to ask questions, to monitor, to criticize and to boycott.

7. Netizens’ freedom of speech encompasses a right to express themselves anonymously. Anonymity enables some authors to express their opinions in ways that best suit their needs. This legal right should be respected as long as an anonymous author is expressing his views in accordance with legal and constitutional requirements.

8. The right to conduct information searches on the Internet is an integral part of netizens’ rights to express, to be informed and to monitor. It is our opinion that legal websites should not be filtered, and that netizens’ rights to conduct searches on public information for personal use should be respected and protected.

9. Online privacy should be respected and protected. Netizens’ real identities and personal information should not be disclosed unless the information is required for a transparent legal proceeding, or else if the disclosure is necessary under the rule of law.

10. The freedom of disseminating information should be respected and protected as long as it is conducted in line with legal and constitutional requirements. Website monitoring, filtering and blockades that go against the principle of freedom of speech should be condemned by public opinion. Netizens are entitled to seek freedom of expression and justice through judicial proceedings.”

It should be noted that China would argue that its restrictions meet the requirements laid out in item two, arguing that such discussions are outside the purview of the local constitution and statutes. This goes to the Chinese argument that such speech is tantamount to a danger to the state, despite Article 35 of their own constitution, which states, “Citizens of the People's Republic of China enjoy freedom of speech, of the press, of assembly, of association, of procession and of demonstration.”[160] Regardless of the mixed messages on free speech given by the Chinese government, it is highly likely they would argue that such discussions are not protected, given their consideration of them as a threat. Also, it should be noted that item three ties the issues of surveillance and censorship together. Certainly, it can be argued that the idea of threat is likely linked to the notion that someone is watching. Thus, governmental censorship, even in the absence of actual censorship would violate these rights as it could encourage a user to not look for content considered controversial. Thus, Chinese attempts to foster “self-censorship” or a “mental firewall” are not immune from the criticisms levied within this document. Lastly, it is important to note that much of what is put forth is this discussion has to do with the production of material and not the viewing of material, as it goes to the ability of groups and individuals to produce news and opinion online without interference. This is one side of the coin. However, the other side of the coin is the ability of people to be able to view such material. This would be difficult if such material was censored by government or third party sources. Such a declaration is weaker on this point than on issues of surveillance, intimidation, and destruction of inflammatory information. It remains to be seen what the reaction in the internet community will be to the right to read as opposed to a right to publish.

[160] “Article 35,” *Constitution of the People’s Republic of China,* adopted on 04 December 1982, as published by The People’s Daily, http://english.peopledaily.com.cn/constitution/constitution.html.

Part III: Censorship

James Fallows notes that "China is frequently cited as one of the most censorious countries in the world."[161] He argues that this is because the country has a series of "choke points" for its internet access.[162] He notes that there are only three fiber optic entrances, one at Beijing-Qingdao-Tianjin for the North, one at Shanghai for the Central, and one at Guangzhou for the South.[163] This makes it easier for China to monitor foreign data because it restricts the disbursement of the censorship apparatus.[164] China's goal – make searches just difficult enough for a casual user to quit, something he refers to as a mental firewall.[165]

This is shown in the US-China Economic and Security Commission's (USCC) Annual Report to Congress in 2010, which notes:

> "China's leadership, at all levels of the government, increasingly uses the Internet to interact with the Chinese people. This practice, interwoven with strict censorship controls, affords the government the ability to allow a controlled online debate about certain issues, especially those that do not relate to China's political situation."[166]

Still, the commission comes back to note that China has one of the most pervasive censorship regimes in the world, as noted below:

[161] James Fallows, "China's Internet Censorship is Effective," in *Censorship: Opposing Viewpoints*, ed. Scott Barbour (Farmington Mills, MI: Greenhaven Press, 2010), 113.
[162] Ibid, 114-15.
[163] Ibid, 115.
[164] Ibid.
[165] Ibid, 118.
[166] US-China Economic and Security Commission, "China's Domestic Internet Activities," *Annual Report to Congress 2010*, Chapter 5, Section 1, 221.

> "The Commission has previously noted that China employs one of the largest and most sophisticated Internet content filtering systems in the world. Developments in 2010 reinforce the evidence that pervasive online censorship and restrictions on speech remain the norm in China. These censorship measures, combined with efforts to direct the nature of discussions on the Internet, play an increasingly prominent role in Chinese authorities' governing strategy. Key documents released in 2010 articulate this strategy and include other information about the Chinese government's policies and approach to the Internet."[167]

Much of China's censorship is tailored to not only hide activities committed by the Chinese government, but to paint the West in a negative light. This is noted in the USCC report, which says:

> "The congressman (Chris Smith) cited an example of how China's censorship and propaganda efforts are finely tuned to shield the Chinese Communist Party from criticism. Specifically, Representative Smith conducted an online search for materials by Manfred Nowak, United Nations (UN) Special Rapporteur on Torture. Mr. Nowak's report about the treatment of detainees at Guantanamo Bay was available to Chinese Internet users; a separate report that found widespread torture within China, however, was not."[168]

The report referred to such efforts as "selective censorship." The report loops this into a larger discussion of how the Chinese have managed the internet as part of a social conversation on conditions. The report concludes their discussion as such:

> "Chinese authorities have managed skillfully to balance their perceived need to limit speech on the Internet with the Chinese public's need to feel a part of an ongoing and participatory discourse about the country's social conditions. The Chinese government has used all available means to bind the content and scope of this conversation. At the same time, the government has been selectively responsive and has attempted to remediate some of the nation's most serious irritants in order for the Chinese Communist Party to maintain power. This confluence of conditions might be termed 'network authoritarianism.'"[169]

Zhao also discusses the fact that much of the effectiveness of Chinese censorship may come from its division of labor between the CCP, which handles the policy and the propaganda

[167] US-China Economic and Security Commission, "China's Domestic Internet Activities," *Annual Report to Congress 2010*, Chapter 5, Section 1, 221.
[168] Ibid, 224.
[169] Ibid, 235.

surrounding the internet, and the government, which handles the structural and industrial aspects of the censorship.[170] Zhao argues that the Chinese are decentralizing their censorship to be more effective with less political cost.[171] Part of this effort to be more effective is through"passive censorship," a practice of limiting the impact of an offending story by relegating it to a small group of isolated members of society.[172] According to Zhao, this is seen as more practical, as the Chinese government has "given up" on mass indoctrination.[173]

Despite all of this, the Chinese government still proclaims that the Chinese people enjoy freedom on the internet, noting in their 2010 White Paper on the Internet:

> "Chinese citizens fully enjoy freedom of speech on the Internet. The Constitution of the People's Republic of China confers on Chinese citizens the right to free speech. With their right to freedom of speech on the Internet protected by the law, they can voice their opinions in various ways on the Internet. Vigorous online ideas exchange is a major characteristic of China's Internet development, and the huge quantity of BBS posts and blog articles is far beyond that of any other country. China's websites attach great importance to providing netizens with opinion expression services, with over 80% of them providing electronic bulletin service. In China, there are over a million BBSs and some 220 million bloggers. According to a sample survey, each day people post over three million messages via BBS, news commentary sites, blogs, etc., and over 66% of Chinese netizens frequently place postings to discuss various topics, and to fully express their opinions and represent their interests. The new applications and services on the Internet have provided a broader scope for people to express their opinions. The newly-emerging online services, including blog, microblog, video-sharing and social networking websites, are developing rapidly in China, and provide greater convenience for Chinese citizens to communicate online. Actively participating in online information communication and content creation, netizens have greatly enriched Internet information and content."[174]

[170] Yuezhi Zhao, *Communications in China: Political Economy, Power, and Conflict,* (Lanham, MD: Rowan and Littlefield Publishers, Inc., 2008), 24.
[171] Ibid, 34.
[172] Ibid.
[173] Ibid.
[174] "Guaranteeing Citizens' Freedom of Speech on the Internet," *Chinese White Paper on the Internet*, 08 June 2010, accessed 26 March 2011, http://www.gov.cn/english/2010-06/08/content_1622956_5.htm.

In one of the more ironic twists, the Chinese White Paper on the Internet 2010 says, "The Internet's role in supervision is given full play."[175] This is especially ironic given the supervision and surveillance that the Chinese government goes through with its population. The Chinese government shows a remarkable knack for understatement when it states:

> "China advocates the rational use of technology to curb dissemination of illegal information online. Based on the characteristics of the Internet and considering the actual requirements of effective administering of the Internet, it advocates the exertion of technical means, in line with relevant laws and regulations and with reference to common international practices, to prevent and curb the harmful effects of illegal information on state security, public interests and minors."[176]

Despite all of this, some see the openings in the Chinese system as a way to circumvent Chinese censorship. April Gu contends that stories such as Wang Keqin and Gao Yaojie show that "blogs are still a problem" for China's internet controls.[177] Gu still acknowledges that the Chinese government uses self-censorship to counteract blogs.[178]

What is missed by Gu and others like her is that the Chinese engage the internet to serve as a propaganda tool for them in conjunction with their censorship and surveillance tactics. As such, they are able to reinforce their position with the internet, even if they do not effectively control the entire space. The idea used by the Chinese government is as much about information control as it is about censorship. Failing to recognize this may be the key reason why so many authors have fallen into the cyber utopianism camp. Further, Zhao's discussion of "passive censorship" and the willingness of the other authors to concede that not all stories are censored should serve as a counterbalance to arguments by Gu and others. No one is arguing that the Chinese are trying

[175] "Guaranteeing Citizens' Freedom of Speech on the Internet," *Chinese White Paper on the Internet*, 08 June 2010, accessed 26 March 2011, http://www.gov.cn/english/2010-06/08/content_1622956_5.htm.
[176] Ibid.
[177] April Gu, "China's Internet Censorship can be Circumvented," in *Censorship: Opposing Viewpoints*, ed. Scott Barbour, (Farmington Hills, MI: Greenhaven Press, 2010), 123-26.
[178] Ibid, 126.

to create an airtight system. Instead, they are arguing that they are creating a system that catches most stories and marginalizes the others to the point at which they are no longer effective. This is partly done through propaganda.

Part IV: Propaganda

According to David Shambaugh and others, "propaganda and indoctrination were a hallmark of the Maoist state."[179] Shambaugh notes, "The roles played by official propaganda in China today have declined considerably since the Maoist era, but remain an important part of Chinese political and cultural life."[180] One thing is clear - China's propaganda system is vast and far reaching, extending into most aspects of life.[181] When we consider this with the censorship apparatus of China and the attempts of the Chinese government to quarantine information, one can see how the Chinese control information. Shambaugh notes this by saying:

> "Censorship, however, is only one side of the coin. The CCPPD is much more regularly engaged in what might be described as *proactive* propaganda—writing and disseminating the information that it believes *should* be transmitted to, and inculcated in, various sectors of the populace."[182]

Shambaugh lays out the complexity of the Chinese propaganda apparatus, noting that several governmental layers comprise the system that engages in propaganda activities in China, allowing for the country to maintain a vigorous and nuanced system of information control. Shambaugh notes that the system has departments for ideological research, media control, and cultural study.[183] All of this shows how the Chinese propaganda apparatus is

[179] David Shambaugh, "China's Propaganda System: Institutions, Processes, and Efficacy," *The China Journal* 57 (January 2007): 26.

[180] Ibid, 27.

[181] Ibid, 27-28.

[182] Ibid, 29.

[183] Ibid, 39.

able to continually evolve to provide the government with new means of information control.

Shambaugh acknowledges that propaganda activities have lost some of their effectiveness in the modern world, even as censorship and control capabilities remain strong, noting:

> "While its control and censorship abilities remain substantial, the propaganda authorities have lost some of their control in the face of technological modernization, social pluralization, economic marketization and globalization."[184]

In general, Shambaugh notes, "It is particularly evident that propaganda and public security authorities are intent on controlling Internet access and blog discourse."[185] As such, one can readily discern that the propaganda and censorship apparatuses of the Chinese government are related in that they are both being used to control the internet. While propaganda activities have waned in recent history, censorship has remained the driving force, consistently evolving and adjusting, blended with propaganda and surveillance activities to engage in an overall control strategy for the internet. It is important to note the collective notion of Chinese internet control. Only talking about one of these aspects limits the perception of the effectiveness of the Chinese regime and could lead to misguided thoughts about the internet being able to fill the numerous holes left by the government. Such thoughts, unchecked, fail to take into account the Chinese efforts to manipulate their own public opinion through propaganda, surveillance, and other measures that discredit information that comes through and limit the amount of controversial data published. As such, the failure to understand this relationship could lead to horrible consequences for dissidents and others in China based on its lack of understanding of the local Chinese context and reliance on cyber utopian views. This is not merely a pragmatic

[184] David Shambaugh, "China's Propaganda System: Institutions, Processes, and Efficacy," *The China Journal* no. 57 (January 2007): 55.

[185] David Shambaugh, "China's Propaganda System: Institutions, Processes, and Efficacy," *The China Journal* no. 57 (January 2007): 57.

discussion. Government officials and others have proclaimed that Asian nations have a unique set of values, often called Asian Values, which makes their actions of repression and control permissible. These values will be discussed in the next section as another avenue used by the Chinese to control the populace and defend their actions in the absence of an actual defense. As such, the next section will seek to debunk such claims as a whole, showing that such values are not universally accepted in China or the rest of Asia and showing other flaws within these values.

Part V: Asian Values vs. Universal Values

The idea of Asian values was developed by the leaders of Singapore and Malaysia to explain differences between Western and Eastern thought on issues in which Western thought deemed a universal viewpoint. According to Krzysztof Gawlikowski:

> "In the 1990s Mahathir bin Mohamad, Prime Minister of Malaysia, and Lee Kwan Yew, former Prime Minister of Singapore, promoted the concept of "Asian values." They both challenged a supposition cherished by numerous Western politicians and intellectuals that Western values and democratic institutions constitute a universal paradigm that should be adopted by all the nations of the world."[186]

Gawlikowski continued, noting, "Both Asian leaders, along with their numerous Asian supporters, maintain that Asia has her own system of values, different from that of the West."[187] Further, Gawlikowski notes the often discussed idea of "cultural imperialism" as a part of the formation of Asian Values, much of which comes from the colonial legacies of many of the countries in Asia. Such a discussion would have to include China, which spent much of the 19th century being ruled over by the West.[188] According to Gawlikowski:

[186] Krzysztof Gawlikowski, "'Asian Values' and Western Universalism," *Dialogue and Universalism* 10, 1-2 (2000): 183.
[187] Ibid.
[188] Dr. Erick Novotny, Interview with Joseph House, Washington, DC, 16 February 2011.

> “Moreover, it is their view that Asian values are much more universal and commonly acceptable than Western values based on the individual. They consider the West's attempts to impose its own value system a kind of "cultural imperialism" and a remnant of colonial ideology. They therefore defend the rights of the Asians to possess and uphold their own values. Although their opinions have met with fierce opposition in the West, certain eminent scholars, such as Samuel P. Huntington, have essentially accepted the vision of numerous civilizations with their own values. Furthermore, they believe that the West and non-Western civilizations should learn to co-exist without imposing their own values on others and without condemning them as "barbarous" merely because they cherish different values and priorities.”[189]

Singapore, being one of the first countries to develop Asian Values, has been instrumental in the definition of these values. Former Singaporean ambassador to the United States Tommy Koh has gone so far as to list the ten values that he believes makes up the core of Asian Values. These values are listed below in Table 5:[190]

[189] Ibid.

[190] Tommy Koh, “The Ten Values That Undergird Asian Strength and Success,” *The New York Times*, 11 December 1993, accessed 08 September 2009, http://www.nytimes.com/1993/12/11/opinion/11iht-edkoh.htm. Note: This piece was originally written as Mr. Koh’s personal comment to the *International Herald Tribune.* It included his discussions of why these values made Asian societies better than those in the West. These comments, as they did not deal with the specific values, were removed. As such, each of the ten values listed is shorter than originally published. Each deletion is noted with an ellipsis.

Table 5. Tommy Koh's List of Ten Values That make up the Concept of Asian Values

1) East Asians do not believe in the extreme form of individualism practiced in the West. We agree that every individual is important. However, he or she is not an isolated being, but a member of a nuclear and extended family, clan, neighborhood, community, nation and state….

2) East Asians believe in strong families….

3) East Asians revere education. Unlike the West, this is a value held not only by the elite but by all strata of society. Asian mothers would make any sacrifice to help their children excel in school….

4) East Asians believe in the virtues of saving and frugality….

5) East Asians consider hard work a virtue - the chief reason this region is outcompeting Europe….

6) East Asians practice national teamwork. Unions and employers view each other as partners, not class enemies. Together, government, business and employees work cooperatively for the good of the nation….

7) There is an Asian version of a social contract between the people and the state. The government will maintain law and order, provide citizens with their basic needs for jobs, housing, education and health care. Governments also have an obligation to treat their people with fairness and humanity. In return, citizens are expected to be law-abiding, respect those in authority, work hard, save, and motivate their children to learn and be self-reliant….

8) In some Asian countries, governments have sought to make every citizen a stakeholder in the country….

9) East Asians want their governments to maintain a morally wholesome environment in which to bring up their children…. There is no reason Asians must adopt the Western view that pornography, obscenity, lewd language and behavior, and attacks on religion are protected by the right of free speech.

10) Good governments in East Asia want a free press but, unlike the West, they do not believe that such freedom is an absolute right. We do not want our press to be mere mouthpieces of government. Yet we believe that the press must act responsibly. For example, it has no right to instigate trouble between racial, religious or linguistic groups, or between countries. We also insist that the press should give those whom it has attacked the right to reply

The shortcomings to Koh's argument come in his generalizations. While many of these values seem to be things that anyone could get behind, they are often general and overarching, leading to conclusions that are probably unwarranted. Working to ensure a strong education for one's children, for example, would seem like a goal that all, but the most negligent of parents, would strive to attain. Certainly, Koh cannot be arguing that there are no negligent parents in Asia. And certainly many in the West view hard work as a virtue as well. Koh's reliance on generalization chips away at his reasoning that we are fundamentally different societies.

Koh's more controversial points (that Asian countries believe that pornography and obscenity should be limited, and that the free press is not an absolute right) are also far too general. Who can discern pornography, given that the United States Supreme Court had to rely on an argument that they would "know it when they saw it."[191] A similar question exists for obscenity and the other evils that Koh talks about. Further, Koh's assertion that the press should not intervene in relations between states or between ethnic groups, so as to not cause divisions is problematic. The statement is so general that it could easily be corrupted and twisted to such a point that the press is fully restricted by the government. Indeed, this may well be the case in a country like China, which has consistently argued that speech that has been restricted in all forms of media is tantamount to a threat to the state or the welfare of the Chinese society.

Asian Values could well exist. However, their current format is too general to be of use writ large. These values have to be expanded upon and explained so that they cannot be twisted and corrupted to cover for the sins of an authoritarian regime. Further, it is important to recognize that Asian values are not accepted as the same in all parts of Asia, one should consider that communist China takes a different view than Malaysia or Singapore, which have different heritages. Paul J. Magnarella notes:

> "There are at least four major critiques of universal human rights coming out of Asia. The communist critique treats human rights in terms of the class struggle and regards them as interests acquired from the government by the bourgeoisie to the disadvantage of the working class. The communitarian critique focuses on the allegedly excessive liberalism of individual freedoms of human rights, and advocates shared community values in their place. The pragmatist criticism questions claims of innate human rights and maintains instead that society is based at most on a temporary consensus. The cultural relativist critique argues that because values vary

[191] Justice Stewart, Consenting Opinion, Jacobellis v. Ohio, 378 US 174 (1964).

> with cultural context, and because human rights as presently conceptualized developed mainly in a Western context, they are not universal."[192]

Magnarella proceeds to cite Robert Weatherley regarding the historical underpinnings of China's version of Asian Values. What is laid out is a series of values that is informed by Confucian teachings and Marxist ideals. Magnarella paraphrases Weatherly, saying:

> "Weatherley maintains that Confucianism has been an influence in China for about two millennia (221 BC to 1911 CE), and that today's conceptions of Chinese human rights have been molded by pre-existing Confucian thought. In many respects, Weatherley argues, Confucianism was inhospitable to the concept of human rights, and the emphasis on duties overwhelmed any idea of individual rights (p. 10). Confucian social order was based on a moral hierarchy in which persons occupying some statuses, such as officials, husbands, fathers, were regarded as morally and socially superior to their complements: non-officials, wives, offspring."[193]

What is important about the Confucian inspiration for Chinese interpretations of Asian Values is that the inspiration had no foundation for individual rights, lacking the term or even the concept of rights.[194] Magnarella notes this, saying, "Weatherley quotes Chinese scholars Liu Zehua and Ge Quan: "There was basically no place for the individual or for individual rights in traditional Confucian society."[195] Regarding the influence of Marxist ideology on the Chinese version of Asian Values, Magnarella points again to Weatherley, but also provides a caveat, noting:

> "With the rise of the Chinese Communist Party and the establishment of the People's Republic of China (PRC) in 1949, rights in China have been influenced by Marxist ideology. However, Weatherley claims, the People's Republic still owed its duty-based orientation to Confucian morality. Mao Zedong, himself, spoke of the "Sinification of Marxism""
>
> While Westem, capitalist states, such as the United States, stress civil and political rights, China's rulers maintain that economic rights should take precedent. This

[192] Paul J. Magnarella, "Communist Chinese and 'Asian Values' Critiques of Universal Human Rights," *Journal of Third World Studies* XXI, 2 (2004): 179-80.
[193] Ibid, 180.
[194] Ibid.
[195] Ibid.

> emphasis on welfare rights over political rights had a great deal to do with the mass poverty that prevailed in China of the 1940s, just as it did in the early years of the Soviet Union."[196]

However, it should be stressed that not all groups in Asia prescribe to such viewpoints. Notable amongst this group is the Dalai Lama, who said, regarding the controversial issue of the relationship between economic and individual rights:

> "Many nations consider respect for the individual's civil and political rights to be the most important aspect of democracy. Other countries, especially in the developing world, see the rights of the society--particularly the right to economic development--as overriding the rights of the individual. I believe that economic advancement and respect for individual rights are closely linked. A society cannot fully maximize its economic advantage without granting its people individual civil and political rights. At the same time, these freedoms are diminished if the basic necessities of life are not met.[197]

The Dalai Lama further argues that democratization and rights are not the exclusive province of Western leaders and scholars. Such an argument takes away from the insistence of Asian leaders who assure the world that Asian societies are convinced of the sound nature of Asian values. Given the fact that each Asian society seems to have differing views of what should be their defining social norms, and that individual groups within these societies also have different interpretations of these norms, there are serious questions about the validity of a monolithic concept of Asian Values. When this is coupled with the overly general values that are often promoted to represent Asian Values, a definite argument can be made for the use of Asian Values as a smoke screen for authoritarian regimes that seek to violate the rights of their citizenry. As such, Chinese arguments for the presence of a unique set of Asian or Chinese values are not something that this author can take as valid. Instead, it seems like these arguments are the mere posturing of a repressive regime that is looking to prevent dissident groups from

[196] Paul J. Magnarella, "Communist Chinese and 'Asian Values' Critiques of Universal Human Rights," *Journal of Third World Studies* XXI, 2 (2004): 180-81.

[197] His Holiness the Dalai Lama, "Buddhism, Asian Values, and Democracy," *Journal of Democracy* 10, 1 (1999): 4-5.

having a voice within the country. The next two sections will discuss how this occurring, looking at the idea of coordination goods and how the control of coordination goods through the politics of technology in China is helping the regime to stay in power.

Part VI: Coordination Goods

The term, coordination goods, comes from an article by Bruce Bueno de Mesquina and George Downs discussing democracy and development. Bueno de Mesquina and Downs define the term, coordination goods, as, "…those public goods that critically affect the ability of political opponents to coordinate but that have relatively little impact on economic growth."[198] According to the authors, coordination goods are part of strategic coordination, or "the set of activities that people must engage in to win political power in a given situation."[199] In general, Bueno de Mesquina and Downs argue that authoritarian states must be viewed as active participants in their own governance, something that they consider missing from the usual discussion of democratization. They note that many who study democratization have instead viewed authoritarian states as passive, saying:

> "Lipset's followers have also tended to overlook the fact that autocratic states are not passive observers of political change; in fact, they set the rules of the game and can rig them to suit their interests. Autocrats enjoy a marked advantage over the average citizen in their ability to shape institutions and political events. And they have proved far more savvy at this than expected, adroitly postponing democratization often while still continuing to achieve economic growth."[200]

Bueno de Mesquina and Downs note that the potentially biggest factor in the continued survival of some regimes (they mention three – China, Venezuela, and Russia) has been the

[198] Bruce Bueno de Mesquina and George Downs, "Development and Democracy," *Foreign Affairs* 84, 5 (2005): 82.
[199] Ibid, 80.
[200] Bruce Bueno de Mesquina and George Downs, "Development and Democracy," *Foreign Affairs* 84, 5 (2005): 80.

focus on maintaining economic growth while limiting political liberalization.[201] In this endeavor, communication is viewed as very important by the authors, who say:

> "A diverse and largely unregulated press (and other forms of media) is also vital to effective political opposition, since it enables the dissemination of information that can bring diverse groups together around common interests. Like political rights, the right to a free press is a largely negative one, since it generally requires the government not to interfere. It may also require affirmative steps, however, such as granting licenses to radio and TV frequencies, guaranteeing public access to those and other media, and translating official documents into regional languages."[202]

The authors cite a survey that indicates that: 1) the provision of coordination goods limited the lifespan of authoritarian regimes; 2) modern autocrats suppress coordination goods more consistently than other goods; 3) more suppression of coordination goods leads to lag between economic growth and political liberalization; and 4) economic growth can largely be sustained even with the suppression of coordination goods.[203] The authors argue that this is important given Western tendencies to focus on economic liberalization as a method to lead to political liberalization.[204] If authoritarian states are able to maintain economic development while resisting political liberalization, then traditional narratives on democratizing authoritarian states through economic means become difficult. Further, such a discussion is important in this context because the censorship of the internet and the use of propaganda to limit effective communications goes to the heart of the issue of limiting coordination goods.

Ying Ma notes that many instances where technology or other forces entered into China and the West assumed that China would liberalize. Instead, she notes, "Each time, however, China showed that it was determined to extract the economic or governing benefits of

[201] Ibid, 82.
[202] Ibid, 83.
[203] Ibid, 83-84.
[204] Ibid.

Liberalizing forces and instruments while stifling their political powers."[205] Ma argues that the effective stifling of coordination goods and the sustained economic growth are major factors in the resilience of Chinese authoritarianism.[206] Authoritarian resilience, a term coined by Andrew J. Nathan, will be more fully discussed in the next chapter. What seems clear is that the Chinese government has clear benefit in limiting certain aspects of the internet.

Part VII: Coordination Goods, Technology, and Politics in China

Lauri Paltemaa and Juha A. Vuori note that China has a long history of political use of technology, saying:

> "Since the Communist victory in the civil war in 1949, science and technology have been at the heart of socialist, and after 1978 what has increasingly become market socialist, construction in China. From the beginning of its reign, the CCP made the modernization of Chinese science and technology - and thereby achieving wealth, power and international status - one of its main goals."[207]

The authors especially reference the steel furnaces in backyards and the bizarre politically-driven, technically-unsound distortions, many of which led to famines and other problems throughout Communist China's history. However, regardless of this checkered past, the Chinese government has maintained their control and has adjusted their communication control strategies in more modern history. This is noted by the Post-Maoist shift of the Deng Xiaoping regime in China, of which the authors say:

> "In turn, the transition to the Dengist regime meant that there should be less restrictions and limits to the ways technology was to be developed and used, as well as more tolerance to technology's social impact. A social hierarchy based on expertise was now accepted, technological borrowing from the West became encouraged, and the masses' role in technological development was played down.

[205] Ying Ma (February and March 2007), "China's Stubborn Anti-Democracy," *Policy Review* (February and March 2007) *6.*

[206] Ibid.

[207] Lauri Paltemaa and Juha A. Vuori, "Regime Transition and the Chinese Politics of Technology: From Mass Science to the Controlled Internet," *Asian Journal of Political Science* 17, 1 (April 2009): 8.

> However, like before, technologies were not allowed to threaten the monopoly of the power of the CCP."[208]

Regarding the internet, the authors note that the introduction of the technology was initially state led.[209] They have a succinct discussion of the use of the internet and propaganda to support the Chinese regime.

> "From the point of view of post-totalitarian politics of technology, the manipulation of Internet technology is a means to a clear end. It is used as part of the protective belt around the systemic core. As demonstrated by firewalls, filters, pre- and post-facto censorship and the active promotion of the publication of approved online content, the aim is to create automated grids that channel user flows to 'safe' forums of communication and make transgression of the grids both difficult and susceptible to detection. Producing safe Internet content telling favourable stories of and about the regime is also an essential part of this policy, as in Aldous Huxley's Brave New World (1932), citizens are directed away from thinking or communicating harmful ideas by offering them harmless forms of activities for filling their lives through technologies that are thus designed." [210]

China is a great example of the use of media control and manipulation to block coordination goods. On top of reducing effective speech, the Chinese have instated a speech that limits the effectiveness of any speech that gets through the net. By marginalizing dissidents through agenda setting and censoring content, the Chinese government is effectively able to place itself in an advantageous position. Such positioning ability will likely exist until economic factors begin to encroach on the citizenry based on the control apparatus of the government or until other factors become too strong to ignore. In short, until the repression of the internet and other communications becomes an economic burden to the Chinese society, one must conclude that the Chinese will be able to maintain both their economic growth, through ties with the international community, and their repression of the rights of their citizens. Western arguments that economic engagement with the Chinese will lead to political liberalization fail to recognize

[208] Lauri Paltemaa and Juha A. Vuori, "Regime Transition and the Chinese Politics of Technology: From Mass Science to the Controlled Internet," *Asian Journal of Political Science* 17, 1 (April 2009): 12.

[209] Ibid, 13.

[210] Ibid, 15.

the neutralizing power of China's information control strategy. As such, they may actually be maintaining the superiority of the Chinese regime by allowing it to maintain a favorable economic climate in the country while still repressing rights. As such, Western strategy towards the country should likely be re-examined, although it is likely that little can be done to change this overall strategy, given the length of time it has been implemented. As such, new strategies may have to be implemented to limit the effectiveness of the Chinese government's strategies on these issues.

Part VIII: Conclusion

China implements a system in which the human rights of citizens are routinely violated. This includes a number of actions that physically violate the rights of dissidents and others. It also includes the censorship and repression of information, including information on the internet. Such measures are supplemented with a robust practice of information marginalization and propaganda that strengthens the Chinese government's position. All of this is justified with a Chinese version of Asian Values, which have been proposed as an effective counter to the Western meme of universalism. However, it must be noted that Asian values are not even consistent across the region or amongst its scholars and leaders, significantly weakening a supposedly cultural argument. Further, the overgeneralization of Asian Values as they have been presented makes one question their validity as an objective set of norms and not just a smoke screen for authoritarian regimes. China's actions related to human rights, censorship, and propaganda help one to understand the nature of coordination goods and their repression as a method to limit strategic coordination (something that would improve the ability of dissident groups to effectively take hold in China.) In short, the repression of communications and other coordination goods through the management and censorship of the internet and other means is important for the very survival of the Chinese regime. All of this discussion is important for the resilience of China’s state, something that will be discussed in greater detail in Chapter 5.

Chapter 5: China's Justifications and Authoritarian Resilience

So far, this thesis has focused on the actual instances of the Chinese government censoring the internet. However, what this thesis has yet to discuss is the reasoning of the Chinese government for censoring the internet. This chapter will posit that the Chinese government is censoring the internet to maintain the regime stability of the current, authoritarian system in China. In doing this, we will look at Andrew Nathan's discussion of authoritarian resilience. This argument will be balanced by a discussion of the potential security concerns that the internet can provide, looking at the terms hacktivism, electronic civil disobedience, network activism, and cyberterrorism. Thus, this chapter will show two competing ideas of the reasons why the internet is being censored in China. One will focus on the idea of regime stability and security. The other will focus on actual physical security. This chapter will argue that the notion of a physical security threat that is dangerous enough to warrant the level of censorship seen from the Chinese government is unrealistic. As such, this chapter will argue that any security arguments posed by the Chinese government or the Chinese Communist Party (CCP) are merely smoke screens for an effort to maintain regime stability and security.

Part I: Authoritarian Resilience and Chinese Censorship of the Internet

The notion of authoritarian resilience was posed by Andrew Nathan in relation to the Chinese government. The theory was originally brought up in the wake of the Tiananmen Square massacre and the international response. Nathan brought up the theory because the Chinese government, counter to what many in the international community were saying, failed to collapse under the weight of the outcry, both inside and outside China. Nathan notes:

> "Regime theory holds that authoritarian systems are inherently fragile because of weak legitimacy, overreliance on coercion, overcentralization of decision making, and the predominance of personal power over institutional norms. This particular authoritarian system, however, has proven resilient."[211]

Nathan's theory, as he puts it, focuses on four aspects of the CCP's continued stability. These four aspects are:

> "1) the increasingly norm-bound nature of its succession politics; 2) the increase in meritocratic as opposed to factional considerations in the promotion of political elites; 3) the differentiation and functional specialization of institutions within the regime; and 4) the establishment of institutions for political participation and appeal that strengthen the CCP's legitimacy among the public at large."[212]

Nathan notes that this is not an exclusive list. Further, he argues that these points, and others like them, "caution against too-hasty arguments that it (the Chinese government) cannot adapt and survive."[213] This is certainly bolstered by the presence of China's censorship and blocking of coordination goods.[214] Further, as noted by Ying Ma, such institutionalization has been coupled with spectacular GDP growth.[215] Ma also mentions the suppression and repression, of the Chinese government:

> "Of course, regime institutionalization alone cannot quell political discontent, dissent, or opposition, but this is where the effective suppression and cooptation of rival political groups come in. Beijing has brutally suppressed the spiritual group Falun Gong, a Buddhist sect that surprised and alarmed the regime by massing outside of its walled leadership compound in Beijing in a 10,000-strong silent protest on April 25, 1999. Similarly, the CCP has effectively cracked down on the China Democracy Party, which democracy activists in 1998 attempted to organize as the first national opposition party under communist rule."[216]

[211] Andrew Nathan, "China's Changing of the Guard: Authoritarian Resilience," *Journal of Democracy* 14, 1 (January 2003): 6.
[212] Ibid, 6-7.
[213] Ibid, 7.
[214] See Chapter 4 for a complete discussion of coordination goods.
[215] Ying Ma, "China's Stubborn Anti-Democracy," *Policy Review,* (February and March 2007): 7.
[216] Ibid, 8.

Ma also notes that the Chinese have co-opted those they can't repress:

> "Simultaneously, the CCP has keenly and successfully co-opted potential political competitors. According to Minxin Pei, the party has built coalitions with I) intellectuals, who were at the forefront of criticizing the regime in the 1980s and in leading the Tiananmen Democracy Movement of 1989; 2) private entrepreneurs, who comprise the emerging middle class that many believed would demand more rights as they acquired fuller stomachs; and 3) technocratic reformers, who focus on the changes necessary to institutionalize and modernize China's governance. By doling out everything from party membership to senior government positions to financial perks, the party has rendered moot the political threat from these three potent and potential opposition groups."[217]

Ma also brings in the discussion of coordination goods, linking the repression of such goods directly to "censoring the press and the Internet."[218]

The argument made by the scholars here is that the Chinese government is not sitting idly by while reformers and revolutionaries are working in their country. Further, this discussion serves to show that brutal repression is not the only tool in the arsenal of an authoritarian regime. The use of censorship and propaganda (while still repression) certainly is more appealing than mass torture, detention, and murder. Also, it is far easier to spin as for the security of the Chinese state; something the Chinese government has consistently focused on, painting those who would fight for democracy or freedom as separatists or terrorists. This is a topic we will examine further later on in this chapter. Also, moves like co-opting potential reformers and reforming the bureaucratic nature of the state are far more conciliatory than actions of brutality and violence. Thus, such a discussion of authoritarian resilience is important not just to show how the Chinese government attempts to control its population, but for understanding the modus operandi of modern authoritarian states.

[217] Ying Ma, "China's Stubborn Anti-Democracy," *Policy Review,* (February and March 2007): 8.
[218] Ibid.

Part II: Hacktivism, Electronic Civil Disobedience, Network Activism and Cyber Terrorism

The terms Hacktivism, Electronic Civil Disobedience, Network Activism, and Cyber Terrorism have often been confused. When examining Hacktivism or Electronic Civil Disobedience, this is not a huge issue, but when you include cyber terrorism, the issue becomes dangerous, as it allows for repressive regimes to lump peaceful activists with dangerous terrorists. These definitions are important to this chapter because the confusion around them helps to show the Chinese defense of their censorship regime and its potential for spin and misdirection. Basically, the presence of these terms and the confusion around them allows the Chinese government to claim their efforts at censorship are nothing more than an effort to protect their state. This section will seek to lay out succinct and delineated definitions of each term before moving on to the Chinese defense of their actions.

These terms are, according to Eric Novotny, part of the discussion that flows from the ideas of cyberconflict and cyberwarfare. Novotny notes that the terms cyberwarfare and cyberconflict are often used interchangeably, often to the detriment of the discussion at hand.[219] According to Novotny, cyberconflict is merely adding an electronic dimension to the general idea of conflict. As such, cyberconflict is the more general term, encompassing a series of activities that can be carried out online. However, cyberwarfare, as per Novotny, needs to meet the criteria of an actual war, in which physical infrastructure is damaged.[220] As such, the terms hacktivism, electronic civil disobedience, network activism, and cyberterrorism are bred out of the arena of cyberconflict and not cyberwarfare, given that these actions are largely not connected to the destruction of physical infrastructure.

[219] Dr. Eric Novotny, Interview with Joseph House, Washington, DC, February 16, 2011.

[220] Ibid.

Sub-Part I: Hacktivism

According to some, Hacktivism is more of a blanket term for actions such as electronic civil disobedience (ECD). According to Dorothy Denning:

> “Hacktivism is the convergence of hacking with activism, where Ahacking@ is used here to refer to operations that exploit computers in ways that are unusual and often illegal, typically with the help of special software (Ahacking tools@). Hacktivism includes electronic civil disobedience, which brings methods of civil disobedience to cyberspace.”[221]

However, such definitions are difficult because they also tend to include actions that are peaceful and violent; as well as actions that are done by individuals and by groups. Denning continues, “This section explores four types of operations: virtual sit-ins and blockades; automated e-mail bombs; Web hacks and computer break-ins; and computer viruses and worms.”[222]

Others, including Paul Taylor take a much more general definition for hacktivism. Taylor defines the term as “the combination of hacking techniques with political activism.”[223] Taylor argues this is the more political aspect of technological hacking.[224] Both Taylor and Denning include ECD tactics in their definition. However, this author thinks we need to investigate the lack of technical skill needed for ECD activities, as opposed to the higher skills needed for hacktivism. Further, we have to include the ethics of hacktivism that have actually been created and the nature of hacktivism as an individual action.

[221] Dorothy Denning, “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy,” *Computer Security Journal* (Summer 2000): 15.

[222] Ibid.

[223] Paul A. Taylor, “From hackers to hacktivists: speed bumps on the global superhighway?” *New Media and Society* vol. 7 (2005):626.

[224] Ibid.

Julie Thomas defines Hacktivism as “a policy of hacking, phreaking or creating technology to achieve a political or social goal.”[225] This definition does not include virtual sit-ins or other actions that would more appropriately be put into ECD. Further, Tomas also discusses a series of ethics related to hacktivism. However, even Thomas fails to separate the practices aligned with civil disobedience and those related to hacktivism. This author thinks that the consistent mixing of ECD with hacktivism is a mistake. The creative nature of the hacking used indicates that hacktivism is individual and more high tech than ECD. This is noted by Tatiana Bazzichelli, who writes:

> “Hacking is a creative practice; an irreverent and playful way of using computers which might also address an ethical and cooperative modality of relating to knowledge; activism indicates individual or collective action for achieving social goals and developing political battles.”[226]

This is also said well by Alexandra Samuel, who says:

> “Hacktivists use their knowledge of computer programming, network design, and Internet traffic to stage politically motivated disruptions on the Internet. These disruptions can take many forms, from “denial of service” (DoS) attacks that tie up web sites and other servers, to electronic graffiti that places political messages on government or corporate sites, to the theft and publication of private information on the Internet.”[227]

What can be seen by these definitions and discussions of hacktivism is that it is indeed the merging of hacking and activism. However, as opposed to ECD, discussed below, there is a much more individualized feeling in hacktivism. It is the idea of a technologically savvy lone wolf being able to infiltrate a massive company and do damage in a number of ways. ECD, on the other hand, is more about a large group (often with varying degrees of technical savvy)

[225] Julie Thomas, “Ethics of Hacktivism,” *GIAC Practical Repository* (2001): 1.

[226] Tatiana Bazzichelli, “On Hacktivist Pornography and Networked Porn (upcoming)” in the *Arse Elekotronika Catalogue*, edited by Monochrom (AT), Re/Search Publications, San Francisco (2010): http://www.tatianabazzichelli.com/PDF_files/Bazzichelli_Hacktivist_Pornography.pdf.

[227] Alexandra Samuel, “Decoding Hacktivism: Purpose, Method, and Identity in a New Social Movement,” paper presented at Innovations for an e-Society: Challenges for Technology Assessment conference, Berlin, Germany (2001): http://www.itas.fzk.de/eng/e-society/preprints/egovernance/Samuel.pdf.

banding together to make themselves known through technological means. Often, this is as simple as overloading a website and does not involve the technical skill or creativity of hacktivism. Those authors that have mixed these terms have confused these terms. Such confusion gives authoritarian countries, which are looking to stop all avenues of activism (as long as that activism is counter to the state's goals) a way to claim that one type of activism is akin to another. As hacktivism can contain more violent or destructive acts than ECD, mixing these terms gives authoritarian states the ability to restrain often peaceful ECD activities under the guise of security for their own state.

Sub Part II: ECD

ECD was a term coined in the early 1990s by the Critical Arts Ensemble (CAE):

> "These outdated methods of resistance [traditional civil disobedience] must be refined, and new methods of disruption invented that attack power (non)centers on the electronic level. The strategy and tactics of CD can still be useful beyond local actions, but only if they are used to block the flow of information rather than the flow of personnel."[228]

The term is based in the theory of civil disobedience as promoted by Thoreau, Gandhi, and King. Activities that would fall under this definition include sit-ins and other activities popularized by the civil rights movement and other political movements. The only difference with ECD is the addition of technology. It is also clear that, as opposed to hacktivism, ECD is a more group activity.

The term was further defined by the breakaway group, Electronic Disturbance Theatre (EDT), which argued that the sit-ins and other activities should be advertised and conducted in public.[229] Further, the development of FloodNet, which simplified these actions, opened up the

[228] Critical Arts Ensemble, *Electronic Civil Disobedience,* Autonomedia, Brooklyn, NY (1996): 9.
[229] Graham Meikle, "Electronic Civil Disobedience and Symbolic Power," *Cyber Conflict and Global Politics,* Athina Karatzogianni (ed.), Routledge, New York (2009): 180.

actions to the public and made ECD a more group activity. Further, the lack of technical expertise, since the program was developed by a few with technical expertise and given to the layman masses, shows a difference between Hacktivism and ECD.[230] This is furthered by the lack of deeper hacking, as much of the blocking of sites is done through large numbers.[231] The idea of an elegant solution (proposed in the original definition of a "Hack"[232]) matches with the idea of art brought up in ECD. However, the large numbers discussion of ECD does not match with this.

Given the split between CAE and EDT over the idea of whether or not actions should be public and large in scope, we can divide ECD into two models, the CAE Model and the EDT Model. From this we can see why some have confused hacktivism and ECD. The CAE Model, characterized by technical skill and keeping their actions private, lends itself to the notions put forth under hacktivism. The EDT Model seems to be more in line with the definition of ECD that this author is promoting. Authors must show more constraint in their willingness to mix the definitions of ECD and hacktivism. Adopting more nuanced typologies, like the ones shown below, would help to reduce confusion and prevent overgeneralizations that can aid dictators and authoritarian regimes who seek to make those engaging in civil disobedience into rebels or threats

.

[230] Graham Meikle, "Electronic Civil Disobedience and Symbolic Power," in *Cyber Conflict and Global Politics,* ed. Athina Karatzogianni, (New York: Routledge, 2009), 180.

[231] Stefan Wray, "Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics," *Switch* 4, 2: http://switch.sjsu.edu/web/v4n2/stefan/.

[232] Graham Meikle, "Electronic Civil Disobedience and Symbolic Power," in *Cyber Conflict and Global Politics,* ed. Athina Karatzogianni, (New York: Routledge, 2009), 180-83.

Figure 5. Breakdown of ECD

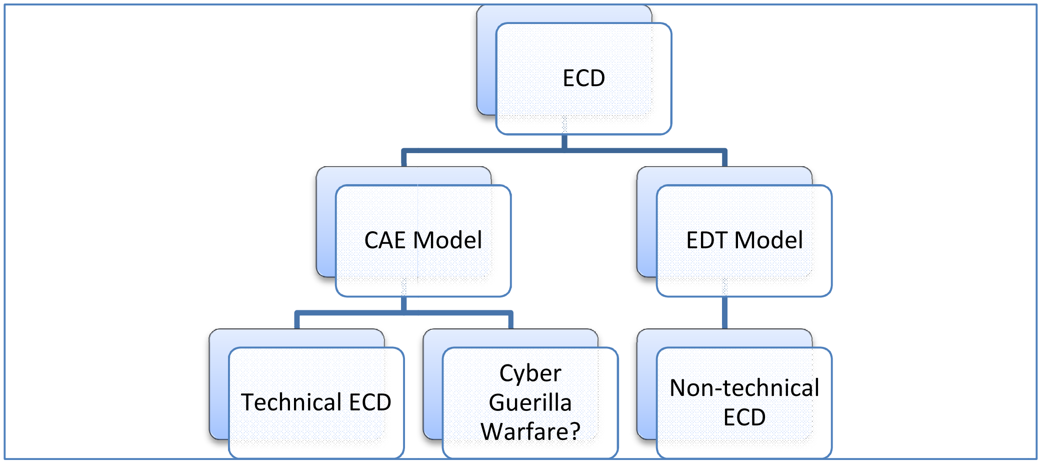
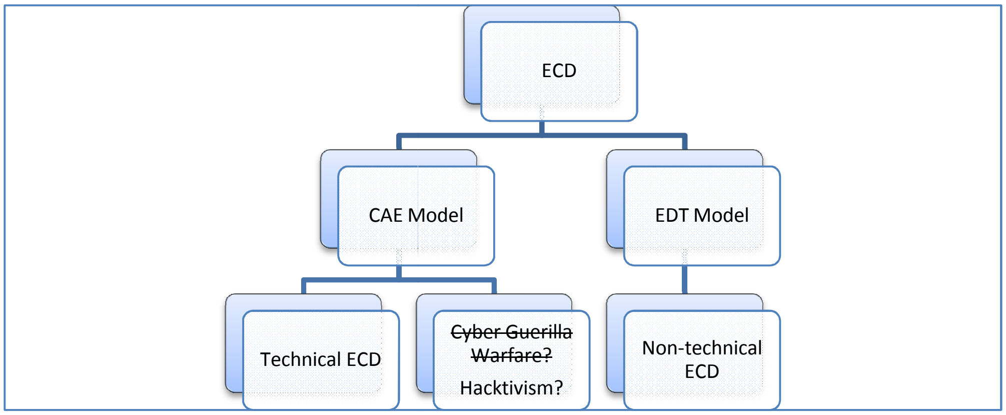


Figure 6. Revised Breakdown of ECD, Showing the Confusion with Hacktivism



Sub-Part III: Network Activism

Network activism, also called web activism, is a term that is much more benign in nature than that of electronic civil disobedience. Quite simply, it is the use of the internet and global communications to supersede the mainstream media and give sovereignty to groups that would normally lack sovereignty in the international sphere.[233] (Michael Dartnell, "Web Activism as an Element of Global Security," The idea, according to Michael Dartnell, is to promote a point of view regarding a specific issue. According to Meikle, as cited by Dartnell, an important aspect is

[233] Michael Dartnell, "Web Activism as an Element of Global Security," in *Cyber Conflict and Global Politics*, ed. Athina Karatzogianni, (New York: Routledge, 2009), 64.

raising awareness for specific issues. In this context, Meikle cites EDT and the use of ECD as a form of web activism.[234]

Activism often takes the form of civil disobedience and, thus, electronic activism could easily take the form of electronic civil disobedience. However, we must note that the important difference between network activism and ECD is in scope. Network activism is far more focused on a macro-level goal, the dissemination of a message. ECD, hacktivism, and other tactics used by those who may engage in network activism campaigns are merely tactics. Further, network activism in a general sense can include far more peaceful measures than hacktivism or ECD. These measures, according to Dorothy Denning, could include activities that are as everyday as searching for information on the internet or sending e-mails on a particular issue.[235] Much emphasis is put on the idea of being able to locate and collect information. John Naughton, in his article, "Contested Spaces: The Internet and Global Society," talks about how the internet can allow for people to collect and disseminate information to one another, allowing for people to compare policies and confer with one another on global issues.[236]

Denning draws the line for activism at activities that engage in hacking without causing any significant damage. Thus, actions under the heading of ECD would not fall into this category.[237] According to Denning:

[234] Michael Dartnell, "Web Activism as an Element of Global Security," in *Cyber Conflict and Global Politics*, ed. Athina Karatzogianni, (New York: Routledge, 2009), 64.
[235] Dorothy Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," *Computer Security Journal* (Summer 2000): 2.
[236] John Naughton, "Contested Space: The Internet and Global Civil Society," *LSE Yearbook 2001: Global Civil Society*, 147.
[237] Dorothy Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," *Computer Security Journal* (Summer 2000): 2.

> “It [internet activism] facilitates activities such as educating the public and media, raising money, forming coalitions across geographical boundaries, distributing petitions and action alerts, and planning and coordinating events on a regional or international level. It allows activists in politically repressive states to evade government censors and monitors.”[238]

What can be derived from the discussion of network activism is that there are also a number of other, benign activities that can be engaged in online that can aid organizations and groups seeking to better their situation. Merely disseminating information is important. This ties nicely to the discussion of coordination goods in Chapter 4. Further, this goes to show that the Chinese censorship model, which goes to extreme lengths to block information, is also hindering this peaceful practice, further undermining their claims that their technological actions are in place to stop those who would do the country harm.

Sub-Part IV: Cyberterrorism

The next topic that must be discussed is the idea of cyberterrorism. As a concept, cyberterrorism has gotten a lot of play. Indeed, it is the very essence of what the Chinese government would seem to be afraid of if it were truly trying to protect its security with its censorship regime. However, the actuality of cyberterrorism has yet to match the theoretical danger that is consistently put forth. According to Gabriel Weimann, “The potential threat is, indeed, very alarming. And yet, despite all the gloomy predictions, no single instance of real cyberterrorism has been recorded.”[239] According to Novotny, terrorists may well be using the internet for financing, communications, and other activities. However, they are not very likely to be engaging in activities to destroy or damage networks, because it hurts their individual actions

[238] Dorothy Denning, “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy,” *Computer Security Journal* (Summer 2000): 26.

[239] Gabriel Weimann, “Cyberterrorism: How Real is the Threat?” *United States Institute of Peace Special Report* 119 (May 2004): 1.

and because they view a working internet as more valuable than an internet that has been knocked out, particularly given the lack of drama inherent in such attacks.[240]

Further, it would seem China would actually be more insulated from the threat of cyberterrorism, even if there were reported cases of the phenomenon. Given the country's relatively low amount of networking, especially in rural areas, one would conclude that the threat of cyberterrorism is far more acute in Western societies. Weimann notes this, saying:

> "Because most critical infrastructure in Western societies is networked through computers, the potential threat from cyberterrorism is, to be sure, very alarming. Hackers, although not motivated by the same goals that inspire terrorists, have demonstrated that individuals can gain access to sensitive information and to the operation of crucial services. Terrorists, at least in theory, could thus follow the hackers' lead and then, having broken into government and private computer systems, cripple or at least disable the military, financial, and service sectors of advanced economies."[241]

As such, we have to view the threat of cyberterrorism as real. However, not all articulations of the threat are real. As such, not all items justified by this threat will be real either. We must question the logic and reasoning of the Chinese, given that they are using the threat of cyberterrorism to justify a wide swath of censorship that would seem to expand well beyond the scope of cyberterrorism. Further, we must be cautious regarding all threats or concerns about cyberterrorism. Again, quoting Weimann:

[240] Dr. Eric Novotny, Interview with author, 16 February 2011, Washington, DC.

[241] Gabriel Weimann, "Cyberterrorism: How Real is the Threat?" *United States Institute of Peace Special Report* 119 (May 2004): 2.

> "Concern about the potential danger posed by cyberterrorism is thus well founded. That does not mean, however, that all the fears that have been voiced in the media, in Congress, and in other public forums are rational and reasonable. Some fears are simply unjustified, while others are highly exaggerated. In addition, the distinction between the potential and the actual damage inflicted by cyberterrorists has too often been ignored, and the relatively benign activities of most hackers have been conflated with the specter of pure cyberterrorism."[242]

In short, we must be careful to not allow anyone to lump activists in with radicals in an attempt to paint any dissident with a single brush stroke. We must remember that activists are not necessarily violent and that the actions of activism can take a wide array of forms. These various forms may be benign or violent. However, we must caution against poorly defined terms that are too general and allow for benign and beneficial activities to be combined with violent and destructive activities.

Part III: China's Security Concerns

China has at times argued that it is has engaged in the technological activities that it has engaged in largely because of security concerns. According to a 2010 statement by the Chinese government, "Online information which incites subversion of state power, violence and terrorism or includes pornographic contents are explicitly prohibited in the laws and regulations."[243] Such a general statement would indicate that the Chinese government is engaging in censorship activities as a means to stifle potential threats to its state, particularly physical threats, given the references to subversion of the state and terrorism. However, we must caution ourselves from accepting China's generalizations on face value. China has often called peaceful ideals and leaders "terrorists" or those who are "subverting state power." For proof of this, one only needs to look at the Chinese descriptions of the Dalai Lama. In 2008, China said that the Dalai Lama

[242] Gabriel Weimann, "Cyberterrorism: How Real is the Threat?" *United States Institute of Peace Special Report* 119 (May 2004): 2.

[243] "China says Internet regulation legitimate and reasonable," Gov.cn: Chinese Government's Official Web Portal, 25 January 2010; accessed 3 April 2011: http://english.gov.cn/2010-01/25/content_1518404.htm.

was working with Muslim terrorists to destabilize the country in the run up to the Beijing Olympics.[244] They also accused the leader of organizing violent protests in March 2008 and Tibetans of preparing for suicide bombings in the months before the 2008 Olympic Games.[245] These claims have never been promoted by other sources and the Australian Prime Minister Kevin Rudd even contradicted the Chinese in the run up to a state visit to the country.[246]

China's continued reliance on deeming anyone who disagrees with the party line as a terrorist or a subversive does more than discredit their argument that their internet censorship is meant to protect their nation. It further promotes the idea that the country is looking to improve its regime stability, given that many of the targets of their accusations disagree with the Chinese government on important political questions. Further, the Chinese seem to be initiating the same overreaction to benign uses of the internet (finding information and other peaceful activities) as they do with peaceful individuals (the Dalai Lama and Tibetan monks, for example). As such, their security argument is further discredited. Novotny notes that the use of internet activities against certain actors (particularly in those areas that are not effectively connected to online technology) is relatively useless, given the lack of connection to the internet exhibited in daily life. Novotny uses the example of the United States striking back at the North Korean state with a cyber attack in the aftermath of a cyber attack launched by the North Koreans. Because North Korea is much less connected to the internet or, as Novotny puts it, "there is no cyberspace in North Korea," such a cyber attack is useless.[247] A similar argument can be made regarding China and censorship of the internet. If so little of the conflict areas are effectively connected to the

[244] Jane McCartney, "China Accuses Dalai Lama of Being a Terrorist," *The Sunday Times (UK)*, 24 March 2008; accessed 3 April 2011: http://www.timesonline.co.uk/tol/news/world/asia/article3607668.ece.

[245] Mary-Anne Troy, "Dalai Lama a Terrorist: China," *The Sydney Morning Herald (AU)*, 3 April 2008: http://www.smh.com.au/news/world/dalai-lama-a-terrorist-china/2008/04/02/1206851012042.html.

[246] Ibid.

[247] Dr. Eric Novotny, Interview with Joseph House, Washington, DC, 16 February 2011.

internet, then why does Chinese internet censorship protect security? This is noted by Ben Carrdus and Royce Priem of the International Campaign for Tibet who note that the internet in Tibet is very rudimentary and extremely controlled. This is so extensive that any attempt to use the internet by Tibetan dissidents would be relatively fruitless as a strategy against the Chinese government.[248] The security argument made by the Chinese government is overblown and a smokescreen for their real intentions, limiting communications as a way of controlling the agenda and creating an environment in which their regime, not the country at large, is safe.

Conclusion

The Chinese government is motivated by a desire to protect their regime, not their citizenry and country, when it censors the internet. This is borne out by the illogical nature of their statements on why they are censoring the internet. Further, the government's attempts at censoring the internet and, as such, blocking coordination goods, serve as a way to fulfill Andrew Nathan's theory on authoritarian resilience, as articulated by both Nathan and Ying Ma. The actions taken, coupled with China's strong economic growth have allowed for a system in which the Chinese government is able to maintain power while repressing the rights of its citizens, even if the reasons provided are ridiculous.

[248] Ben Carrdus and Royce Priem, interview with Joseph House, Washington, DC, March 9, 2011.

Chapter 6: Conclusion

China has continually expanded its physical telecommunications infrastructure and has implemented numerous methods of both direct and indirect control on that infrastructure. The aim of these methods has been to control the use and content on the networks that use this infrastructure. China has evolved its censorship and regulation structures over the years from basic filtering to a structure which controls the system in a general sense and prevents information from becoming politically damaging. This is done both through the blocking of information and the discrediting of information through propaganda and other measures. Further, the government has become more reliant on self-censorship to accomplish its goals. Any discussion of this topic that solely focuses on internet censorship in China, without talking about other efforts of the government to control the narrative of political and sensitive information on the internet is flawed. In short, China's efforts regarding the internet are not merely a matter of blocking the internet. Instead, their efforts indicate a concerted effort to control, and not merely, deny information.

China implements a system in which the human rights of citizens are routinely violated. This includes a number of actions that physically violate the rights of dissidents and others. It also includes the censorship and repression of information, including information on the internet. Such measures are supplemented with a robust practice of information marginalization and propaganda that strengthens the Chinese government's position. All of this is justified by a Chinese version of Asian Values, which have been proposed as an effective counter to the notion of universal rights and values, which is popular in the West. However, it must be noted that Asian values are not even consistent across the region or amongst its scholars and leaders, significantly weakening a supposedly cultural argument. Further, the overgeneralization of Asian

Values as they have been presented makes one question their validity as an objective set of norms and not just a smoke screen for authoritarian regimes. The Chinese system provides a great example of coordination goods and their repression as a method to limit strategic coordination (something that would improve the ability of dissident groups to effectively take hold in China.) In short, the repression of communications and other coordination goods through the management and censorship of the internet and other means is important for the very survival of the Chinese regime.

The presence of a large number of MNCs in the Chinese market makes the issues of censorship in China difficult to untangle. The Shi Tao case and others like it show the situations that MNCs are often put in when they enter the Chinese market, given the rules and regulations that Yahoo! was required to sign onto, along with the need for the company to join with Alibaba. The Google case further shows these issues, showing the tense relationship that can develop between company and government, especially in the case of a company that has a low market share and is the target of numerous incidents of government harassment (perceived or otherwise). These cases are all further complicated by the presence of companies like Narus, which are staffed by former government officials. All of these dilemmas make it difficult to promote an effective legal or norm based regime from the international community. Current solutions and proposed solutions have been shown to suffer from two major problems, either being overly generalized and unenforceable or lacking in the political will to be effectively passed and implemented.

The Chinese government is motivated by a desire to protect their regime, not their citizenry and country, when it censors the internet. This is borne out by the illogical nature of their statements on why they are censoring the internet. Further, the government’s attempts at censoring the internet and, as such, blocking coordination goods, serve as a way to fulfill Andrew Nathan's theory on authoritarian resilience, as articulated by both Nathan and Ying Ma. The actions taken, coupled with China's strong economic growth have allowed for a system in which the Chinese government is able to maintain power while repressing the rights of its citizens, even if the reasons provided are ridiculous.

In China, the democratizing power of the internet is unclear, if not in serious doubt. Merely having people connected through social networking is likely not enough to change a regime that is as interested in the control of information as it is in the censorship of it. As such, Gladwell may have a point when he emphasizes the need for strong connections between activists, which are often fostered through direct, close connection – as opposed to the weak connections fostered through acquaintances on social networking sites.[249] However, it is important to note the fact that it is not only dissidents that can use the internet to gain advantage in a given country or situation. As can be seen by the close relations between the Chinese government and several companies, including Narus, internet technologies can be used by the Chinese government to track and even repress citizens that seek to revolt or rebel against their government. Thus, it is important to look at the usage of internet technologies in China with a wary eye. If we are truly to follow the cyber-realist framework, then we must recognize that China has the ability to control the internet just as much as its citizens have the ability to use it. Continually thinking that the internet gives the citizens in a given country the upper hand is utopian and foolish. Hence, there is a need to continue to extensively study China's internet censorship behaviors if we are to truly understand the impact of the internet in the Chinese system.

[249] Malcolm Gladwell, "Small Change," The New Yorker, 4 October 2010, accessed 29 January 2011: http://www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell?currentPage=all.

While it may be possible to use the internet to aid in democratization in certain contexts, this author would argue that the internet cannot be used alone in the pursuit of democratization. There needs to be ample political will on the ground, in the form of an existing group fighting for democratization. These strong connections can then be aided by the internet in their cause. Further, the technologies and networking activities used should be used strategically and sparingly, given their potential to backfire and work against dissidents, particularly in a more complex system. Governments, like China, which seek to control information, rather than merely suppress it, may indeed be at a greater advantage than other authoritarian regimes, a line of inquiry that bears greater study. Because of these issues, the relations between governments and multinational corporations regarding the internet comes into sharp relief. As such, we can see numerous ties to the discussion in Chapter 3 regarding multinational corporations and the Chinese government. This thesis must stress that nuance and caution are taken when looking at the democratizing power of the internet. An instrumental view of the internet is likely a bad idea, given the issues that have been uncovered by Gladwell and Morozov. Indeed, the best policy proposal might be for governments to put less emphasis on getting information technologies into the hands of dissidents and more emphasis on keeping companies that are working in authoritarian state from providing dictators with the tools of virtual repression. Further, future policy proposals must focus on the idea of context. Policy proposals must be informed by the actions of a particular state. Ill-informed policy proposals that are utopian in nature may, in many cases, put the dissidents in a particular country at risk.

Measures taken by Western countries must acknowledge these shifting and, at times, contradictory and confusing issues. Western countries must recognize the impact of the Chinese system and the impact of the numerous multinational corporations in the country. However, policy makers must also note that the promotion of internet freedom alone cannot effectively crush an effective regime for information control, such as the one implemented in China. Until the full scope of Chinese policy is recognized, with its focus on propaganda, agenda setting, self-censorship and other avenues, no effective policy can be designed. Rather, policies designed without this level of focus are destined to miss out of key elements of Chinese strategy and posit theories and policies that do nothing to impede the Chinese government or, worse yet, empower the regime to be bolder. Such failures can be seen in the Global Compact and the Global Online Freedom Act, which have been ineffective or stuck in bureaucracy because the policymakers who put forth these respective pieces of legislation failed to look at the full scope of the argument.

It is clear that the role of the internet in the Chinese context is not yet understood. Policy proposals made with the current understanding of the Chinese situation are at a very high risk of seeming utopian and incomplete, preventing the policies from being effective and, possibly, even making them counterproductive. It is imperative that a more thoughtful study of the Chinese internet context be conducted. Without a deep and complete knowledge, policy provisions will be impossible. Any such study must include a) a study of the history of the Chinese political system, with special focus on the Chinese government's role in communication issues; b) a study of the external factors that play into the Chinese context (MNCs); and c) a discussion of China's activities to both censor and use communications as a means to control its population. Further, any such study of the technological context in China must acknowledge that the internet is a tool for communication and coordination and not a silver bullet. Future studies must resist the utopian treatment that has been previously given to this topic. Given the extremely nuanced and adapting censorship and propaganda regimes in China, this author would argue that no simple policy prescription regarding China and the internet can be made. Human rights groups should continue activities to “name, blame, and shame” the Chinese government and the companies that have worked with the Chinese government, but proactive action runs too high a risk of being counterproductive, but governments should resist the temptation to provide internet technologies as a means to promote democratization in China. Indeed, China may not be a country fit for the Google Doctrine. This author would go so far as to argue that, given the nature of the Chinese system of information control, with its limited international access points, use of both propaganda and censorship, and large role of technologically advanced multinational corporations, that freeing the internet would likely come after democratization in China, not lead to it.

References

"A New Approach to China." (12 January 2010). The Official Google Blog: http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

"A New Approach to China – An Update." (22 March 2010). The Official Google Blog: http://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html.

"Article 35." *Constitution of the People's Republic of China.* Adopted on 04 December 1982. As published by The People's Daily: http://english.peopledaily.com.cn/constitution/constitution.html.

Bazzichelli, Tatiana. "On Hacktivist Pornography and Networked Porn (upcoming)." In the *Arse Elekotronika Catalogue*, edited by Monochrom (AT), Re/Search Publications, San Francisco (2010): http://www.tatianabazzichelli.com/PDF_files/Bazzichelli_Hacktivist_Pornography.pdf.

Boas, Taylor C. "Weaving the Authoritarian Web: The Control of Internet Use in Non-Democratic Regimes." in *How Revolutionary was the Digital Revolution,* edited by Zysman and Newman. Stanford, CA: Stanford Business Books, 2000.

Bueno de Mesquina , Bruce and George Downs. "Development and Democracy." *Foreign Policy* 84, 5 (September-October 2005).

Carrdus, Ben and Royce Priem. Interview with Joseph House. Washington, DC. March 9, 2011.

"China Internet Population Hits 384 Million." Reuters, 15 January 2010.

"China says Internet regulation legitimate and reasonable." Gov.cn: Chinese Government's Official Web Portal. 25 January 2010. Accessed 3 April 2011: http://english.gov.cn/2010-01/25/content_1518404.htm.

Congressional-Executive Commission on China. "The Impact of the 2008 Olympics on Human Rights and the Rule of Law in China." 110th Congress, 2nd Session. 27 February 2008.

Critical Arts Ensemble. *Electronic Civil Disobedience.* Autonomedia. Brooklyn, NY (1996).

Dartnell, Michael. "Web Activism as an Element of Global Security." in *Cyber Conflict and Global Politics,* edited by Athina Karatzogianni, (New York: Routledge, 2009).

Damm, Jens and Simona Thomas, ed. *Chinese Cyberspaces: Technological Changes and Political Effects*. New York: Routlege, 2006.

Deibert, Ronald. "China's Cyberspace Control Strategy: An Overview and Consideration of Issues for Canadian Policy." Canadian International Council China Papers 7 (2010).

Deibert, Ronald and Nart Villeneueve. “Firewalls and Power: An Overview of Global State Censorship of the Internet.” in *Human Rights in the Digital Age*, ed. Mathias Klang and Andrew Murray. (New York: Routledge Cavendish, 2005).

Denning, Dorothy. “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy.” *Computer Security Journal* (Summer 2000).

Deva, Surya. “Corporate Complicity in Internet Censorship in China: Who Cares for the Global Compact or the Global Online Freedom Act?” George Washington Law Review 39, 2 (2007).

Esler, Brian W. “Filtering, Blocking and Rating: Chaperones or Censorship.” in *Human Rights in the Digital Age*, ed. Mathias Klang and Andrew Murray. (New York: Routledge Cavendish, 2005).

Fallows, James. “China’s Internet Censorship is Effective.” in Censorship: Opposing Viewpoints, ed. Scott Barbour. (Farmington Hills, MI: Greenhaven Press, 2010).

Fewsmith, Joseph. “Feedback without Pushback? “Innovations in Local Governance.” Statement to Congressional-Executive Commission on China. “Political Change in China? Public Participation and Local Governance Reforms.” May 15, 2006.

Gawlikowski, Krzysztof. “Asian Values’ and Western Universalism.” *Dialogue and Universalism* 10, 1-2 (2000).

Gladwell, Malcolm. “Small Change.” The New Yorker. 4 October 2010. Accessed 29 January 2011: http://www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell?currentPage=all.

“Google’s Hong Kong Question Page Blocked in China.” Reuters. 3 August 2010: http://www.reuters.com/article/2010/08/03/us-google-china-idUSTRE6720HN20100803.

“Government – Intelligence.” Narus. http://www.narus.com/index.php/industries/government-intelligence.

Gu, April. “China’s Internet Censorship can be Circumvented.” in Censorship: Opposing Viewpoints, ed. Scott Barbour. (Farmington Hills, MI: Greenhaven Press, 2010).

“Guaranteeing Citizens' Freedom of Speech on the Internet.” *Chinese White Paper on the Internet*. 08 June 2010. Accessed 26 March 2011: http://www.gov.cn/english/2010-06/08/content_1622956_5.htm.

Harwit, Eric and Duncan Clark, “Government Policy and Political Control over China’s Internet.” in *Chinese Cyberspaces: Technological Changes and Political Effects*, edited by Jens Damm and Simona Thomas. New York: Routlege, 2006.

His Holiness the Dalai Lama. “Buddhism, Asian Values, and Democracy.” *Journal of Democracy* 10, 1 (1999).

Hisao, Russell. “China’s Cyber Command?” China Brief 10, 15 (July 22, 2010).

Hughes, Christopher. “Fighting the Smokeless War: ICTs and International Security.” in LSE Research Online, http://eprints.lse.ac.uk/9641/.

________________. “Fighting the Smokeless War: ICTs and International Security.” in China and the Internet: Politics of the Digital Leap Forward, ed. Christopher R. Hughes and Gudrun Wacker. (London: Routlege, 2003).

Information Warfare Monitor. “Tracking GhostNet: Investigating a Cyber Espionage Network.” Information Warfare Monitor (2009).

Karr, Timothy. “One U.S. Corporation's Role in Egypt's Brutal Crackdown.” The Huffington Post. 29 January 2011.

Koh, Tommy. “The Ten Values That Undergird Asian Strength and Success.” *The New York Times*. 11 December 1993. Accessed 08 September 2009: http://www.nytimes.com/1993/12/11/opinion/11iht-edkoh.htm.

Kurlantzick, Joshua. “The Dragon Still Has Teeth: How the West Winks at Chinese Repression.” *World Policy Journal* XX, 1 (Spring 2003).

Ma, Ying. “China’s Stubborn Anti-Democracy.” *Policy Review* (February and March 2007).

Magnarella, Paul J. “Communist Chinese and ‘Asian Values’ Critiques of Universal Human Rights.” *Journal of Third World Studies* XXI, 2 (2004).

McCartney, Jane. “China Accuses Dalai Lama of Being a Terrorist.” *The Sunday Times (UK)*, 24 March 2008; accessed 3 April 2011: http://www.timesonline.co.uk/tol/news/world/asia/article3607668.ece.

Meikle, Graham. “Electronic Civil Disobedience and Symbolic Power.” in *Cyber Conflict and Global Politics,* edited by Athina Karatzogianni, (New York: Routledge, 2009).

Mirsky, Jonathan. “US Companies are Abetting Internet Censorship in China.” in *Censorship: Opposing Viewpoints,* edited by Scott Barbour. (Farmington Hills, MI: Greenhaven Press, 2010).

Morozov, Evgeny. ”Is Hillary Clinton Launching a Cyber Cold War?” Foreign Policy. 21 January 2010: http://neteffect.foreignpolicy.com/posts/2010/01/21/cyber_cold_war.

_______________. *The Net Delusion: The Dark Side of Internet Freedom*. New York, PublicAffairs, 2011.

_______________. “Try Different Keywords.” The New York Times. 16 January 2010.

Nathan, Andrew J. “China’s Changing of the Guard: Authoritarian Resilience.” *Journal of Democracy* 14, 1 (January 2003).

Naughton, John, “Contested Space: The Internet and Global Civil Society.” *LSE Yearbook 2001: Global Civil Society*.

Novotny, Eric. interview with Joseph House. Washington, DC. 11 February 2011.

Paltemaa, Lauri and Juha A. Vuori. “Regime Transition and the Chinese Politics of Technology: From Mass Science to the Controlled Internet.” *Asian Journal of Political Science* 17, 1 (April 2009).

Peters, Robert. “China, Democracy, and the Internet,” in *Information Technology and World Politics*, edited by Michael J. Mazaar. New York: Palgrave MacMillan, 2002.

“PLA sets up cyber base, assures it's not for war,” The Times of India. July 23, 2010.

Priem, Royce. Interview by Joseph House. Washington, DC. 9 March 2011.

Qiu, Jack Linchaun. *Working-Class Network Society: Communications and the Information Have-Nots in Urban China.* Cambridge, MA: The MIT Press, 2009.

Samuel, Alexandra. “Decoding Hacktivism: Purpose, Method, and Identity in a New Social Movement.” Paper presented at Innovations for an e-Society: Challenges for Technology Assessment Conference, Berlin, Germany (2001): http://www.itas.fzk.de/eng/e-society/preprints/egovernance/Samuel.pdf.

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

Shirky, Clay. “The Political Power of Social Media,” Foreign Affairs 90, 1 (2011).

Stewart, Potter. Consenting Opinion. Jacobellis v. Ohio. 378 US 174 (1964).

Taylor, Paul A. “From hackers to hacktivists: speed bumps on the global superhighway?” *New Media and Society* vol. 7 (2005).

"The 10 Principles." The United Nations Global Compact: http://www.unglobalcompact.org/AboutTheGC/TheTenPrinciples/index.html.

Thomas, Julie "Ethics of Hacktivism." *GIAC Practical Repository* (2001).

Troy, Mary-Ann "Dalai Lama a Terrorist: China." *The Sydney Morning Herald (AU)*, 3 April 2008: http://www.smh.com.au/news/world/dalai-lama-a-terrorist-china/2008/04/02/1206851012042.html.

U.S. Congress. House of Representatives. Committee on International Relations. "The Internet in China: A Tool for Freedom or Suppression?" 109th Congress, 2nd Session. 15 February 2006.

U.S. Congress. House of Representatives. Committee on Foreign Affairs. "Yahoo! Inc.'s Provision of False Information to Congress." 110th Congress, 1st Session. 6 November 2007.

US-China Economic and Security Commission. "China's Domestic Internet Activities." *Annual Report to Congress 2010*. Chapter 5, Section 1.

Watts, Jonathan. "How Internet Giant Google Turned on Gatekeepers of China's Great Firewall." The Guardian. 14 January 2010.

Wacker, Gudrun. "The Internet and Censorship in China." in China and the Internet: Politics of the Digital Leap Forward, ed. Christopher R. Hughes and Gudrun Wacker. (London: Routlege, 2003).

Weinberger, David. "The Internet as a Human Right." *Joho the Blog.* Published 19 September 2010. accessed 24 September 2010: http://www.hyperorg.com/blogger/2010/09/19/the-internet-as-a-human-right/.

Weimann, Gabriel. "Cyberterrorism: How Real is the Threat?" *United States Institute of Peace Special Report* 119 (May 2004): 1.

Woesler, Martin. "Internet Censorship Focus: Human Rights Not Found." in China's Digital Divide: The Impact of the Internet on Chinese Society, ed. Zhang Junhua and Martin Woesler. (Berlin: European University Press, 2004).

Wray, Stefan. "Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics." *Switch* 4, 2: http://switch.sjsu.edu/web/v4n2/stefan/.

Yeung, C.A. "Internet Human Rights Declaration." *Under the Jacada Tree Blog*. Published 08 October 2009. accessed May 30, 2010: http://underthejacaranda.wordpress.com/2009/10/08/internet-human-rights-declaration/.

Zhao, Yuezhi. *Communication in China: Political Economy, Power, and Conflict*. Lanham, MD: Rowan & Littlefield Publishers, 2008.