TIERED TECHNOLOGIES OF POWER: SUBJECT-MAKING IN CHINA THROUGH ELECTRONIC CENSORSHIP

Hope Reidun St. John
Urban Studies & Global Studies
May 2014

Faculty Adviser: Dr. Lisa Hoffman

Essay completed in partial fulfillment of the requirements for graduation with Global Honors, University of Washington, Tacoma.

TIERED TECHNOLOGIES OF POWER: SUBJECT-MAKING IN CHINA THROUGH ELECTRONIC CENSORSHIP

Hope Reidun St. John
Urban Studies & Global Studies
May 2014

Faculty Adviser: Dr. Lisa Hoffman

Essay completed in partial fulfillment of the requirements for graduation with Global Honors, University of Washington, Tacoma.

Approved:

_____ _____
Faculty Adviser Date

_____ _____
Director, Global Honors Date

It is an overcast Wednesday in late August 2013 in Fort Meade, Maryland when Bradley Manning, a 25-year-old private first class in the U.S Army, is sentenced to 35 years in federal prison (Serrano, 2013). His charge is espionage, a crime he was found guilty of after revealing state secrets through the notorious website WikiLeaks (Serrano, 2013). A few days later in Yinchuan, China, activist Shi Tao, imprisoned for a similar crime of divulging "state secrets" in an online internet forum, is released after serving eight years of a ten year sentence (Gough, 2013). In the wake of the "information age," the internet has become a powerful global platform through which dissidents such as Shi Tao and whistleblowers such as Manning can challenge the authority and legitimacy of the state. As a result of these emergent threats, both democratic and authoritarian regimes have been placed under greater pressure to develop new controls that mitigate the threat while preserving the internet as a social and economic space. In the context of the People's Republic of China, these controls have emerged in the form of systems of electronic censorship, based on the combination of technological, institutional, and internal regulation. Within the context of the expansion of the internet as a global network, the development of electronic censorship systems are pertinent both in terms of the questions they raise and the transformations they reveal about shifting modes of governing and subject formation in an increasingly global, decentralized society.

As the case of Bradley Manning illustrates, the global communicative capacities of the internet make it a potential danger to governing bodies, both democratic and non-democratic (Serrano, 2013). However, while the internet can be destabilizing at a political level, it can also afford connective possibilities that enable sharing of all manner of content, an increasingly pertinent capability as China continues to lead the world as the nation with the most internet users (over 600 million in 2013) — a position it has held since 2008 (CNNIC, 2012). Yet, as

China continues to develop, the internet also represents an important and emerging economic frontier, making the technology a simultaneously valuable asset and governmental challenge. New internet-based phenomena of resistance illustrate how symbolism and discontent can become potent and volatile mixtures that, when disseminated through the speed and breadth of the internet, can become movements. As such, it is unsurprising that the regulation of the internet is not a strictly authoritarian pursuit, nor is it limited to governmental and security-related content. The regulation of the cybersphere represents a governmental response to global technologies and their increasing popularity.

For authoritarian and democratic regimes alike, internet regulation originated as legislation that sought to control the dissemination of speech and electronic content through law (Stevenson, 2007). During the late 1990s, several Western nations, including the United States and Australia, moved to implement legislation that would restrict internet content that could be considered “obscene” or “disturbing” (Stevenson, 2007, p. 534-5). During the same period, China introduced similar legislation, which sought to restrict content that was deemed undesirable or threatening (Stevenson, 2007). This was achieved through the introduction of a system of content regulation via government approval and registration (Stevenson, 2007). Though originating from different places, the development of internet regulation in democratic and nondemocratic regimes suggests that the internet represents a destabilizing entity, whether to society or the state. As such, it requires the development of new governance practices that mitigate the threat and, in doing so, safeguard the state through tiered technologies of power that are both technical and socially formative. In the quest to regulate the cybersphere, China has emerged at the cutting edge, becoming a model of technical censorship referenced by countries such as Cuba and Vietnam (Lagerkvist, 2005, p. 121).

Through the global nature of the internet and the threats it poses to state control as a decentralized entity, the regulation of the internet remains a specifically global issue that has given rise to the formation of new governmental rationalities in response to emerging global threats. In this paper, I argue that issues of internet censorship in China represent an important example of the emergence of new techniques of governing stem from new, globalized threats to state control. As a fundamentally global network, the internet ranks among one of the most pressing of these threats, requiring new regulatory practices in both authoritarian and non-authoritarian regimes. Unlike communication and information platforms of the past, the internet is decentralized and presents new challenges to regulation. As a result, regulatory practices have also shifted toward decentralization, augmenting existing centralized techniques of control and, in the process, constructing tiered technologies of power through which subjects are produced and governed. I analyze the emergence of these practices and their impacts by first examining the implications of globalization trends — both economic and technological — on governance by building on the Foucauldian concept of "governmentality" (Foucault, 1991). I then describe and contextualize the electronic censorship in China within existing discourses about the internet as a potentially political platform and space, arguing that it functions through the simultaneous evolution of control and resistance.

With this paper, I begin in the first section by articulating the challenges posed by the internet as a space of both potential economic growth and dissension, a reality which I will then place into contexts of governance, decentralization, and emergent global threats in the second section, arguing that the expansion of the internet has created new governmental challenges within both authoritarian and non-authoritarian regimes. I subsequently examine the Chinese government's response to these threats through what I have termed tiered technologies of power.

I will then examine each of these tiers in detail before concluding with an assessment of emerging governmental practices in China with regard to the internet and their global relevance.

The Cybersphere as Commercial Space

Within the global context, China represents an internet colossus that requires a unique combination of strategies to regulate and control its space. By the end of 2008, China had surged ahead of the U.S. to become the nation with the largest online population in the world — 298 million at the time (Liu, 2012, p. 48; CNNIC, 2012). By the end of 2013, the number of internet users in China had more than doubled to 618 million over the course of a mere five years (CNNIC, 2014). While much of the Chinese government's efforts concentrate on developing the internet as a non-threatening commercial space, the internet remains a highly expressive platform that resists regulation through the marriage of e-commerce and sociopolitical subversion.

With its formal introduction into China in 1994, the internet ushered in a new age of information sharing and lucrative economic opportunities (Yang, 2003; Lei, 2011; Lagerkvist, 2005). As a mass communication tool, the internet operated outside the realm of well-controlled, centralized mass media, making it a potential platform of dissension; however, the internet also facilitated new avenues of economic growth (Lei, 2011; Xiao, 2011). As of December 2013, 93.1% of enterprises in China used computers while "83.2% used the Internet to handle official business in China," including corporate giants such as Alibaba, which has filed to become a publically traded company in the United States and is set to become the largest American initial public offering (IPO) in history (CNNIC, 2014, p. 5; Goel, De La Merced, & Gough, 2014). Within the twelve-month period measured by the CNNIC — January through December 2013 — the

number of internet shoppers in China rose 6 percentage points to 302 million (CNNIC, 2014, p. 8). As such, the internet represents a promising arena for economic expansion, a possibility that has facilitated the emergence of systems of governance that seek to eliminate the threat to the state while harnessing the economic power of the medium (MacKinnon, 2011; Guo & Feng, 2011; Stevenson, 2007; Wu, 2005).

Global Technology and Governmental Challenges

Though conceptualized as a singular entity, the internet, in fact, comprises a global network system of digitally connected computers, servers, and routers that interact through a series of unique internet protocol (IP) addresses to send and receive data packets (Leiner et al., 2009). Communication between these devices and smaller sub-networks are enabled by common protocols that allow different devices and smaller networks to interact and link with the global network (Shuler, 2005). Though most strongly associated with the last decade of the 20th century, the technology upon which the internet is based originated in the 1960s with a series of experiments that tested the viability of limited multicomputer networking (Leiner et al., 2009). However, it was not until the mid-1980s that these experiments were translated into a public setting in the United States and United Kingdom through institutions of higher education (Leiner et al., 2009). At present, the internet has developed into a distinctively global network of devices through which information is exchanged and transmitted across geo-political borders. This construct predisposes the internet to decentralization, posing a new regulatory challenge to the nation-state. In China, this challenge has been confronted through technological solutions, such as the Great Firewall of China (GFC), and the emergence of tiered technologies of power.

Though the internet is often depicted as shapeless and borderless within its global context, it is divisible into localized spheres through regulatory technologies such as the GFC. In her discussion of "networked authoritarianism," MacKinnon (2011) aims to conceptualize the internet spatially through four "deliberative spaces" (MacKinnon, 2011, p. 36). Of these spaces, the GFC targets the fourth, "international deliberative spaces," and is designed to control the inflow of information from outside China and regulate citizen access within the nation's cyberborders (Min as cited in MacKinnon, 2011, p. 36; MacKinnon, 2011). As such, these technologies seek to control the flow of information into China, while preserving the economic viability of the internet by harnessing its global connective potential in a delicate balancing act between prosperity and security.

As a product of technological advancement in the 20th century, the internet has emerged as an important component of globalization, reflecting the emergence of a virtually borderless enterprise through global communication networks and technologies. As economic and social networks become increasingly intertwined across geo-political boundaries, the systems and processes associated with them have been adapted and augmented to meet the emerging challenges and demands of a globalizing society. As a result, globalization has produced new systems and structures, reconfiguring the roles of the corporation and the nation-state through phenomena of transnationalism and decentralization. For the purposes of this paper, I am interested in the implications of these processes and the rise of the transnational corporation within the context of developing governmentalities that address the challenges to state security by an increasingly networked, global world. I seek to specifically address the involvement of the transnational corporation in governing processes as they are reconfigured to meet the emerging challenges of decentralized technologies and globalization.

Although the internet may be considered emblematic of decentralization processes and the spaces they produce, it is by no means unique. As Leslie Sklair (2012) and Susan Strange (2012) argue, transnationalism and decentralization represent hallmarks of globalization. In her discussion of globalization, Sklair suggests that the transnationalism of practices and corporations that has emerged since the 1960s is itself based on a shift in the capitalist system that allowed it to globalize (Sklair, 2012, p. 62-63). Such processes have yielded a transnational capitalist class, which is integrated into primary spheres of influence (e.g., economic, political, and cultural), and propels "globalizing processes" (Sklair, 2012, p. 57). Susan Strange asserts that in the wake of globalization, states have experienced a decline in centralized authority and power, a process accompanied by the simultaneous "diffusion" of power into other institutional bodies (Strange, 2012, p. 220).

The emergence of new governing systems and apparatuses — including what I have termed tiered technologies of power — respond directly to the challenges of the internet's decentralized and global nature. According to Xiao Qiang (2011), the primary goal of censorship is "preventing the widespread distribution of information that could lead to collective action such as mass demonstrations or signature campaigns" (Xiao, 2011, p.52), an assertion supported by King, Pan, and Roberts (2013, p. 326). In the past, this goal could be achieved through a centralized governmental entity or bureau. However, these systems are ill-suited to decentralized technologies such as the internet, through which information and rhetoric can be dispersed quickly and easily. As a platform of mass communication and a "venue for political struggle," the internet represents a new kind of potential threat to state security and stability through its connective capacity (Lei, 2011, p. 295). In recognition of this capacity and the internet's discursive potential, scholars such as Geoffry Taubman (1998) predict that authoritarian

governments "will face greater difficulties in maintaining their hegemony" (Taubman, 1998, p. 357).

In tracing the development of governance practices related to the emergence of the internet, it is important to first understand the global network itself as a governmental problem, which has necessitated a reconfiguration of governing systems and practices. According to Sklair and Strange, processes of globalization have given rise to new systems and configurations of power (Sklair, 2012; Strange, 2012). Such shifts have constituted new governmental challenges and required the evolution of new governmental systems, the impacts of which have been discussed by Stephen Collier and Andrew Lakoff (2008) within the context of global health. They write, "The global scale of these threats crosses and confounds the boundaries of existing regulatory jurisdictions" (Collier & Lakoff, 2008, p. 8). As such, they require new "interventions" to safeguard the security of the state (Collier & Lakoff, 2008, p. 8).

Though Collier and Lakoff's work emphasizes biosecurity and the evolution of global health, the frame through which they understand the ongoing formation of "ways of understanding and intervening in contemporary threats to health," remains highly relevant as we conceptualize systemic shifts based emerging global processes (Collier & Lakoff, 2008, p. 9). As Collier and Lakoff illustrate, global connectivity experienced through the internet poses new hazards to the state and its security that require new ways of governing (Collier & Lakoff, 2008). While these governmental strategies have heretofore focused on elimination of hazard through regulation, threats at the global level cannot be managed in this way and have, as such, facilitated a shift in governing that emphasizes preparedness rather than elimination, recognizing the decentralization of state security threats (Collier & Lakoff, 2008). In establishing and developing internet censorship in the People's Republic of China, the government has engaged in an

"intervention" that reconfigures technologies and processes of government to preserve and protect the state from emerging global threats.

In examining the emergence and expansion of internet censorship, I build on the work of Michel Foucault and the later analyses of Collier and Lakoff to understand the emergence of new governmentalities within the context of global networking and regulation. Though these shifts and developments are pertinent across the political spectrum, they are particularly important for one-party, authoritiarian systems such as China's for which control represents a source of legitimacy. In addressing these issues of state control, I employ a Foucauldian understanding of governmentality in which "…one has a triangle, sovereignty-discipline-government, which has as its primary target the population and as its essential mechanism the *apparatuses of security*" (Foucault, 1991, p. 102; emphasis added). As such, "governmentality" references the processes by which interpersonal and institutional relations are governed through these apparatuses (Gordon, 1991, p. 2-3; Collier & Lakoff, 2008, p.14). Over the course of the last several decades, with the advent of globalization and networking technologies such as the internet, these appartuses have undergone a transformation, revealing the ongoing adaptation and evolution of governmental rationalities in response to new threats understood as more technologically sophisticated.

Further developing this emerging conceptualization, Wu (2005) describes the internet in China as five-dimensional and asserts that by virtue of its decentralization, the internet requires the development of new governing techniques to implement regulation (see also Qiu 1999/2000). In addition, Wu asserts that the media structure in China has shifted from being "uni-polar" to "tri-polar" by necessity, stemming from the "virtual sphere," referring to strategic regulation across ownership types, including state-owned enterprises, collectively-owned enterprises, and

their privately-owned counterparts (Wu, 2005, p. 218). In this way, the introduction of the internet in China has not caused a reduction in regulation, but rather an evolution in which old regulatory practices associated with mass media have been adapted and expanded (Wu, 2005; Qiu, 1999/2000). Through these processes of adaptation, the Chinese government is actively adjusting and responding to emerging threats to state security tied to the rise of decentralization attached to globalization and global network technologies such as the internet (Wu, 2005; Qiu, 1999/2000).

Electronic Censorship and Tiered Technologies of Power

According to scholars such as Taubman (1998), the introduction of the internet in China represented a loss of control and a move toward democratization. However, this perspective has been roundly critiqued in recent years by authors such as Lijun Tang and Peidon Yang (2011), who describe the assumption that, "…as long as people have the resources to access the internet, they are in a position to make their voices heard" (Tang & Yang, 2011, p. 676). Such assumptions of "visibility" and voice highlighted and critiqued by Tang and Yang dramatically oversimplify the realities of the Chinese internet, which operates within the context of powerful systems of censorship. However, while Taubman recognized the internet's democratic potential, it has been largely unrealized. As such, in recent years, many scholars have chosen to reexamine the emergence of the internet in authoritarian regimes, articulating a complex reality in which the internet is both a platform of dissension and a highly controlled space, leading to complex new questions of governance and government (Tsui, 2003; Qiu, 1999/2000).

The development of electronic censorship in China has marked a distinctive shift away from centralized authority and toward decentralized power and regulation (Tsui, 2003; Xiao, 2011; Wu, 2005). In order to manage new types of perceived threats to regime legitimacy, China has developed new censorship systems that function in tiers, ranging from overt to implicit, through which power acts on the subject. Building on the censorship techniques of mass media, the Chinese government has instituted systems of "virtual censorship," what I have called "electronic censorship," to regulate the internet as a communicative space and maintain "old hegemonic modes of political communication" (Qiu, 1999/2000, p. 23; Ying, 2012). These emerging techniques that compose China's tiered technologies of power include: 1) direct censorship through data filtering, blockage, and content removal; 2) institutional censorship through web-hosting sites and the corporations that operate them; and 3) self-censorship through internal regulation. Through the utilization of imported security technologies, the Chinese government has begun to construct new methods of governmental control within the emerging space of the internet (Qiu, 1999/2000). This transition is fundamentally based on a restructuring of the Chinese censorship system that utilizes the multidimensional technologies listed above to regulate and control internet usage among citizens (Stevenson, 2007; Wu, 2005; Guo & Feng 2011; Crandall et al., 2007; MacKinnon, 2008). As the works of Stevenson (2007) and King, et al. (2013) demonstrate, the Chinese censorship system operates at multiple levels, including public, private, and institutional. However, at the most direct and overt level — content blockage and filtering — the system remains highly technical (Stevenson, 2007; Crandall et al., 2007).

Direct Censorship

On its face, the internet is a fundamentally global network, theoretically accessible to anyone with the technical means to log on. However, to users in China, the actual access afforded is limited through a combination of technical and institutional systems of electronic censorship (MacKinnon, 2008; Tsui, 2003; Stevenson, 2007, p. 540; Crandall et al., 2007). The Great Firewall of China is among the most widely recognized of these methods and has become increasingly controversial over the past decade as a result of the technology's Western origins (Crandall et al., 2007; Stevenson, 2007). Among the most commonly referenced of China's direct regulatory technologies both in popular and scholarly discourse, the GFC is one of several technical censorship methods, including blocking individual IP addresses and domain name service (DNS) redirection (Crandall et al. 2007, Keyword-based Censorship, para. 9). However, the precise definition of the Great Firewall remains ambiguous. In his discussion of internet censorship, Stevenson employs the GFC to describe the totality of censorship mechanisms while more technical articles, such as those by Crandall, et al. put forth a more specific, technological definition (Stevenson, 2007; Crandall et al., 2007). For the purposes of this paper, I utilize the understanding put forth by Crandall, et al. for whom the GFC is a system of government-controlled routers that block websites and search terms within China's cyberborder (Crandall et al., 2007).

Though fundamentally global, the Chinese cybersphere is bounded by the Great Firewall, a permeable cyberborder comprised of routers, both private and public, through which data packets pass (Crandall et al., 2007). When packets containing blacklisted keywords, such as "political persecution" (政治迫害), "civil rights movement" (民运), or "Chinese riots" (国人暴动), pass through a GFC router, a reset is triggered at both the destination and source IP

addresses, halting the data transmission (Crandall et al., 2007, Tables 2-3). This filtering process effectively constitutes what Stevenson (2007) refers to as a "second tier" of internet access that "provides government control over the borders between the Chinese Internet and the rest of the world" (Stevenson, 2007, p. 540).

Through the emergence of tiered technologies, the universality of the internet has been challenged based on the regulatory practices of nation-states in the process redefining the "global network" within the national context. Through technical regulation, the GFC represents an attempt to localize the internet and, therefore, control potentially destabilizing actions and communications within China's electronic borders. At the same time, other, less direct technologies of corporate and self-censorship regulate simultaneously within a distinctly national context. While the internet remains essentially global, it is regulated by nation-states— both directly and indirectly — that seek to control global networking technologies, harnessing their potential while minimizing security risks to the state.

Institutional Censorship and Transnational Corporations

In recent decades, one way countries such as the People's Republic of China have sought to control the web has been through the utilization of technologies produced by multinational, U.S.-based corporations, such as Cisco Systems and Nortel Networks, while simultaneously employing regulatory parameters of acceptable content (Lagerkvist, 2005). This has pushed issues of electronic censorship to the fore through a succession of public controversies and the enactment of new legal standards regarding the involvement of the United States and its corporations in the development of censorship both domestically and abroad (Stevenson, 2007).

These have been aimed, in part, at corporations such as Cisco and Nortel, which have participated in the sale of censorship technologies such as routers or surveillance software (Newbold, 2003; Lagerkvist, 2005). However, these controversies and actions have been primarily oriented toward corporations that have actively participated in censoring content or aided government surveillance of dissidents, such as Yahoo!, Microsoft, and Google (Newbold, 2003; Deva, 2007; Stevenson, 2007; Gough, 2013). As Lagerkvist points out, censorship is by no means an exclusively authoritarian practice (Lagerkvist, 2005). However, it has blossomed in the wake of rising, and potentially destabilizing, internet technologies.

While systems of censorship in China remain highly complex, the origins of institutional and corporate involvement can be traced to early legislative acts shortly after the introduction of the internet, such as the "Interim Provisions Governing Management of Computer Information Networks in the People's Republic of China Connecting to the International Network," which was enacted and successively amended in 1998 and 2000, respectively, and regulated web content through systems of government approval and registration (Stevenson, 2007, p. 537). These legislations provided the basis for subsequent corporate regulations, such as the "Public Pledge on Self-discipline for the Chinese Internet Industry" and the 2005 revision of existing regulations (Provisions for the Administration of Internet News Information Services; Chinalawinfo.com). Among these revisions were new stipulations on the publishing on "Internet news," which limited the ability of unapproved blogs to report news items (Stevenson, 2007; Chinalawinfo, 2012). Through this critical revision, corporations became legally accountable for the content posted by their users, transforming them into non-governmental censors and thereby integrating them into the newfound censorship structure (Stevenson, 2007; MacKinnon, 2008).

Within the context of tiered technologies of power, the 2005 legislation provisions represented a critical development in the arena of electronic censorship in China, giving rise to a secondary tier between direct regulation and self-censorship — institutional censorship. At a legislative level, this responded to the need for integration of new regulatory practices into existing, centralized censorship systems by shifting legal responsibility for content regulation onto corporate web-hosts, creating a new category of non-governmental internet censors. Additionally, while blogs and internet content remains regulated, this regulation occurs not directly through the state but often through U.S.-based, multinational corporations (MacKinnon, 2008; Stevenson, 2007). Increasingly, private companies such as blog hosting sites, including Bokee — a Chinese webhosting site — and Microsoft's MSN, have become responsible for the direct oversight of content under the watchful eye of the Chinese government (MacKinnon, 2008). This has become controversial in recent years as it has implicated Western companies in new ways in the practice of censorship and, as such, raises questions about the role of the transnational corporation in state security (MacKinnon, 2008; Newbold, 2003; Deva, 2007; Stevenson, 2007).

Whereas the GFC and other censorship strategies, such as IP address blocking, sought to utilize government security to directly regulate cyber content, legal controls have augmented technical censorship and self-censorship through the decentralization of regulatory responsibility from the state to corporate and institutional actors (Stevenson, 2007). However, the practice of censorship in China is not limited to the use of the GFC as an information blocker, employing technologies from transnational corporations such as Cisco and Nortel (Stevenson, 2007). MacKinnon asserts, "Chinese networked authoritarianism *cannot work without the active cooperation of private companies,*" who have become practitioners of censorship through the

imposition of legal responsibilities onto these private service providers (MacKinnon, 2011, p. 37; emphasis added). As such, MacKinnon argues the Chinese government has created a system of censorship operating on multiple levels to control the electronic spread of information both directly and indirectly through what she describes as a "simultaneously vital and dangerous" system (MacKinnon, 2011, p. 37).

Even as regulatory systems and technologies have become increasingly adapted to the challenges of the cybersphere, resistance continues to manifest. One of the most popular recent examples includes the fictional grass-mud horse, a furry manifestation of resistance that employs the image of the alpaca as a symbol of subversion and discontent (Tang & Yang, 2011). The term "grass-mud horse" (草泥吗) emerged through a song consisting of an innocuous story made up of obscene homophones and puns, posted as an online response to the Chinese government's "cleaning up the internet" initiative launched in 2009 (Tang & Yang, 2011, p. 679). The song itself and the image of the grass-mud horse, an alpaca, have become synonymous with resistance to powers of authority, both in sociocultural and political contexts, and representative of a challenge to authoritarian control (Tang & Yang, 2011). The phenomenon that surrounded it, including the birth of the grass-mud horse as a commercial enterprise through the sale of plush alpacas, signaled decisive and collective pushback against authoritarian censorship using the very medium the state sought to control (Tang & Yang 2011). In this way, the internet's status as a space of economic and commercial activity has afforded new avenues of dissension through commercial outlets, which respond directly to the exercise of regulatory power.

Self-Censorship

Technical systems of censorship represent only a small component of a much larger censorship system that relies on additional regulatory tiers, including corporate and, perhaps most importantly, self-censorship. Within these tiers, the Chinese government has also created a "safety valve" in cyberspace through which discontent can be expressed within the confines of a regulated, electronic space (MacKinnon, 2008, p. 33). This enables animosities and tensions to be released in a "safe" way, thus preventing a destabilizing reaction in the form of mass movements or facilitated uprising (MacKinnon, 2008). As such, censorship has become an increasingly sophisticated apparatus through which information flows are managed both within global and local contexts. In this way, the communicative capacity of the internet is preserved.

Yet, while the internet possesses communicative and connective potential, MacKinnon argues that it should be conceived of not as a cause of increased media transparency or civil society, but as a platform that derives its status and meaning from its users (MacKinnon, 2008). In doing so, she pushes back against the assumption that the internet is a fundamentally democratizing force, positing instead that the rise of internet activism may "serve to bolster regime legitimacy" rather than threaten it (MacKinnon, 2011, p. 35). Instead of creating a political cleft, the challenge to the regime posed by dissidents through the use of online platforms facilitates a unification to confront the challenge rather than a disintegration of power and authority (MacKinnon, 2011). However, this challenge from the people has been limited due to self-regulation among citizen-subjects. While Crandall et al. (2007) demonstrated that nearly 30% of Chinese IP addresses are uncensored by the Great Firewall, dissension remains minimal (perhaps in part due to additional surveillance technologies, an issue which I do not discuss here; Crandall et al. 2007, Introduction, para. 4). In addition, while savvy netizens may know about

proxy servers — a common censorship workaround — relatively few choose to utilize them, demonstrating the phenomenon of self-regulation described by Crandall et al. and Lokman Tsui's (2003) "modalities of control" (MacKinnon, 2008; Crandall et al., 2007; Tsui, 2003, p. 66).

Though the participation of Western — specifically U.S.-based — corporations in the creation and maintenance of authoritarian security systems remains controversial, their presence may also be considered reflective of U.S. dominance in the global cybersphere (Liu, 2012). While a system such as the GFC represents a distinctively Chinese innovation, it relies on technologies originating in the West (Stevenson 2007). According to Liu, the information technology sector has been historically dominated by U.S.-based corporations, fuelling recent attempts by the Chinese government to gain technological independence from international firms and systems (Liu, 2012). However, the issue of electronic censorship and its technologies in China is not only a matter of sovereignty; it remains highly relevant as an indicator of governmental shifts that respond to the challenges of a globalizing society. Utilizing foreign technologies, the Chinese government seeks to safeguard the state's power, but in doing so becomes dependent on Western transnational corporations, simultaneously participating in and resisting the processes of globalization.

As the Chinese internet has expanded, it has required the development of new, technical modes of governing through systems such as the GFC. However, studies suggest that the GFC itself is in fact much more permeable than the name suggests, indicating evolving practices of self-regulation in the cybersphere (MacKinnon, 2011; Crandall et al., 2007; Stevenson, 2007). In creating "ConceptDoppler," a method of decoding search terms blacklisted by the Chinese government," researchers Jedidiah R. Crandall, et al. found that only one-quarter of filtered

internet data was filtered at the Chinese cyberborder, and that the majority of filtering occurred within China (e.g., on Chinese devices; Crandall et al. 2007, Introduction, para. 4). Furthermore, only 71.1% of the IP addresses the researchers probed utilized a government router, leaving 28.9% of IP addresses filter-free (Crandall et al. 2007, Introduction, para. 4). As such, Crandall, et al. illustrate not only technological processes of censorship but the emergence of power that is based less on fortitude and overt regulation and more on self-regulation (Crandall et al., 2007). It is useful to think of this as a "panoptic" practice, one which evidences governmental shifts that are increasingly reliant on the internalization of power rather than the direct exercise of government discipline.

The perception of the internet as panoptic space builds upon Foucauldian understandings of power that require minimal exertion to achieve regulation. In conceptualizing the Chinese cybersphere this way, scholars such as Tsui (2003), Qiu (1999/2000), and Crandall et al. (2007) reject arguments that the internet is an inherently democratic space. Instead, they assert the presence of new mechanisms of regulation and forms of power, formulating a false dichotomy between regulation and dissension in the process (Tsui 2003; Qiu, 1999/2000; Crandall et al., 2007). As such, the internet has become a space of incipient regulation in which new apparatuses of state security are being constituted through what Tsui termed "modalities of control," which have emerged in tandem with the internet in China (Tsui, 2003, p. 67). These "modalities" include the law, the market, social norms, and design (Tsui, 2003, p. 67). Through their presence and functionality, these modalities serve a direct regulatory function but also provide the potential for the development of virtual panopticism and the evolution of norms of electronic self-censorship, potential that Tsui asserts is slowly being realized through the internet's recent emergence as a "technology of control" through which subjects are governed (Tsui, 2003, p. 66).

By questioning the internet's seemingly inherent status as a free communicative platform, we may bring into focus issues of power and subject formation linked to the integration of new regulatory technologies and the reconfiguration of state-subject relations in the global online cybersphere (Ying, 2012; Tsui, 2003). As such, the internet in China and the blogosphere, in particular, is managed through technologies of the self, yielding governable subjects who regulate themselves and thus require minimal enforcement of external censorship (Ying, 2012). The ability to manage subjects in this way is the product of socioeconomic shifts that have produced a "self-centred" and "rebellious" generation, which requires less overt strategies of governance, providing internet-users with a sense of autonomous choice (Ying, 2012, p. 42).

Power and the Future of Governance in the Cybersphere

In the wake of growing internet usage in the People's Republic of China, the Chinese state has seen the emergence of new threats to its stability and security as citizens become increasingly engaged with global technologies, introducing new governmental challenges in the process. Though censorship itself represents an age-old practice, the growing prevalence of decentralized and global networking technologies such as the internet has required these practices to evolve to meet the regulatory challenge posed by the cybersphere. In China, this evolution has manifested via the emergence of tiered technologies of power through which the subject is governed and electronic space is regulated.

Supported by the tiering of technologies, China's emerging censorship system responds to the challenges of decentralization and the tensions between security-driven regulation and economically-motivated freedoms. As the nation continues to develop, the preservation of the

internet's economic potential and its cultivation remains an important consideration for the Chinese government (Wu, 2005), helping — along with considerations of ongoing state security and stability — to shape the development of new governing systems and practices as a result. By instituting direct forms of censorship such as the Great Firewall, China has endeavored to create a kind of cyberborder that controls information flow within the country while preserving economic and commercial freedoms conducive to enterprise (Crandall et al., 2007; Stevenson, 2007). The government has employed corporate institutions as regulators of content by shifting legal responsibility of policing internet posts onto web-hosting sites such as Yahoo! and MSN, creating a second tier of institutional regulation that is itself decentralized (MacKinnon, 2008; Stevenson, 2007; Chinalawinfo, 2012). At the same time, the state has utilized a burgeoning sense of surveillance and panopticism to facilitate citizen self-regulation in the cybersphere (Tsui, 2003). In combination, these regulatory apparatuses illustrate an evolution and augmentation of existing censorship practices that have yielded a series of multifaceted, multidimensional systems through which power is articulated and the state is secured, facilitating the formation of new kinds of citizen-subjects in the process.

However, as we consider the development of new censorship and governmental practices within the context of global networking, it remains important to recognize that China's tiered technologies of power are reliant on foreign technologies, many developed and sold by U.S.-based transnational corporations such as Cisco and Nortel Networks (Stevenson, 2007; Newbold, 2003). As such, the issue of governance in the internet age remains an inherently global one, not only in the networking factors that facilitate new governmental rationalities, but also in solutions that have arisen to meet these challenges. Increasingly, the transnational corporation has become integrated into state governance, including through the provision of state security. This

integration raises new questions about the role of transnational corporations in the maintenance of the Chinese Communist Party and implicates Western firms specifically in the perpetuation of authoritarian rule in China through the suppression of speech and subject regulation.

Yet, as the 2013 case of Bradley Manning illustrated, concern about the internet as a new type of threat to state security is not limited to authoritarian regimes but also their democratic counterparts (Serrano, 2013). As such, the emergence of global networking technologies poses new governmental challenges across the political spectrum, raising key questions about how these issues will be addressed. As the internet continues to develop as a global system, it becomes increasingly important that we critically examine the role of the transnational corporation and similarly global entities in the formation of new systems of governance and governmental rationalities, as well as the ultimate effects on the formation of the citizen-subject through evolving regulatory practices. Although examined here in a national context, the development of new global threats remains pertinent across the globe and the way in which these threats are managed will influence not only the lives of affected subjects through shifting citizen-state power relations but global relations as well.

References

Chinalawinfo. (2012). Provisions for the administration of internet news information services. Retrieved May 2, 2014. Retrieved from http://www.lawinfochina.com/display.aspx?id=4569&lib=law

Chinese Internet Network Information Center (CNNIC). (2012). Internet timeline of 2008. Retrieved April 7, 2014. Retrieved from http://www1.cnnic.cn/IDR/hlwfzdsj/201209/t20120904_36019.htm

Chinese Internet Network Information Center (CNNIC). (2014). *Statistical report on internet development in China*. Chinese Internet Network Information Center.

Collier, S., & Lakoff, A. (2008). The problem of securing health. *Biosecurity interventions* (pp. 1-16). New York: Columbia University Press.

Crandall, J. R., Zinn, D., Byrd, M., Barr, E. T., & East, R. (2007). ConceptDoppler: A weather tracker for internet censorship. Paper presented at the *ACM Conference on Computer and Communications Security,* 352-365.

Deva, S. (2007). Corporate complicity in internet censorship in China: Who cares for the global compact or the Global Online Freedom Act. *George Washington International Law Review, 39*, 255.

Foucault, M. (1991). Governmentality. In G. Burchell, C. Gordon & P. Miller (Eds.), *The Foucault effect: Studies in governmentality* (pp. 87-104). Chicago: University of Chicago Press.

Goel, V., De La Merced, Michael J., & Gough, N. (2014, May 6). Chinese giant Alibaba will go public, listing in U.S. *New York Times*. Retrieved from http://dealbook.nytimes.com/2014/05/06/alibaba-files-to-go-public-in-the-u-s/?_php=true&_type=blogs&_php=true&_type=blogs&smid=fb-nytimes&WT.z_sma=DB_CGA_20140507&bicmp=AD&bicmlukp=WT.mc_id&bicmst=1388552400000&bicmet=1420088400000&_r=3

Gordon, C. (1991). Governmental rationality: An introduction. In G. Burchell, C. Gordon & P. Miller (Eds.), *The Foucault effect: Studies in governmentality* (pp. 1-51). Chicago: University of Chicago Press.

Gough, N. (2013, September 7). Chinese democracy advocate is freed after 8 years in prison. *New York Times.* Retrieved from http://www.nytimes.com/2013/09/08/world/asia/shi-tao-chinese-democracy-advocate-is-released-from-prison.html?_r=0

Guo, S., & Feng, G. (2012). Understanding support for internet censorship in china: An elaboration of the theory of reasoned action. *Journal of Chinese Political Science, 17*(1), 33-52.

King G., Pan J. Roberts M.E. (2013). How censorship in China allows government criticism but silences collective expression. *American Political Science Review,107*(2), 326-343.

Lagerkvist, J. (2005). The rise of online public opinion in the People's Republic of China. *China: An International Journal, 3*(1), 119-130.

Lei, Y. W. (2011). The political consequences of the rise of the Internet: Political beliefs and practices of Chinese netizens. *Political Communication*, *28*(3), 291-322.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., & Wolff, S. (2009). A brief history of the Internet. *ACM SIGCOMM Computer Communication Review*, *39*(5), 22-31.

Liu, Y. (2012). The rise of China and global internet governance. *China Media Research, 8*(2), 46-55.

MacKinnon, R. (2008). Flatter world and thicker walls? Blogs, censorship and civic discourse in China. *Public Choice, 134*(1-2), 31-46.

MacKinnon, R. (2011). China's "Networked Authoritarianism. *Journal of Democracy 22* (2), 32-46.

Newbold, J. R. (2003). Aiding the enemy: Imposing liability on US corporations for selling China internet tools to restrict human rights. *University of Illinois Journal of Law, Technology & Policy 503*, 503 - 529.

Qiu, J. L. (1999/2000). Virtual censorship in China: Keeping the gate between the cyberspaces. *International Journal of Communications Law and Policy, 4*(Winter), 1-25.

Serrano, R. A. (2013, August 21). WikiLeaks trial: Bradley Manning sentenced to 35 years in prison. *Los Angeles Times.* Retrieved from http://articles.latimes.com/2013/aug/21/nation/la-na-nn-wikileaks-bradley-manning-sentenced-20130820.

Shuler, R. (2005). How does the internet work? Retrieved April 28, 2014, Retrieved from http://www.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm

Sklair, L. (2012). Sociology of a global system. In F. J. Lechner, & J. Boli (Eds.), *The globalization reader* (pp. 57-63). Malden, MA: Wiley-Blackwell.

Stevenson, C. (2007). Breaching the great firewall: China's internet censorship and the quest for freedom of expression in a connected world. *Boston College International and Comparative Law Review, 30*(2), 531-558.

Strange, S. (2012). The declining authorities of states. In F. J. Lechner, & J. Boli (Eds.), *The globalization reader* (pp. 217-225). Malden, MA: Wiley-Blackwell.

Tang, L., & Yang, P. (2011). Symbolic power and the internet: The power of a `horse'. *Media, Culture and Society, 33*(5), 675-691.

Taubman, G. (1998). A not-so world wide web: The internet, China, and the challenges to nondemocratic rule. *Political Communication, 15*(2), 255-272.

Tsui, L. (2003). The panopticon as the antithesis of a space of freedom control and regulation of the internet in China. *China Information, 17*(2), 65-82.

Wu, X. (2005). Red net over China: China's new online media order and its implications. *Asian Journal of Communication, 15*(2), 215-227.

Xiao, Q. (2011). The battle for the Chinese internet. *Journal of Democracy, 22*(2), 47-61.

Yang, G. (2003). The co-evolution of the internet and civil society in China. *Asian Survey, 43*(3), 405-422.

Ying, J. (2012). *Cyber-nationalism in China : Challenging Western media portrayals of internet censorship in China.*