Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

The Chinese Internet: Control Through the Layers

Shirley Hung

October 30, 2012

Acknowledgements: This work is funded by the Office of Naval Research under award number N000140910597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the Office of Naval Research.

I. Introduction

China is often described as having the world's most advanced Internet censorship and surveillance regime.[1] It garners much fear and attention in the media and among policymakers, yet most reports focus on specific incidents or capabilities, not the system as a whole. The Great Firewall, which generally refers to the technical implementation of controls, is the most well-known part of the system, but the overall control regime includes a significant human element ranging from police persecution of dissidents to human censors who review individual blog and social media posts to the self-censorship that has become an almost reflexive response among citizens. The control regime implemented by China is in many ways exactly what one would expect of a rational, forward-looking, planning-oriented authoritarian regime determined to remain in power while retaining legitimacy: extensive, pervasive, deeply integrated into the technical apparatus of the Internet, and both reflective of and entwined with the political and social structures in which it is embedded. It is not a perfect regime – not every post the government would deem undesirable is caught or removed – but it is good enough. It utilizes technical tools, self-censorship, and human review to create a system with enough built-in flexibility to enable a fine-grained control of which most political leaders around the world can only dream.

As for the political impact of this elaborate control system, it is often suggested that the widespread Internet access—over 500 million users by the end of 2011[2]—will 'open up' China and lead to greater democratization and liberalization, and possibly even the overthrow of the

[1] For typical discussions of the censorship and circumvention regime, see:
http://topics.nytimes.com/topics/news/international/countriesandterritories/china/internet_censorship/index.html;
http://www.businessweek.com/technology/content/jan2006/tc20060112_434051.htm;
http://www.time.com/time/world/article/0,8599,1981566,00.html

[2] http://news.yahoo.com/chinas-number-users-rises-513-million-023844706.html

Communist regime. The rapid growth in Internet users and social media use[3] has been an area of particular optimism for those hoping for liberalization and regime change since Arab Spring, and indeed, the Internet and particularly social media represent one of the few comparatively free forums for expression of ideas. Recent years have seen a surge in local protests and use of social media to air grievances against local officials and social injustices.[4] Yet as some researchers have pointed out, the protests in China rarely lead to significant change. Instead, real protest calling for a change in (top) leadership is swiftly quashed, while protests against lower-level officials are sometimes used a way to monitor and channel public opinion, rid the lower levels of corrupt officials, enhance the Party's legitimacy by appearing responsive, and ultimately perhaps strengthen its stability by allowing a managed means for the public to blow off steam.[5]

II. Control: of whom, by whom, for what? And how?

Social stability and preservation of the Party's rule are near-synonymous terms for the Chinese leadership. The Party's legitimacy rests on two pillars: nationalism, often viewed as

[3] Nearly 40% of China's population is online as of 2011, http://www.ministryoftofu.com/2011/12/infographics-how-big-is-chinas-social-media-and-digital-market/; according to the World Bank, this number was less than 5% in 2002, and less than 15% five years ago, http://www.google.com/publicdata/explore?ds=d5bncppjof8f9_&met_y=it_net_user_p2&idim=country:CHN&dl=en&hl=en&q=internet+users+in+china. Over half of Internet users are on social media. http://www.resonancechina.com/2012/03/27/china-social-media-users-to-reach-414-million-by-2014/

[4] Guobin Yang, *The Power of the Internet in China* (New York: Columbia University Press, 2009), esp Ch. 2. For more recent examples, see: Wukan protests of December 2011 (http://www.ft.com/cms/s/0/f5e8ffa8-4055-11e1-82f6-00144feab49a.html#axzz1rBidQJ1G), Li Gang incident (http://chinadigitaltimes.net/2010/10/car-accident-gate-my-dad-is-li-gang/), melamine-tainted milk (http://blogs.wsj.com/chinarealtime/2011/12/28/chinese-internet-takes-on-mengniu/), Foshan toddler death story (http://www.theatlantic.com/international/archive/2011/10/on-that-horrible-toddler-death-story-from-china/247280/), Shanghai high-speed-rail crash stories, any of assorted incidents cited in NYT Magazine Chinese Internet Humor (http://www.nytimes.com/2011/10/30/magazine/the-dangerous-politics-of-internet-humor-in-china.html?_r=1&adxnnl=1&ref=magazine&pagewanted=all&adxnnlx=1319904759-ZbvDOZs+1f/GshTxjA9AiQ), http://www.nytimes.com/2012/01/02/opinion/in-china-the-grievances-keep-coming.html?_r=1&ref=opinion

[5] See: Lokman Tsui, Yongnian Zheng, *Technological Empowerment*, Rebecca MacKinnon. I cannot help but think of the parallels between the government's tacit endorsement of certain 'blowing-off-steam' episodes on sina.com and its periodic encouragement of nationalist anger. E.g., rock-throwing at the Japanese embassy during the Aisan Cup in 2004; busing in protestors to the US embassy after the 2001 EP-3 incident and 1999 Belgrade embassy bombing.

territorial integrity (hence the importance of retaining Taiwan and Tibet), and economic development/ prosperity. The introduction of the Internet in 1994 was initially seen by the Party primarily as a means of furthering economic development. To this date, the government views this as the Internet's main function.[6] Yet economic development, as throughout Chinese history, takes second place to social stability; Chinese history, including that of the Communist Party itself, has long taught that social unrest leads to revolution.[7]

Structure of the control regime

The technical and social apparatus the Chinese government has assembled to control the content of the Chinese Internet permeates every layer of the Internet and deep into the social structure. In terms of organization of government bodies and affiliates, it reflects the dual Party-government structure of the Chinese political system itself. Functionally, it relies strongly upon self-censorship; the control structure is far from monolithic and impermeable, but instead accepts some degree of 'leakage' as long as overall stability is preserved. In accordance with practice in other areas, broad goals are set at the top, but the actual responsibility for implementation is pushed downward and outward to local officials in cooperation with the private sector actors that dominate the Internet landscape and to quasi-NGOs (quangos) that extend, interpret, codify, and carry out the not-always-clearly-specified will of the government. This has the effect of creating a form of bureaucratic competition to see which regions (provinces, municipalities) can devise the most effective, and efficient means of implementing policy directives, though in truth much of the actual censorship is done by personnel within Internet companies.

[6] Internet White Paper 2010, available at http://china.org.cn/government/whitepaper/node_7093508.htm
[7] See, for example, Elizabeth Perry, *Rebels and Revolutionaries in North China* (Palo Alto: Stanford University Press, 1983); Elizabeth Perry and Mark Seldon, eds., *Chinese Society: Change, Conflict and Resistance* (Routledge, 2010); Jonathan Spence, *God's Chinese Son* (W.W. Norton, 1996), Jeffrey Wasserstrom, *Student Protests in Twentieth-Century China* (Stanford, 1991).

The overlapping jurisdictions and authorities of the thirty-plus Party and government organs and quangos that populate the regulatory landscape serve multiple purposes. (Figure 1) The parallel Party-government parallel structure is a function of the Soviet-style Communist system, reflecting the dominance of the Party over government. The overlapping membership of the parallel organs presumably serves to channel and implement political directives and to hide internal debate within the Party organs.[8] It is unclear why so many offices at so many levels are involved in Internet regulation, though officials concede that the system is highly fragmented and coordination very difficult.[9] The extension into local government, and through local government into various ISPs and Internet companies and sites, allows for greater flexibility in implementation, as decisions are made closer to the ground and presumably more closely tailored to local environments and conditions. However, it also results in a greater diversity (or inconsistency) in implementation, as different municipalities and different companies may choose to interpret regulations and guidelines differently.[10] The large number of Beijing-based government bodies and quangos is due to the basing of most of the major national commercial websites and ISPs in Beijing.

The involvement of quangos spares the government the impossible task of monitoring every single posting on the Web. Instead, Internet corporate organizations, citizen volunteer groups, and other semi-autonomous civil society groups take on this task, interpreting guidelines handed down from the central or local government. China does not have civil society in the de

[8] This has been the assumption among China scholars for some period of time not just with reference to Internet control but to broader policymaking. The actual deliberative process behind policymaking at the Politburo level is quite opaque.

[9] I suspect, but have no proof, that is largely a function of bureaucratic creep and the Internet being a relatively new technology. Wang Chen, the head of the State Council Information Office, estimated at a talk at Brookings in December 2011 that about 26 formal government bodies have some degree of jurisdiction or involvement in Internet censorship and regulation. These bodies exist at various levels, federal and local, and action is not coordinated among them; in fact even lines of authority are not clear.

[10] For example, see Rebecca MacKinnon on the variation in strictness of censorship and censorship policies among blog hosts in China. http://firstmonday.org/article/view/2378/2089

Tocquevillian sense. They do not have civic organizations. Rather, civic organizations in China do not exist separate from the state, but instead are often required not only to register but to complement government organizations and functions in providing services and maintaining social order.[11] Each layer of the regulatory structure monitors the one below it, mirroring the *hukou* household registration system from imperial China, in which each unit bore responsibility for the actions of those below it.[12] It also allows the Chinese government to concentrate resources on monitoring the relatively few web portals that capture the vast bulk of Internet traffic, rather than wasting resources monitoring the 'long tail'. These resources, however, are extensive in personnel terms: human rights organizations such as Amnesty International and Freedom House estimate the number of people directly employed by the Chinese government to monitor the Internet at between 40,000-50,000, a number that does not include those employed by private firms such as Baidu (China's Google) and Sina (owner of Weibo.com, China's Twitter).[13]

What this means functionally is that actual interpretation and implementation of the censorship guidelines often occurs outside of government and within companies. While the automated technical censorship such as blocking of IP addresses and DPI filtering of sensitive keywords may occur at the ISP level (and the largest Chinese ISPs are state-owned), the more fine-grained controls – individually reviewing blog posts and microblogs -- occur within Internet

[11] Wang & Zhang 2007, in Min Jiang; Yang chapters 7 and 8 on the lack of civil society within physical society and its emergence on the Internet.

[12] For example, the head of household was held responsible for all wrong-doing by members of his family, so he was incentivized to ensure that his family members followed the rules. The head of the block of households was responsible for the actions of all the households on the block. The head of the village was responsible for the actions of heads of households. And so on up the line.

[13] http://bigthink.com/ideas/how-to-censor-the-internet-in-china-2?page=all; http://whymycountrysucks.com/asia/more-than-50000-chinese-internet-police-responsible-for-internet-censorship/; http://www.guardian.co.uk/technology/2005/jun/14/newmedia.china#article_continue (Figures from 2005 estimate 30,000)

companies that employ entire staffs dedicated to scanning for and deleting content the government deems undesirable.

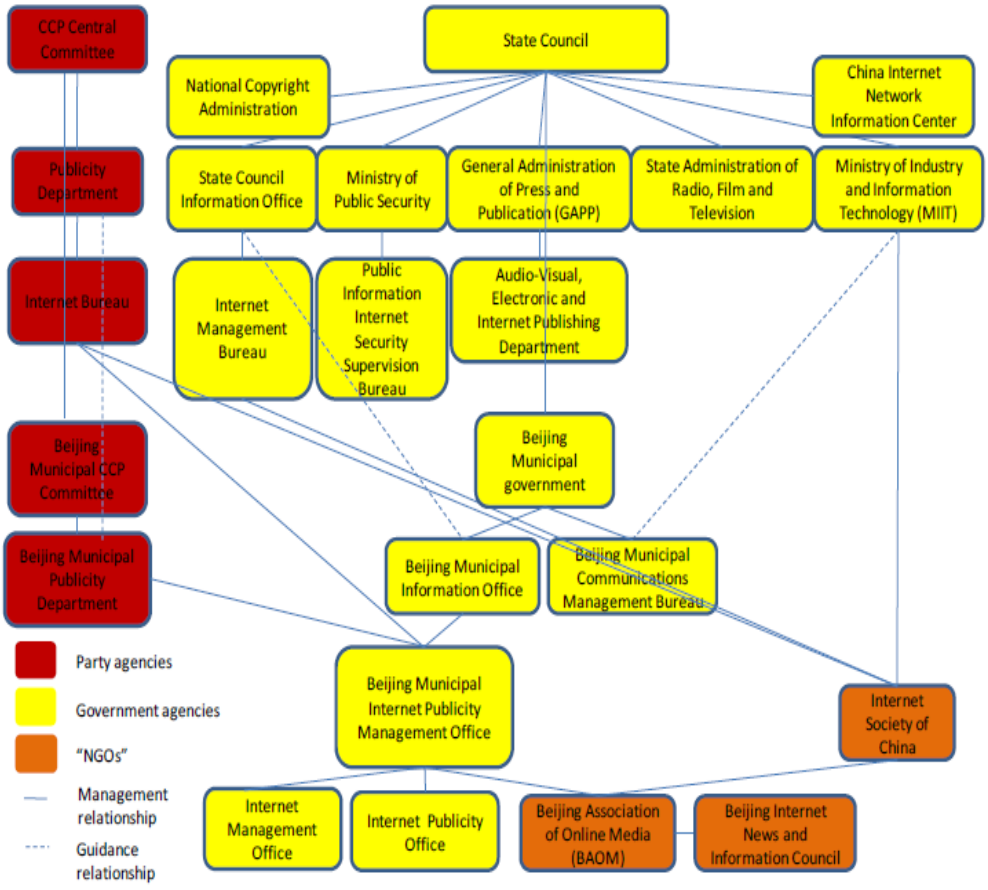


Figure 1[14]

The reliance on self-censorship – on the panopticon, on deterrence – both simplifies the task of the government organs and has potential pernicious effects on society. The benefits to the government of 'outsourcing' responsibility and implementation are clear. The downsides for society bear mentioning. First, there is the potential for over-censorship by corporations and individuals alike: erring on the side of caution. (I suspect the government counts on this.) Studies

[14] China Human Rights Defenders, "Tug of War over China's Cyberspace," March 13, 2009.

have shown that wide variation exists in the censorship policies of major corporations even on known sensitive topics.[15] Second, fear of reprisal may deter individuals from trying to seek out potentially sensitive information, a corollary to self-censorship: not only do individuals restrict what they are willing to say, they restrict what they are willing to risk reading. Third, censorship policies by websites and search engines may not make clear when information is being censored or limited. It is one thing to know content has been deleted from a website, or the website inaccessible, but how do you know what you don't know? Before Google exited the Chinese market, it made many friends in the Chinese netizen community for its policy of explicitly noting when search results were being censored as a result of government restrictions, a policy most Chinese search engines do not follow. Again, this overall panopticon system mirrors the social censorship system that has existed in Communist China for decades; Perry Link, an eminent China scholar, once memorably described the phenomenon as the "anaconda in the chandelier."[16]

Layers: controls at each layer

Discussions of the Great Firewall often assume it is all-encompassing and impenetrable. Ironically, like its namesake the Great Wall, it is neither.[17] The image of an ongoing cat-and-mouse game, or arms race, is far closer to the truth. Moreover, the tussle is not merely over censorship in the sense of availability of information. Much of the tussle is over shaping the discourse—setting the agenda, setting the terms of discussion, determining participants and

[15] See MacKinnon on variation in censorship policies in Chinese blogs; Nart Villeneuve on search engine variation, http://citizenlab.org/wp-content/uploads/2011/08/nartv-searchmonitor.pdf
[16] http://www.asianresearch.org/articles/2599.html
[17] On the historical failings of the 'impenetrable' Great Wall, see Arthur Waldron, *The Great Wall of China* (Cambridge University Press, 1992). In this sense the Great Firewall mitigates one of the major problems of all walls: this one moves and adapts. It's a terrible metaphor. Others have tried to come up with better ones, such as water management systems. (Tsui) So far nothing has stuck.

degree of participation--not just access or deletion. It does not look quite the same as it does in a democracy, but it is nonetheless a form of deliberation.[18]

What China's system of Internet control does do is permit the government a relatively high degree of control that becomes increasingly fine-grained as it moves up through the Internet layers. (Figure 2) As far as I know, no other country has a system of similar scale or scope. China's system creates what is in essence a 'walled garden' in which most citizens can roam freely, without any sense of where the walls are (or that they exist).[19] The perceived freedom within the (unperceived) walls creates the sense of liberalization, reducing pressure on the Party, while allowing for growth of the Internet-driven economic and technology sectors, which further enhances Party legitimacy.

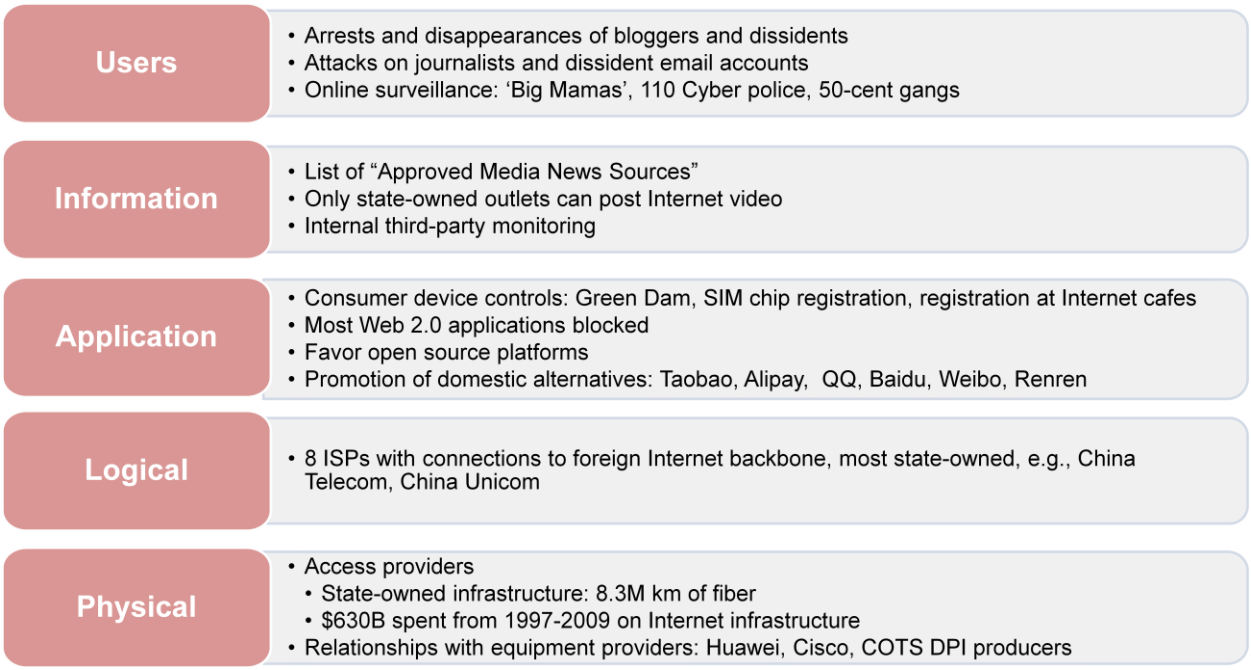
Technologists use a layered model to describe the Internet. The pervasiveness of China's Internet control regime can be seen when the various control mechanisms are mapped against this layers model: controls exist at every layer, with increasing number and variety as one moves up the layers to the information layer, where the most politically and socially sensitive content resides.[20] (Figure 2)

The Internet layers model describes a way of understanding the technical architecture of the Internet.[21] It is often drawn as an hourglass, with a narrow 'waist' that is the logical layer. The implication is that the logical layer has fixed technical protocols that allow for greater technical variation and innovation in the layers above and below. From the bottom up, the layers

[18] Min Jiang, "Authoritarian deliberation on the Chinese Internet," *Electronic Journal of Communication,* Vol. 20, Nos. 3&4, 2010.
[19] For an extensive discussion of the walled garden effect, see Rebecca Mackinnon's writings on networked authoritarianism at http://rconversation.blogs.com/ and her book *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (Basic Books, 2012).
[20] David Clark, *Control Points Analysis* working paper
[21] It seems every computer scientist draws this hourglass slightly differently, with the slightly different degrees of detail at various layers. The details of various protocols are not important for this paper. The description used here is generalized version that most computer scientists will recognize and which will serve for a non-technical paper.

are: physical, logical, application, information, and users. (One could put the "God layer"[22] – government regulation – above users, but given the structure of Chinese society, that would unnecessarily complicate this model.)

Figure 2.



Physical Layer

The physical layer is the hardware that makes up the architecture of the Internet: fibers, copper wires, coax cables, undersea cables, routers and switches, and all of physical infrastructure that the Internet runs on. Although many people think of the Internet as intangible information flows, the "tubes" those bits run through are very real.[23]

[22] Apparently a joke among computer networking types
[23] For an excellent description of the many physical components of the Internet, see Andrew Blum, *Tubes* (NY: Harper Collins, 2012). The title "tubes" refers to a widely mocked statement by Senator Ted Stevens describing the Internet as a "series of tubes".

This physicality presents an opportunity for Chinese regulators, particularly with respect to managing content originating overseas. Most overseas traffic – which presumably contains a higher proportion of potentially undesirable or sensitive content – coming into China passes through undersea cables. These undersea cables provide a natural chokepoint. All of the international undersea cables that go to China terminate at one of three points (one in the south near Guangdong, one near Shanghai, and one in the north in Shandong province).[24] The landing stations seem like a natural place to install filtering technology ('boxes') – the Internet equivalent of border control. All of these cables are controlled by state-owned telecom companies, most notably China Telecom.

The physical layer provides less opportunity for management domestically, as what concerns the government most is content management, and content management done at the physical layer is necessarily blunt. (Egypt's leaders discovered this the hard way during the Arab Spring, when ordering ISPs offline became the only way to shut down discussion.)[25] It is unclear how much China has spent building the Golden Shield project, which is a larger surveillance system that includes a network of cameras and facial recognition software, of which what we call the Great Firewall is only a portion. Unsurprisingly, no figures have been published.[26]

Logical Layer

The logical layer is comprised of the technical protocols (code) that define how the Internet works. Generally speaking, this refers to the TCP/IP (Transmission Control Protocol/

[24] See http://www.cablemap.info/ for a map of landing sites and list of cables. Hong Kong is also a major termination point but as it is subject to different Internet management policies than China proper, I exclude it from this discussion.
[25] http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml
[26] One report that did leak out was a presentation from Cisco, believed to have been made in support of a bid to provide hardware for the Golden Shield project, detailing the various components involved and the structure of the state security bureaus. Cisco Systems, "Overview of the Public Security Sector", 2002.

Internet Protocol) suite. The Internet was designed to be 'neutral', an end-to-end model with no intelligence in the middle of the network, no promise of successful transmission ("best-effort"), and no preference for any particular user or content. In simplified terms, the TCP/IP suite handles the process of opening a connection, transmitting data across the networks, and receiving it at the other end. (By analogy, imagine it as process of writing the address on the envelope, putting the letter in the envelope, dropping it in the mailbox, the various routing and delivery actions required to get the letter to the recipient, and opening the letter at the other end.)

The description given above is the original design of the Internet. In the decades since, as followers of the "Net Neutrality" debates know, more intelligence has moved into the middle of the network. In China, the best-known part of the control – blocking of IP addresses and filtering based on sensitive keywords such as "Taiwan independence" or "Falungong" – has been inserted in this layer.[27]

China's eight major ISPs with connections to the foreign Internet backbone, as well as the myriad smaller ones, are subject to strict government controls. The largest ISPs, China Telecom and China Unicom, are state-owned. The rest are required to register and are subject to content regulations that are handed down from the State Internet Information Office or various local agencies, which are often issued in the form of memorandum directing the removal of content.[28] (I assume, but have not verified, that peering arrangements may also play a role in ensuring 'good behavior' by any small ISPs.)

[27] *Access Denied*, *Access Controlled*, various ONI publications

[28] There is an excellent archive of examples of these censorship instructions, which are issued to the media and/or Internet companies by various organs of the central and sometimes local government, that have leaked at ChinaDigitalTimes.com. These are often referred to as directives from the "Ministry of Truth" by Chinese journalists and Netizen wags.

The Firewall employs a variety of means to restrict access to 'sensitive' information, including but not limited to (and some of these probably belong in the application layer discussion but are bundled here for convenience):

- DNS: false or incorrect addresses, restricting access to some DNS servers
- Control of routes, especially at borders
- Blocking of websites and ports (IP blocking)
    - Blocking of specific websites, such as falungong.org
    - Blocking of ports known to be used by circumvention software, such as some commercial VPNs[29]
- Deep packet inspection (DPI) to restrict certain sensitive keywords
    - Use of commercial DPI software, e.g. Sandvine, Netsweeper, Websense, McAfee's SmartFilterii
    - Lists of keywords to be added/ deleted are updated frequently and distributed to both ISPs and relevant information layer players (search providers, etc.)
- TCP resets: users requesting sensitive information are simply 'booted' off the system by returning a TCP reset packet. Only certain searches will trigger a TCP reset; sometimes the reset will only limit network access very briefly, while sometimes it has been reported that network access for that IP address is rendered unavailable for an hour or more.

Application Layer

[29] This includes both free and paid VPNs such as Freedur and Witopia http://www.streetarticles.com/international/the-beginning-of-the-end-blocked-vpns-in-china as well as TOR bridges

The application layer is probably the layer most end-users are most familiar with, as this is how users actually interact with the Internet. It consists of the programs we use every day: e-mail, the Web, voice over IP, etc.

The control system begins to gain nuance at the application layer. The layers model used here is a generalization, so for our purposes it will include both the platforms and the consumer devices upon which end-users access the Internet. Mirroring its dual goals of social stability and economic growth, the Chinese government's approach to Web 2.0 applications is also twofold: block most foreign social media applications, as they are not as easily controlled, and promote domestic alternatives, which are far more easily monitored. The Arab Spring of 2011 confirmed many of the Chinese government's worst fears about the potential for social media such as Facebook and Twitter for fomenting unrest. Both of those sites have been blocked in China for years. Instead, China has actively promoted domestic alternatives, which because they are owned by Chinese companies headquartered on Chinese soil (and with servers within the borders), are far easier to control.[30] Almost every major Western site has a Chinese equivalent, which at least in part due to language barriers (and/or being blocked) is dominant in its sector in China:

- Facebook = Renren
- Twitter = Sina Weibo (microblogs, called 'weibos', also exist on Tencent, Sohu, etc.)
- Google = Baidu
- eBay = Taobao
- PayPal = Alipay
- MSN Live/ Yahoo Messenger/ Google Talk/ AIM / ICQ/ assorted other instant messaging programs = Tencent QQ

[30] Jack Goldsmith and Tim Wu, *Who Controls the Internet* (Oxford University Press, 2006). Goldsmith and Wu argue that governments have the most leverage over companies with assets within their borders.

- Skype = TOM Skype[31]
- Youtube = Youku

Consumer devices are also subject to control. Many users in China still access the Internet through either Internet cafes or on their phones. Internet café patrons are required to register using their national identity cards (equivalent to a photo ID containing one's social security number, current address, and birth certificate) each time they want to access the Internet. Internet cafes are required to keep logs of users. The computers in those cafes also have surveillance software pre-installed. (See below, Green Dam)

Those accessing the Internet on their cell phones are no better off, as all SIM chips must also be registered using a national identity card, and photos of the registrant are taken at time of purchase and filed with the SIM card registration forms. Moreover, in 2011 the Chinese government announced that 'for purposes of social stability' it would begin monitoring large and unusual concentrations of people by tracking unusual patterns of cell phone activity/ pinging of cell towers.[32] What was not mentioned in the government statement, however, was the connection to registration of SIM cards, which would mean that the government would not only know how many cell phones were in a given place at a given time, but also their owners.

Another control mechanism that received much media attention was the Green Dam project. Originally announced in June 2009 as a mandatory program to have content-control software for Windows pre-installed or shipped on CDs with all new personal computers sold in mainland China, the directive was later modified to be voluntary for end-users, and then

[31] See Nart Villeneuve, "Breaching Trust: An analysis of surveillance and security practices on China's TOM-Skype platform," 2008.
[32] http://www.guardian.co.uk/world/2011/mar/04/china-tracking-beijing-citizens-mobiles

suspended indefinitely for home and business use.[33] Schools, Internet cafes, and other public use computers, however, are still required to run the software.

Information Layer

The information layer is the content on the Internet. It is the news articles, blog posts, microblog posts and Facebook updates, photographs, Youtube videos, music and movies, etc.

The most elaborate and extensive control mechanisms exist at the information and user layers. Regulatory bodies use a variety of tools of control:

- Licenses, registrations, and permits
  - Online forums must register with the Ministry of Industry and Information Technology (MIIT) as well as other subsidiary bureaus. As with any bureaucracy, though perhaps expanded to Kafka-esque proportions in China, a wide variety of permits are required to conduct day-to-day business. These permits, licenses, and registrations provide the various government agencies multiple, repeated, ongoing opportunities to signal, regulate and tweak behavior.
  - Only companies partially or wholly owned by the state can provide Internet audio and video services, and only with permits from SARFT and MIIT, although this rule is widely flouted
- Online forums must have stand-alone servers placed in a room of a company (ISP or web host, generally) certified by Communications Management Bureau, so as to provide easy access for censors
- Cyber 110 'virtual police'

[33] http://en.wikipedia.org/wiki/Green_Dam

- Each website displays on its front page in an easily accessible location, the icon of the cyber police, which links directly to the website of the local cyberpolice. As most of the major Chinese websites are headquartered in Beijing, this is generally www.bj.cyberpolice.cn. The site features the cartoon mascot with links to forms for citizens to report violations of Internet regulations, e.g., pornography, gambling, phishing, viruses, etc. The website is monitored 24/7, and those reporting are required to submit their real names and identifying information.
- These cyber police are part of the estimated 40,000-50,000 personnel directly employed by the government to monitor the Internet

• An internal third-party monitoring mechanism and point system for commercial ISPs and websites
  - Commercial websites are expected to actively promote a "harmonious society" and other government themes and propaganda
  - The Beijing Municipal Internet Publicity Management Office issues and deducts points for compliance with (or failure to comply with) both specific and generalized instructions. E.g., posting of articles from unofficial sources, articles with a negative tone toward the government result in lost points. Those websites falling below a certain (unspecified) number of points are closed down, and required to replace key members of the staff.[34] Points can also be earned for following some directives, as with instructions to feature articles promoting various attitudes[35]

[34] Tug of War Over China's Cyberspace 16
[35] Again, see archive of the Ministry of Truth at China Digital Times online

  - Compliance is also a function of response time. Websites are given a certain amount of time to comply with various types of instructions, e.g., five minutes to remove a post if given the URL, ten minutes if given only the article title, etc.[36]

- A list of "Approved Media News Sources" from which websites may reproduce content. As with other regulations, it is implied but not stated that news from other sources are *not* approved and therefore cannot be reproduced. No list of 'not-approved' sources exists. The failure to specify again increases government flexibility, and encourages self-censorship/ erring on the side of caution.
- Internal third-party monitoring is required by Beijing Municipal Internet Publicity Management Office. Each website must set up a separate unit or working group parallel to the news center (editorial department) led by someone of rank no lower than company director, who reports directly to the editor-in-chief.[37] The third-party monitor serves as another liaison, parallel to the existing one who is the first point of contact between the Management Office and the website, and also as a check to make sure instructions are carried out.
- Self-regulation is also carried out at this layer through quangos such as the Internet Society of China or various industry groups, which come up with codes of conduct to which all must adhere. These guidelines are, unsurprisingly, frequently look very much like government guidelines, and if anything, are often stricter due – again erring on the side of caution.

Users (not really a layer)

[36] Tug of War 15, 40
[37] Tug of War 18

The portion of the control system the West most often hears about other than the Great Firewall is the intimidation tactics used against dissidents and journalists. However, controls at the user layer are not limited to those imposed by the state on specific targeted users. The state also turns users against each other, often using quangos as organizers.

Among the better-known controls imposed on users:

- Arrests, intimidation, and disappearances of various dissidents, e.g., Ai Weiwei, Gao Zhisheng, Chen Guangchen, Stainless Steel Mouse
- Demanding e-mail providers hand over account information, such as the Yahoo Shi Tao case in which dissident Shi Tao was jailed for ten years because Yahoo handed over his email records to the Chinese government[38]
- Hacking into dissident and journalist e-mail accounts
- Spear-fishing[39]

More creatively, the Chinese state has also turned its citizens against one another. Current estimates of the total number of people employed directly by the government in Internet surveillance range from 30,000-50,000[40], with likely another multiple of that employed by the private sector. Rebecca Mackinnon, an expert on Chinese Internet censorship, testified before Congress in December 2011 estimating that Sina Weibo (Twitter) employs approximately 1,000 people to monitor and censor users.[41] This may account for the over one million pieces of information a day (blog posts, news articles, photos, etc.) that are removed each day from the

[38] http://rconversation.blogs.com/YahooShiTaoLessons.pdf
[39] "The 10 Tools of Online Oppressors," Committee to Protect Journalists, May 2, 2011
[40] http://whymycountrysucks.com/asia/more-than-50000-chinese-internet-police-responsible-for-internet-censorship/
[41] http://newamerica.net/publications/resources/2011/testimony_of_rebecca_mackinnon_to_the_house_subcommittee_on_africa_global

Chinese Internet.[42] Yet even this army of censors is sometimes not enough to cope with floods of information. In early April 2012, Sina Weibo and Tencent Weibo, the two largest microblogging sites in China, shut down comments[43] to prevent users from further spreading rumors of a military coup in Beijing after Bo Xilai, the party boss from Chongqing and leader of the 'new left' (neo-Maoist) faction within Chinese politics, was sacked. Over a dozen additional websites were shut down completely for spreading the rumors.[44] However, in addition to the government censors and those employed in-house, there are additional 'citizen' police who help monitor the Internet:

- "Internet Surveillance Volunteers" must report 50 items of "harmful" information each month with URLs and screenshots. These are recruited, unpaid positions.
- "50-cent gang" of Internet commentators "guide public opinion" from a surveillance center at Beijing IPMO, with 1-3 per major commercial website. These are citizen volunteers who are paid 50 cents RMB (about 8 cents US) per post to write things favorable to the government and to attempt to shift online discussion in the direction the government wishes, whether it be to promote a particular attitude toward a topic or to not discuss another. Generally speaking, the 50-cent gang members specialize in a particular type of site or forum.[45]
- Citizen reporting through the 110 Cyber police
- Big Mamas, online forum 'moderators' who monitor discussions and delete posts and/or posters based on content (these are generally employed by the web companies)

[42] FT.com, December 20, 2010, statement by Wang Chen at year-end reporting that over "350 million pieces of harmful information, including text, pictures, and video, had been deleted".
[43] Notice published on Sina Weibo announcing the shutdown of the comment function: http://www.weibo.com/z/notice20120331/
[44] Stephen Chen and Priscilla Jiao, "Microblog sites punished after coup rumors," South China Morning Post, April 1, 2012.
[45] Both Internet Surveillance Volunteers and 50-cent gangs are from Tug of War, although the 50-cent gangs have been widely documented elsewhere (as well as thoroughly mocked on the Chinese Internet)

III. Conclusion and further research

All of the prior discussion of censorship and control would suggest that the Chinese Internet is a rather dull and monotonous arena, filled with little but official news and propaganda. In fact, nothing could be further from the truth. Much of what is on the Chinese Internet is opaque to Western users simply because of the language barrier, but also due to cultural barriers. There is actually much lively discussion and debate – even about politics – that occurs, though often commentary is masked through the use of homophones and puns, humor, cartoons, images, and other means.[46] In other instances, however, particularly when it channels debate on a topic that the government wants in the public eye, the discussion can be much more direct and forthright.

Thirty-plus years of economic transformation have changed Chinese society. The state no longer controls all resources nor political and social debate. The government recognizes this, and allows much of the social turmoil to vent itself online – within bounds. After much speculation over whether weibo.com (China's Twitter) would be shut down earlier in 2011, tacit approval was given when various government ministries actually opened accounts. You can now follow the cyber police, the People's Liberation Army, the foreign ministry, and various other government agencies and officials on Sina.com. (In fact, as in the US, the contents of various politicians' personal Weibo accounts have also led to scandals.)[47] It was widely understood that the government had chosen to use this as a way to monitor and channel public opinion rather than risk a backlash by repressing it.[48]

[46] http://www.nytimes.com/2011/10/30/magazine/the-dangerous-politics-of-internet-humor-in-china.html?_r=1&adxnnl=1&ref=magazine&pagewanted=all&adxnnlx=1319904759-ZbvDOZs+1f/GshTxjA9AiQ
[47] http://chinadigitaltimes.net/2011/06/chinese-politician-caught-in-social-media-scandal/
[48] http://news.ichinastock.com/2011/09/10-reasons-why-sinas-regulatory-risks-are-overblown/

For example, in late 2011 there was an incident that provoked much commentary and soul-searching on the Chinese Internet and in mainstream media, a result of a gruesome video (taken by a security camera) that was posted onto Youku, China's version of Youtube. A two-year-old girl in Foshan, Guangdong, was hit by a van and left lying in the road, injured but alive. Eighteen people walked or bicycled by, some pointedly not looking at her, some looking over and then walking away, until *another* van ran her over again and also drove off. Again, more people passed by without stopping. Finally, a street-cleaning woman stopped to pull her out of the street and get her help, but by then, it was too late. The child was declared brain dead at the hospital, which presumably would not have happened had someone pulled her out of the road after the first vehicle hit her. One of the 18 passersby, asked by a journalist why he had not stopped to help, replied, "That wasn't my child. Why should I bother?" and the driver of the second vehicle explained why he had driven away by stating that if the child had died, he would only be liable for RMB20,000 (~USD3,174), but if she had lived, he could have been liable for hundreds of thousands of RMB (because he would have been required to pay hospital bills and support her for the rest of her life if she were disabled).

The incident provoked both public outrage and a national discussion about Chinese morality, whether Chinese culture encourages indifference to strangers, and the stupidity of laws and judges that reinforce both. Many online commentators expressed outrage at the death but also understanding of the reasoning behind the passersby's inaction, citing a well-known case in Nanjing in which a judge ruled against a good Samaritan named Peng Yu, who had taken an old woman who had fallen on the street to the hospital and waited to see if she was all right, was later accused by the woman's family of causing her fall. The judge reasoned that "Peng must be

at fault. Otherwise why would he want to help?" and that it was against "common sense" to do so if he were not guilty.[49]

The Internet clearly played a major role in the publicizing of the Foshan toddler incident as well as in the later discussion. Within hours of the incident, Xinhua, China's official news agency, reported that there were over two million posts related to the toddler on Sina Weibo.[50] Many of these commented on the 'sickness' in Chinese society, and noted that the fact the trash-collector woman's actions were considered unusual rather than normal was a reflection of the perversion of Chinese society.[51] The video had been viewed over 2.8 million times within a few days of the incident, and as of April 2012 had over 3.8 million views.[52] Perhaps predictably, a fake Sina Weibo account purportedly belonging to the toddler's mother was set up and began blogging as well.[53] Various government officials seized the opportunity to continue an ongoing campaign against excessive materialism in Chinese society, an ongoing concern for social stability as the gap between rich and poor widens.[54] (Conveniently, diverting the discussion away from an emphasis on getting rich and to social morals neatly takes the spotlight off ongoing

[49] For discussion of the Foshan toddler incident, see: http://www.guardian.co.uk/world/2011/oct/17/toddler-hit-and-run-china; http://www.theatlantic.com/international/archive/2011/10/on-that-horrible-toddler-death-story-from-china/247280/; http://www.chinadaily.com.cn/china/2011-10/24/content_13959139.htm; http://www.guardian.co.uk/commentisfree/2011/oct/22/china-nation-cold-hearts; http://www.theatlantic.com/international/archive/2011/10/from-chinese-readers-and-others-about-the-dead-chinese-toddler/247349/

[50] http://news.xinhuanet.com/english2010/china/2011-10/21/c_131204564.htm

[51] http://thelede.blogs.nytimes.com/2011/10/17/chinese-debate-aiding-strangers-after-toddlers-death/?scp=1&sq=foshan%20toddler&st=cse; http://www.nytimes.com/2011/10/19/world/asia/toddlers-accident-sets-off-soul-searching-in-china.html?scp=2&sq=foshan%20toddler&st=cse&gwh=956AF15057D1ADB90FEC76A877818359

[52] http://v.youku.com/v_show/id_XMzEzMDY4OTcy.html

[53] http://thelede.blogs.nytimes.com/2011/10/21/mother-of-toddler-who-was-run-over-says-microblog-is-a-fake/?scp=3&sq=foshan%20toddler&st=cse

[54] http://news.xinhuanet.com/english2010/china/2011-10/21/c_131204564.htm
Notable incidents that have provoked government crackdowns on excessive materialism include the reality TV dating show that featured a contestant stating she would 'rather cry in the back of a BMW than smile on a bicycle' as she defended her desire to find a rich man. http://www.nytimes.com/2012/01/01/world/asia/censors-pull-reins-as-china-tv-chasing-profit-gets-racy.html?_r=1&scp=1&sq=culture%20and%20control&st=cse; this and other incidents led to a crackdown on 'entertainment shows on TV that restricted them to only a few hours a week per station.

criticism of the corruption and cronyism that has channeled a large portion of China's economic gains to friends and family of government officials.)

Clearly, the Internet and social media, as the fastest-moving component of the Chinese Internet, will play a large role in future political and social discussion. The current Internet control system is evolving to keep up with changes in the Internet, and attempting to manage it, but it seems clear that some degree of troublesome content will continue to exist.

An issue for further research is whether the Internet and particularly social media, which over 50% of Chinese Internet users have active accounts on, will in fact help liberalize and democratize China. This remains to be seen. Using the "Iron Curtain 2.0" (the idea the Internet is a "Trojan Horse" that will topple the government from within) lens to understand China's view of the Internet may be false.[55] States can use online activism to bolster regime legitimacy by showing responsiveness, at least to low-level complaints such as corruption by local officials, thereby allowing the disgruntled to blow off steam. Allowing expression of a range of opinions online may help build support for factions within the Chinese political system, e,g, giving the pro-liberalization camp ammunition in their arguments, as long as criticism stays within limits. The alternative, cutting off communication and protest altogether, leads to hard and soft-liners standing together against the common enemy.[56] In other words, as some have argued, it is possible that "the Internet is a subtle and effective tool through which the CCP is actually prolonging its rule, bolstering its domestic power and legitimacy, while enacting no meaningful

[55] Lokman Tsui, "The Great Firewall as Iron Curtain 2.0: the implications of China's Internet most dominant metaphor for U.S. Foreign Policy," Paper delivered at the 6th annual Chinese Internet Research Conference, June 13-14, 2008, Journalism and Media Studies Center, HK University, cited in MacKinnon, "Networked Authoritarianism", p7

[56] Yongnian Zheng, *Technological Empowerment: The Internet, State, and Society in China* (Stanford University Press, 2008, referencing Albert Hirschman, *Exit, Voice and Loyalty* (Cambridge: Harvard University Press, 1970).

political or legal reforms."[57] Use of "authoritarian deliberation" in "deliberative venues" to bolster regime legitimacy in authoritarian regimes may lead to democratization, but could also easily stabilize and prolong rule by increasing legitimacy.[58]

It would also be interesting to see how the greater prevalence and integration of the Internet into Chinese citizens' everyday lives have altered their expectations for what type of voice they are entitled to, and what the consequences for future political discourse would be. The general tenor of discussion on the Chinese Internet is far freer and more critical than that which exists in 'physical' China, and a generation of digital natives who have grown up feeling relatively free to comment and criticize, and who regard Internet access as a right, may well have far lower tolerance for government efforts to control discourse on the Internet – or more broadly.

[57] MacKinnon, *Networked Authoritarianism*, p 11
[58] Baogang He and Mark E. Warren, "Authoritarian Deliberation: The Deliberative Turn in Chinese Political Development," paper presented at APSA Annual Meeting, Boston, August 28-31, 2008