Networked Authoritarianism in China and Beyond:

Implications for global Internet freedom

By Rebecca MacKinnon
Bernard L. Schwartz Senior Fellow, New America Foundation

e-mail: rmackinnon@post.harvard.edu

A paper presented at:

Liberation Technology in Authoritarian Regimes

Sponsored by the Hoover Institution & the Center on Democracy, Development and the Rule of Law (CDDRL), Stanford University

October 11-12, 2010

Acknowledgments:

The author would like to thank the Open Society Institute Fellowship Program and Princeton University's Center for Information Technology Policy, whose support made this paper possible. All conclusions are of course the author's sole responsibility.

To mark the twentieth anniversary of the fall of the Berlin Wall, a German arts organization launched a website called the "Berlin Twitter Wall." It was a playful way to invite a global conversation in cyberspace about what happened before and after the Iron Curtain crumbled in November 1989. Animated speech bubbles scrolled like a stock ticker across a brightly-colored, cartoon-like, graffiti-decorated wall. Anybody, anywhere on the Internet could use Twitter to post a comment into one of the speech bubbles.[1]

Within a few days of launching, the website was over-run by messages in Chinese. Instead of talking about the end of the Cold War and the fall of communism in Europe, Chinese Twitter users had hijacked the site to protest their own government's Internet censorship. One wrote: "My apologies to German people a million times [for taking over this site]. But I think if Germans learn about our situation, they would feel sorry for us a million times."[2]

Twitter, along with hundreds of thousands of other websites, is blocked in China. What that means more precisely is that if you try to visit Twitter.com from inside China, your browser gives you an error message saying the site can't be found. Still, a growing community of Chinese Internet users are so determined to access Twitter and hold uncensored conversations with people around the world, they've acquired the technical skills to circumvent this blocking system – widely known as the "great firewall of China."

In late January 2010, Secretary of State Hillary Clinton – who two months before had stood at the Berlin Gate with other world leaders to celebrate the the 20th anniversary

---

[1] See http://www.berlintwitterwall.com/, accessed August 13, 2010.

[2] Agence France Presse, "China blocks 'Berlin Wall' Twitter page: organizers" October 29, 2009, accessed August 13, 2010 at: http://www.google.com/hostednews/afp/article/ALeqM5jO_0yPfQ4S1zZxeY9P4aHIt07qxQ

of the fall of the Berlin Wall – gave a 45-minute speech on "Internet Freedom." She spelled out how one single, free and open global Internet is an essential prerequisite for freedom and democracy in the twenty-first Century. "A new information curtain is descending across much of the world," she warned. "And beyond this partition, viral videos and blog posts are becoming the samizdat of our day."[3]

But can we assume that Chinese authoritarianism will crumble as easily and rapidly as the Iron Curtain crumbled two decades ago? This paper examines why it is unwise to make such an assumption about the Internet in China or in other repressive regimes, and discusses some of the difficult issues of government policy and corporate responsibility that must be tackled in order to ensure that the Internet and mobile technologies can fulfill their potential for liberation and empowerment.

The rise of Chinese "networked authoritarianism"

When an authoritarian regime embraces and adjusts to the inevitable changes brought by digital communications technologies, the result is what I call "networked authoritarianism." In the networked authoritarian state, while one party remains in control, a wide range of conversations about the country's problems nonetheless rage on websites and social networking services. The government follows online chatter, and sometimes people are even able to use the Internet to call attention to social problems or injustices, and even manage to have an impact on government policies. As a result, the average person with Internet or mobile access has a much greater sense of freedom – and may even feel like they have the ability to speak and be heard – in ways that weren't

[3] Hillary Rodham Clinton, "Remarks on Internet Freedom," January 21, 2010, accessed August 13, 2010 at: http://www.state.gov/secretary/rm/2010/01/135519.htm

possible under classic authoritarianism. At the same time, in the networked authoritarian state there is no guarantee of individual rights and freedoms. People go to jail when the powers-that-be decide they are too much of a threat – and there's nothing anybody can do about it. Truly competitive, free and fair elections do not happen. The courts and the legal system are tools of the ruling party.

As part of a networked authoritarian society, China's 400 million Internet users are managing to have a lot more fun, feel a lot more free, and are a lot less fearful of their government than was the case even a decade ago. At the same time, thanks to home-grown engineering talent plus lots of help from American and European multinationals, the government has so far managed to keep tabs on enough people enough of the time, and censor and manipulate enough online conversations, that nobody has been able to organize a viable opposition movement. According to the Dui Hua Foundation, in 2008 arrests and indictments on charges of "endangering state security" – the most common charge used in cases of political, religious, or ethnic dissent – more than doubled for the second time in three years.[4] The average Chinese person, however, rarely encounters information about such trends. This in turn makes it much less likely that a critical mass of Chinese citizens would see the need for rapid political change. The system doesn't control everybody all of the time, but it is effective enough that even most of China's best and brightest aren't aware of the extent to which their understanding of their own country – let alone the broader world – is blinkered and manipulated. All university students in China's capitol now have high-speed Internet access. But when a PBS documentary crew went onto Beijing university campuses a couple years ago and showed students the iconic

[4] "Chinese State Security Arrests, Indictments Doubled in 2008," *Dui Hua Human Rights Journal*, March 25, 2009, at: http://www.duihua.org/hrjournal/2009/03/chinese-state-security-arrests.html

1989 photograph of a man standing in front of a tank, most didn't recognize the picture at all.[5] Networked authoritarianism explains why.

Political power in the Network Society

In 1996, as the Internet was just becoming commercially available to ordinary households and businesses beyond the developed, democratic world, communications scholar Manuel Castells published his seminal book, *The Rise of the Network Society*. Castells defined the modern "network society" as "a society in which key social structures and activities are organized around electronically processed information networks."[6] Fourteen years later, the Internet is seeping more deeply into our personal, professional, and political lives with each passing week. Internet and telecommunications companies, plus everybody who creates or distributes web content, have built a virtual place we've come to know as "cyberspace." It has become an extension of human activity. Millions of people around the world can no longer imagine life without it. As technologies grow more sophisticated and the Internet gets ever-more connected not just to our computers and our phones but also to our appliances, vehicles, and homes, our dependence on digital networks will only grow.

In his latest book, *Communication Power*, Castells documents how different social actors have in the past decade used communications and media networks to "program" the way in which people understand their world, and by extension shape their understandings of what is or isn't possible for them to do. He provides examples of

---

[5] "The Tank Man," PBS.org, April 11, 2006, accessed on August 13, 2010 at: http://www.pbs.org/wgbh/pages/frontline/tankman/view/

[6] Manuel Castells, *The Rise of the Network Society, Second Edition (with a new preface)*. (Wiley-Blackwell, 2010).

popular movements and grassroots campaigns in different parts of the world – from China to Spain to the United States – in which "insurgent communities" have succeeded in "reprogramming" public understanding of issues by using the Internet for "autonomous construction of meaning." This "reprogramming" has in a number of instances brought about concrete policy change or decisively influenced elections.[7] Castells is enthusiastic and optimistic about the democratizing power of the Internet. Yet he concludes with a warning: "autonomous construction of meaning can only proceed by preserving the commons of communication networks made possible by the Internet…this will not be an easy task - because the powerholders in the network society must enclose free communication in commercialized and policed networks, in order to close the public mind by programming the connection between communication and power."[8]

Independent activists and pro-democracy movements may have won some early skirmishes, but one cannot assume that their adversaries will remain weak and unskilled in the navigation and manipulation of digital communications networks. In fact, governments and others whose power is threatened by digital insurgencies are learning quickly: pouring unprecedented resources into building their capacity to influence and shape digital communications networks in direct as well as indirect ways. As Stanford's Larry Diamond put it: "It is not technology, but people, organizations, and governments that will determine who prevails."[9]

In the broader contest for freedom and control of the network society, making assumptions about the final outcome, then formulating policy and activism strategies

---

[7] Manuel Castells, *Communication Power,* (Oxford University Press, 2009)
[8] *Ibid.,* pp. 431-2
[9] Larry Diamond, "Liberation Technology, *Journal of Democracy* Volume 21, Number 3 July 2010, p. 82.

based on such assumptions, is no wiser than it would have been for a Brazilian soccer fan to have to bet his children's college fund on a Brazilian victory in the 2010 world cup after only a couple of first-round games had been played.

Recent scholarship on the Internet and politics in China

In the public discourse about the Internet and repressive regimes, Western policymakers and activists frequently use Cold War-era metaphors in ways that are similar to Secretary Clinton's likening of blogs to Soviet-era *samizdat*. Such metaphors are strongest in the policy discourse and news coverage related to Chinese Internet censorship, often dubbed the "Great Firewall of China."[10] The Hong Kong-based communications scholar Lokman Tsui has criticized this "Iron Curtain 2.0" lens through which many in the West seek to understand the Chinese government's relationship with the Internet.[11] "Strategies to break down the Great Firewall," he writes, "are based on the belief that the internet is a Trojan Horse (another metaphor!), that eventually will disempower the Chinese state from within and topple the authoritarian government, as the barbarians in previous times have done for China, and as international broadcasting has done with regard to ending communism in the Cold War."[12] Tsui argues that this framework for understanding the impact of the Internet on Chinese politics is not

[10] As Tsui notes (see next footnote) the first known usage of this term was by Geremie Barmé and Sang Ye, "The Great Firewall of China," *WIRED* Issue 5.06, June 1997, accessed on August 13, 2010 at: http://www.wired.com/wired/archive/5.06/china.html

[11] 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 Centre, Hong Kong University, accessed August 12, 2010 at: http://jmsc.hku.hk/blogs/circ/files/2008/06/tsui_lokman.pdf

[12] *Ibid.,* pp. 8-9.

consistent with the growing body of empirical research, and is therefore likely to result in failed policy and activism strategies.

Guobin Yang, who began researching Chinese online discourse even before the Internet first became commercially available there in 1995, has concluded that in spite of China's increasingly sophisticated system of censorship and surveillance, the Chinese Internet is nonetheless a highly "contentious" place where debate is fierce, passionate, and also playful.[13] After analyzing numerous cases in which Chinese Internet users succeeded in bringing injustices to national attention, or managed to cause genuine changes in local government policies or official behavior, Yang argues that the Internet has brought about a "social revolution, because the ordinary people assume an unprecedented role as agents of change and because new social formations are among its most profound outcomes."[14] The revolution he describes is being waged mainly by Chinese people acting *within* the "Great Firewall."

In examining the use of information and communications technologies (ICTs) by China's "have-less" working classes, Jack Linchuan Qiu documents how Internet and mobile use has spread down to the "lower strata" of Chinese society. This development has given birth to a new "working-class network society" that provides China's less fortunate with tools for mobility, empowerment and self-betterment. However, he also describes how "working class ICTs" provide new levers for government and corporations to organize and control a new class of "programmable labor."[15] While Chinese workers have been able to use Internet and mobile technologies to organize strikes and share

[13] Guobin Yang, *The power of the Internet in China: Citizen activism online* (Columbia University Press, 2009).
[14] *Ibid., p. 213*
[15] Jack Linchuan Qiu, *Working-Class Network Society: Communication Technology and the Information Have-less in Urban China,* (MIT, 2009)

information about factory conditions in different parts of the country, Qiu concludes: "working-class ICTs by themselves do not constitute a sufficient condition for cultural and political empowerment. Given the early formative stage of the technosocial emergence, it still has to involve larger segments of the urban society, including elite members, mass media, and institutionalized forces, especially the state."[16]

In his book *Technological Empowerment: The Internet, State, and Society in China*, Yongnian Zheng points out that the success or failure of online activism in China depends on its scope and focus, and that some online activism – particularly at the local level, or targeting specific policy issues over which there are divisions or turf-wars between different parts of the government – can actually serve to bolster regime legitimacy.[17] The most spectacularly unsuccessful online movements (and the ones leading to the most brutal crackdowns both online and offline) tend to be those that advocate various forms of political "exit," including calls for an end of one-party rule by the Chinese Communist Party, and greater political autonomy or independence for particular ethnic or religious groups. When a movement or group challenges the regime's overall legitimacy, the people involved with it can expect to be silenced – either through censorship, intimidation, or arrest depending on the situation – because all power-holders in the system have a common interest in doing so. "When the regime is threatened by challengers," Zheng writes. "The soft-liners and hard-liners are likely to stand on the same side and fight the challengers."[18] On the other hand, successful online movements in China are usually characterized by what Zheng calls the 'voice' option, or what other

[16] *Ibid., p. 243*
[17] Yongnian Zheng, *Technological Empowerment: The Internet, State, and Society in China,* (Stanford University Press, 2008)
[18] *Ibid., p. 164*

political scientists call the "cooperation option." Such online insurgencies actually provide ammunition to reformist leaders or liberal local bureaucrats in their power struggles against hard-line conservative colleagues. "Voice" activism helps reduce political risks to reformist officials, who can point to online sentiment and argue that without action or policy change there will be more unrest and public unhappiness. Zheng writes: "The voice does not aim to undermine or overthrow the state. Instead, through a voice mechanism, the state can receive feedback from social groups to respond to state decline and improve its legitimacy."[19]

Thus, rising levels of online activism in China cannot automatically be interpreted as a sign of regime instability or vulnerability. Nor do rising levels of online activism necessarily signal impending democratization. One must examine what kind of online activism is succeeding and what kind of online activism is failing. If "voice" activism is for the most part succeeding while "exit" activism is systematically being stifled and crushed – thanks to high levels of systematic censorship and surveillance, in addition to the lack of an independent or impartial judiciary – one can in fact conclude that the Chinese Communist Party has adapted to the Internet much more successfully than most Western observers realize. The "Iron Curtain 2.0" mentality criticized by Tsui may indeed have blinded many Western policymakers, human rights activists, and journalists to what is really happening in China. In 2005 *New York Times* columnist Nicholas Kristof wrote breathlessly: "it's the Chinese leadership itself that is digging the Communist Party's grave, by giving the Chinese people broadband."[20] Zheng's analysis, however, supports the opposite conclusion: that the Internet is a subtle and effective tool through

[19] *Ibid.,* p. 165

[20] Nicholas Kristof, "Death by a Thousand Blogs," *The New York Times,* May 24, 2005, accessed August 13, 2010 at: https://www.nytimes.com/2005/05/24/opinion/24kristoff.html

which the CCP is actually prolonging its rule, bolstering its domestic power and legitimacy, while enacting no meaningful political or legal reforms.

Public policy discourse and deliberation are not exclusive features of democracies at any rate. Political scientists have identified varying amounts of public discourse and deliberation in a range of authoritarian states. In 2008 Baogang He and Mark Warren coined the term "authoritarian deliberation" to explain how China's authoritarian regime utilizes "deliberative venues" to bolster regime legitimacy. "By implication," they write, "deliberation must be sufficiently robust—particularly in lending legitimacy to elite decisions—to serve an authority-maintaining function." While it's possible that the deliberation now taking place within Chinese authoritarianism might bring about eventual democratization, He and Warren believe this is only one of two possibilities. The other is that the deliberative practices embraced by the state could stabilize and prolong the CCP's authoritarian rule.[21]

Min Jiang applies the concept of "authoritarian deliberation" specifically to Chinese cyberspace, identifying four main deliberative spaces: 1) "central propaganda spaces," websites and forums constructed and operated directly by the government; 2) "government-regulated commercial spaces," websites and other digital platforms that are owned and operated by private companies but subject to government regulation, including elaborate requirements for content censorship and user surveillance; 3) "emergent civic spaces," websites run by non-governmental organizations and non-commercial individuals, which are censored less systematically than commercial spaces but nonetheless subject to registration requirements as well as intimidation, shut-down, or

[21] Baogang He and Mark E. Warren, "Authoritarian Deliberation: The Deliberative Turn in Chinese Political Development," paper presented at the American Political Science Association Annual Meeting, Boston, August 28-31, 2008

arrest when authors go too far or administrators fail to control community conversations; and 4) "international deliberative spaces," websites and services hosted outside of Chinese government jurisdiction – some of which are blocked and require circumvention tools to access – where content and conversations not permitted on domestic websites can be found, and where more internationally-minded Chinese Internet users seek to conduct conversations with a broader global public.[22]

Note that the "Great Firewall of China" – the Internet filtration system that blocks websites from view on domestic Internet connections – is deployed by the government to control only the fourth category of deliberative space, located outside of China. The state uses much more direct and proactive means to control the first three deliberative spaces, all of which operate within Chinese government jurisdiction. For websites run by companies, individuals, or organizations located inside China, the government has direct jurisdiction. Undesirable or "sensitive" content is either deleted from the Internet altogether, or blocked from being published in the first place. Jiang points out that the first two categories – central government propaganda spaces and government-controlled commercial spaces – have the greatest impact on Chinese public opinion. She writes: "Those spaces heavily influenced by state and commercial interests are also the very spaces where private lives and the larger political world are bridged and where public opinion is formed."[23]

Speaking at the Sixth Annual Chinese Internet Research Conference at Hong Kong University in 2008, scholar Li Yonggang – whose own Nanjing-based website devoted to independent scholarship was shut down by authorities after 13 months of

[22] Jiang, M. (2010). Authoritarian deliberation on Chinese Internet. *Electronic Journal of Communication*, *20, No.1 and No.2*.
[23] *Ibid,* p. 28

operation – agreed with Tsui that the "Great Firewall" is a misleading frame through which to understand Chinese Internet censorship. A better metaphor, he suggested, is a hydro-electric water management system. Managers have both routine and crisis-management goals: managing daily flows and distribution on the one hand, and managing droughts and floods on the other. It is a huge complex system with many moving parts, requiring management flexibility – it is impossible for the central government to have total control over water levels or quantity. The system's managers learn and innovate as they go along.[24]

Networked Authoritarianism in Action

Indeed, recent Chinese government statements show that like water, the Internet is simultaneously vital and dangerous. The Chinese government made clear in its June 2010 Internet White Paper – the first such Internet policy paper ever issued by the Chinese government – that the rapid, nationwide expansion of Internet and mobile penetration is a strategic priority. The Internet is seen as indispensible for education, poverty alleviation, and the more efficient conveyance of government information and services to the public. The development of a vibrant indigenous Internet and telecommunications sector is also now considered to be critical for China's long-term global economic competitiveness. [25]

---

[24] "Session 10: All-star roundtable: Chinese Journalism in the Internet Age," Chinese Internet Research Conference blog, June 14, 2008, accessed August 16, 2010 at: http://jmsc.hku.hk/blogs/circ/2008/06/14/session-10-all-star-roundtable-chinese-journalism-in-the-internet-age/ ; Rebecca MacKinnon, "Chinese Internet Research Conference: Getting Beyond Iron Curtain 2.0," *RConversation*, June 18, 2008, accessed August 16, 2010 at: http://rconversation.blogs.com/rconversation/2008/06/chinese-inter-1.html

[25] Information Office of the State Council of the People's Republic of China, *The Internet in China,* June 8, 2010, accessed September 13, 2010 at: http://china.org.cn/government/whitepaper/node_7093508.htm

Globally, the Internet is rapidly evolving away from personal computers and onto mobile devices, appliances, and vehicles, with the most rapid rate of growth in Internet and mobile use taking place in Africa and the Middle East. The Chinese government's strategy is for Chinese companies to be leaders in mobile Internet innovation, particularly in the developing world. Last year, Premier Wen Jiabao spoke on multiple occasions about the importance of "the Internet of things," encouraging breakthroughs by Chinese companies in what the Chinese government has designated as a "strategic industry."[26] At the same time, Chinese companies are fully expected to support and reinforce domestic political stability, and to ensure that Internet and communications technologies (ICT's) will not be used in a manner that threatens Communist Party rule.[27]

While the government has direct control over websites run by state-operated media as well as national and provincial-level websites operated by all publicly-facing parts of the Chinese government, by far the largest portion of the Chinese Internet is run by the private sector ("government-regulated commercial spaces" according to Min Jiang's taxonomy of Chinese deliberative digital spaces). Chinese networked authoritarianism cannot work without the active cooperation of private companies – regardless of where their investment comes from or where they are headquartered. Every year a group of Chinese Internet executives are chosen to receive the government's

[26] Richard McManus, "Chinese Premier Talks Up Internet of Things," *ReadWriteWeb,* January 19, 2010, accessed September 13, 2010 at: http://www.readwriteweb.com/archives/chinese_premier_internet_of_things.php

[27] David Talbot, "China: Our Internet is Free Enough," *Technology Review,* June 16, 2010, accessed September 13, 2010 at: http://www.technologyreview.com/web/25592/page1/

"China Internet Self-Discipline Award" for fostering "harmonious and healthy Internet development."[28]

In Anglo-European legal parlance, the legal mechanism used to implement such a "self-discipline" system is "intermediary liability." It is the legal mechanism through which Google's Chinese search engine, Google.cn, was required to censor itself until Google re-directed its simplified Chinese search engine offshore to Hong Kong.[29] All Internet companies operating within Chinese jurisdiction – domestic or foreign – are held liable for everything appearing on their search engines, blogging platforms, and social networking services. They are also legally responsible for everything their users discuss or organize through chat clients and messaging services. In this way, much of the censorship and surveillance work is delegated and outsourced by the government to the private sector – who, if they fail to censor and monitor their users to the government's satisfaction, will lose their business license and be forced to shut down. All of China's large Internet companies have entire departments of employees whose sole job is to police users and censor content around the clock. [30]

In 2008 I conducted a comparative study examining how fifteen different Chinese blog-hosting services censored user-created content. My tests revealed that each company used slightly different methods and approaches in their censorship, and the specific content censored also varied from service to service. In a number of tests, when I tried to post politically sensitive material such as an article about the parents of students killed in

---

[28] Rebecca MacKinnon, "Are China's demands for Internet 'self discipline' spreading to the West?" McClatchy Newspapers syndicated service, January 18, 2010, accessed September 13, 2010 at: http://www.mcclatchydc.com/2010/01/18/82469/commentary-are-chinas-demands.html

[29] Miguel Helft and David Barboza, "Google Shuts China Site in Dispute Over Censorship," *The New York Times*, March 22, 2010, accessed September 13, 2010 at: http://www.nytimes.com/2010/03/23/technology/23google.html?_r=1

[30] Wen Yunchao, "The Art of Censorship," *Index on Censorship* Vol.35, No.1, pp.53-57

Tiananmen square, or a recent clash in a remote town in Western China, internal software systems would block publication of the post entirely. Other posts could be saved as drafts, but "held for moderation" until a company staffer could make a decision about whether they should be allowed. Other postings simply disappeared within hours after publication.[31]

In June 2010, a report giving Internet users a peek behind the veil of secrecy surrounding corporate complicity in Chinese Internet censorship appeared on the popular Chinese website Sina.com for a few hours before – ironically – being censored. It quoted the editor of Sina's Twitter-like microblogging service, Chen Tong, who complained at an industry forum that the government-imposed censorship system is a "real headache" for his staff. Chen went on to describe his company's censorship system in some detail: 24-7 policing; constant coordination between the editorial department and the "monitoring department;" daily meetings to discuss the latest government orders listing new topics and sensitive keywords that must either be monitored or deleted depending on the level of sensitivity; and finally, systems through which both editors and users are constantly reporting problematic content and bringing it to the attention of company censors.[32] In April 2009, an employee of Baidu, China's leading search engine which also runs user-generated content services, leaked a set of detailed documents from Baidu's internal monitoring and censorship department (such a department exists in all Chinese Internet companies of any size), confirming the company's long-standing

[31] Rebecca MacKinnon, "China's Censorship 2.0: How companies censor bloggers," *First Monday* (February 2006), accessed September 13, 2010 at: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2378/2089;

[32] Elaine Chow, "Quote of the Day: Chen Tong, Head Editor of Sina, on the annoyance of censoring tweets," *Shanghaiist*, June 14, 2010 at: http://shanghaiist.com/2010/06/14/quote_of_the_day_chen_tong_head_edi.php; text of the original Chinese-language report at: http://www.chinagfw.org/2010/06/blog-post_1263.html

reputation as industry leader not only as a search engine and online services company, but also in censoring both search engine results and user-generated content. The documents included censorship guidelines, specific lists of topics and words to be censored, guidelines on how to search for information that needs to be deleted, blocked, or banned, and other internal information from November 2008 through March 2009.[33]

In its efforts to manage what Chinese people can learn, discuss, and organize online, the government deploys a range of other tactics. They include:

✔**Cyber-attacks:** The sophisticated, military-grade cyber-attacks launched against Google were targeted specifically at GMail accounts of human rights activists who are either from China or work on China-related issues.[34] This serves as an important reminder that governments and corporations are not the only victims of cyber-warfare and cyber-espionage. Human rights activists, whistleblowers and dissidents around the world, most of whom lack training or resources to protect themselves, have over the past few years been victim of increasingly aggressive cyber attacks.[35] It also reflects a recognition that the "Great Firewall" filtration system in and of itself is too easily circumventable, and insufficient to prevent Chinese citizens from discovering or publishing politically sensitive content on websites hosted overseas, or from forging alliances with people outside of China. Websites run by Chinese exiles, dissidents, and

---

[33] Xiao Qiang, "Baidu's Internal Monitoring and Censorship Document Leaked," *China Digital Times,* April 30, 2009, Part 1 at: http://chinadigitaltimes.net/2009/04/baidus-internal-monitoring-and-censorship-document-leaked/ ; Part 2 at: http://chinadigitaltimes.net/2009/04/baidus-internal-monitoring-and-censorship-document-leaked-2/ ; Part 3 at: http://chinadigitaltimes.net/2009/04/baidus-internal-monitoring-and-censorship-document-leaked-3/

[34] David Drummond, "A new approach to China," *The Official Google Blog,* January 12, 2010, accessed September 13, 2010 at: http://googleblog.blogspot.com/2010/01/new-approach-to-china.html

[35] See *Tracking Ghostnet: Investigating a Cyber Espionage Network*, by Information War Monitor (March 2009), accessed September 13, 2010 at http://www.nartv.org/mirror/ghostnet.pdf

human rights defenders (a part of Min Jiang's fourth category of spaces for digital discourse, "international deliberative spaces") have thus seen increasingly aggressive attacks over the past few years.[36] In other cases the effect is to compromise activists' computer networks and e-mail accounts. Domestic and foreign journalists who report on politically sensitive issues and academics whose research includes human rights problems have also found themselves under aggressive attack in China, exposing their sources and making it much more risky to work on politically sensitive topics.[37]

✔**Device and network controls:** In late spring of 2009 the Ministry of Industry and Information Technology (MIIT) mandated that by July 1st of that year all computers sold in China must be pre-installed with a specific software product called "Green Dam – Youth Escort."[38] While the purpose of "Green Dam" was ostensibly for child protection, researchers inside and outside of China quickly uncovered the fact that it not only censored additional political and religious content, it also logged user activity and sent this information back to a central computer server belonging to the software developer's company.[39] The software had other problems that made it easy for U.S. industry to oppose: It contained serious programming flaws which increased the user's vulnerability

---

[36] "Chinese human rights sites hit by DDoS attack," by Owen Fletcher, *ComputerWorld*, January 26, 2010, accessed September 13, 2010 at: http://www.computerworld.in/articles/chinese-human-rights-sites-hit-ddos-attack

[37] "National Day triggers censorship, cyber attacks in China," Committee to Protect Journalists, September 22, 2009, accessed September 13, 2010 at: http://cpj.org/2009/09/national-day-triggers-censorship-cyber-attacks-in.php

[38] "China Squeezes PC Makers," by Loretta Chao, *The Wall Street Journal*, June 8, 2009, accessed September 13, 2010 at: http://online.wsj.com/article/SB124440211524192081.html

[39] *China's Green Dam: The Implications of Government Control Encroaching on the Home PC*, Open Net Initiative bulletin (June, 2009) accessed September 13, 2010 at: http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc; *Analysis of the Green Dam Censorware System*, by Scott Wolchok, Randy Yao, and J. Alex Halderman, Computer Science and Engineering Division, The University of Michigan, June 11, 2009, accessed September 13, 2010 at: http://www.cse.umich.edu/%7Ejhalderm/pub/gd/.

to cyber-attack. It also violated the intellectual property rights of a U.S. company's filtering product. Faced with uniform opposition from the U.S. computer industry and strong protests from the U.S. government, the MIIT backed down on the eve of its deadline, making the installation of Green Dam voluntary instead of mandatory. [40] The defeat of Green Dam, however, did not diminish other efforts to control and track Internet user behavior at more localized levels within the national "Great Firewall" system – for instance at the level of a school, university, or apartment block as well as at the level of a city-wide Internet Service Provider (ISP). It was reported in September 2009 that local governments were mandating the use of censoring and surveillance products with names like "Blue Shield" and "Huadun." The function and purpose of these products appeared similar to Green Dam, though they had the benefit of involving neither the end user nor foreign companies. [41] Unlike Green Dam, the implementation of these systems has received little attention from foreign media, governments or human rights groups.

✔**Domain name controls:** In December, the government-affiliated China Internet Network Information Center (CNNIC) announced that it would no longer allow individuals to register Internet domain names ending in .cn. [42] Only companies or organizations would be able to use the .cn domain. While authorities explained that this measure was aimed at cleaning up pornography, fraud, and spam, a group of Chinese

[40] "After the Green Dam Victory," by Rebecca MacKinnon, *CSIS Freeman Report*, June/July 2009, accessed September 13, 2010 at: http://csis.org/files/publication/fr09n0607.pdf
[41] "China Clamps Down on Internet Ahead of 60th Anniversary," by Owen Fletcher, IDG News Service, September 25, 2009, accessed September 13, 2010 at: http://www.pcworld.com/article/172627/china_clamps_down_on_internet_ahead_of_60th_anniversary.html ; and "China: Blue Dam activated," by Oiwan Lam, *Global Voices Advocacy*, September 13, 2009, accessed September 13, 2010 at: http://advocacy.globalvoicesonline.org/2009/09/13/china-blue-dam-activated/
[42] "China tightens control on domain name registration," by Zhao Chunzhe, China Daily, December 14, 2009, accessed September 13, 2010 at: http://www.chinadaily.com.cn/china/2009-12/14/content_9174767.htm

webmasters protested that it also violated individual rights.[43] Authorities announced that more than 130,000 websites had shut down in the cleanup. In January a Chinese newspaper reported that self-employed individuals and freelancers conducting online business had been badly hurt by the measure.[44] Later in February, CNNIC backtracked somewhat, announcing that individuals will once again be allowed to register .cn domains, but all applicants must appear in person to confirm their registration, show a government ID, and submit a photo of themselves with their application.[45] This eliminates the possibility of anonymous domain name registration under .cn and makes it easier for authorities to warn or intimidate website operators when "objectionable" content appears. The new Chinese-language top-level domain, ".中国" approved in mid-2010 by the International Corporation for Assigned Names and Numbers (ICANN), the international body that governs the global domain name system, is administered and controlled by CNNIC, the same organization that controls .cn.[46] CNNIC also intends to apply for global rights to the Chinese-language equivalents of ".com" and ".net" (.公司

[43] "China: Online protest against CNNIC," by Oiwan Lam, *Global Voices Advocacy*, December 22, 2009, accessed September 13, 2010 at: http://advocacy.globalvoicesonline.org/2009/12/22/china-online-protest-against-cnnic/

[44] "China: More than 100 thousand websites shut down," by Oiwan Lam, *Global Voices Advocacy*, February 3, 2010, accessed September 13, 2010 at: http://advocacy.globalvoicesonline.org/2010/02/03/china-more-than-100-thousand-websites-shut-down/

[45] "China Further Tightens Rules for Domain Name Owners," by Owen Fletcher, PCWorld, February 23, 2010, accessed September 13, 2010 at: http://www.pcworld.com/article/190013/china_further_tightens_rules_for_domain_name_owners.html

[46] "ICANN Approves Chinese Internationalized Domain Names," ICANN press release, June 25, 2010, accessed August 17, 2010 at: http://www.icann.org/en/news/releases/release-25jun10-en.pdf

and . 网络). [47] Control over popular Chinese-character domain names could thus potentially constitute yet another layer of control over Chinese-language online speech.

✔**Localized disconnection and restriction:** In times of crisis when the government wants to ensure that people cannot use the Internet or mobile phones to organize protests, connections are shut down entirely or heavily restricted in specific locations. The most extreme case is Xinjiang province, a traditionally Muslim region bordering Pakistan, Kazakhstan, and Afghanistan in China's far Northwest. After ethnic riots took place in July of last year, the Internet was cut off in the entire province for six months, along with most mobile text messaging and international phone service. Nobody in Xinjiang could send e-mail or access any website – domestic or foreign. Businesspeople had to travel to the bordering province of Gansu just to communicate with customers. [48] Internet access and phone service have since been restored, but with severe limitations on the number of text messages people can send on their mobile phones per day, no access to overseas websites, and even very limited access to domestic Chinese websites. Xinjiang-based Internet users can only access specially watered-down

[47] CNNIC already operates .公司 and . 网络 within China, but those top-level domains do not yet work outside of China. See: "FAQ for Chinese Domain Name," China Internet Network Information Center website, accessed August 17, 2010 at: http://www.cnnic.net.cn/html/Dir/2005/10/11/3218.htm ; and Rebecca MacKinnon, "China tightens Internet controls in the name of fighting porn, piracy, and cybercrime," *RConversation*, December 13, 2009, accessed August 17, 2010 at: http://rconversation.blogs.com/rconversation/2009/12/china-tightens-internet-controls-all-in-the-name-of-fighting-porn-piracy-and-cybercrime.html

[48] "What Internet? China region cut off 6 months now," by Cara Anna, Associated Press via Yahoo! News, January 19, 2010, accessed September 13, 2010 at: http://news.yahoo.com/s/ap/20100119/ap_on_bi_ge/as_china_internet_blackout

versions of official Chinese news and information sites, with many of the functions such as blogging or comments disabled.[49]

✔**Self-censorship due to surveillance:** Surveillance of Internet and mobile users is conducted in a variety of ways, contributing to an atmosphere of self-censorship. Surveillance enables authorities to warn and harass Internet users either via electronic communications or in person when individuals are deemed to be taking their online activities too far. Detention, arrest, or imprisonment of select individuals serves as an effective warning to others that they are being watched. Surveillance techniques include:

☑ *"Classic" monitoring:* While Chinese surveillance measures are justified to the public as anti-terrorism measures, they are also broadly used to identify, then harass or imprison peaceful critics of the regime. Cybercafes – the cheaper and more popular option for students and less affluent people – are required to monitor users in multiple ways including ID registration upon entry to the café or upon login, surveillance cameras, and monitoring software installed on computers.

☑ *"Law enforcement compliance:"* In a country like China where "crime" is defined broadly to include political dissent, companies with in-country operations and user data stored locally can easily find themselves complicit in the surveillance and jailing of political dissidents. The most notorious example of law enforcement compliance gone badly wrong was when Yahoo's local Beijing staff gave Chinese police account information of journalist Shi Tao, activist Wang

[49] "Blogger describes Xinjiang as an 'internet prison'," Josh Karamay, BBC News, February 3, 2010, accessed September 13, 2010 at: http://news.bbc.co.uk/2/hi/asia-pacific/8492224.stm

Xiaoning, and at least two others engaged in political dissent. [50] There are other examples of how law enforcement compliance by foreign companies has compromised activists. In 2006, Skype partnered with a Chinese company to provide a localized version of its service, then found itself being used by Chinese authorities to track and log politically sensitive chat sessions by users inside China. This happened because Skype delegated law enforcement compliance to its local partner without sufficient attention to how the compliance was being carried out. [51]

✔**Pro-active measures: "astro-turfing" and public outreach:** The government increasingly combines censorship and surveillance measures with pro-active efforts to steer online conversations in the direction it prefers. In 2008 the Hong Kong-based researcher David Bandurski determined that at least 280,000 people had been hired at various levels of government to work as "online commentators." Known derisively in the Chinese blogosphere as the "fifty cent party," these people are paid to write postings that show their employers in a favorable light in online chat rooms, social networking services, blogs, and comments sections of news websites. [52] Many more people do similar work as volunteers – recruited from among the ranks of retired officials as well as college students in the Communist Youth League who aspire to become Party members. This

[50] For detailed analysis of the Yahoo! China case see "Shi Tao, Yahoo!, and the lessons for corporate social responsibility," working paper presented at presented December 2007 at the International Conference on Information Technology and Social Responsibility, Chinese University, Hong Kong, accessed September 13, 2010 at: http://rconversation.blogs.com/YahooShiTaoLessons.pdf

[51] *Breaching Trust*, by Nart Villeneuve, Information Warfare Monitor and ONI Asia Joint Report (October 2008), accessed September 13, 2010 at: http://www.nartv.org/mirror/breachingtrust.pdf

[52] "China's Guerilla War for the Web," by David Bandurski, *Far Eastern Economic Review*, July 2008, accessed September 13, 2010 at: http://www.feer.com/essays/2008/august/chinas-guerrilla-war-for-the-web

approach is similar to a tactic known as "astro-turfing" in American parlance, now commonly used by commercial advertising firms, public relations companies, and election campaigns around the world.[53] In many provinces it is now also standard practice for government officials – particularly at the city and county level – to co-opt and influence independent online writers by throwing special conferences for local bloggers, inviting them to special press events or news conferences about, for example, issues of local concern. [54]

The central government has also adopted a strategy of using official interactive portals and blogs which are cited as evidence both at home and abroad that China is liberalizing.[55] In September 2010, the Chinese Communist Party launched an online bulletin board called "Direct to Zhongnanhai," through which the public is invited to send messages to China's top leaders.[56] Since 2008 President Hu Jintao and Prime Minister Wen Jiabao have held annual "web chats" with China's "netizens."[57] An official "E-Parliament" website, in which citizens are invited to post policy suggestions to the

---

[53] "Astroturfing describes the posting of supposedly independent messages on Internet boards by interested companies and individuals In American politics, the term is used to describe formal public relations projects which deliberately give the impression that they are spontaneous and populist reactions. The term comes from AstroTurf -- the fake grass used in many indoor American football stadiums. The contrast between truly spontaneous or "grassroots" efforts and an orchestrated public relations campaign, is much like the distinction between real grass and AstroTurf." From http://www.answers.com/topic/astroturfing, accessed September 13, 2010

[54] "How China polices the internet," by Kathrin Hille, *Financial Times*, July 17, 2009, accessed September 13, 2010 at: http://www.ft.com/cms/s/2/e716cfc6-71a1-11de-a821-00144feabdc0.html

[55] "Political Advisor Proposes Gov't Blog to Promote E-democracy," Xinhua News Agency, March 14, 2007, accessed September 13, 2010 at: http://www.china.org.cn/english/2007lh/202901.htm

[56] Katryn Hille, "Beijing tries e-mail route to citizens," *Financial Times,* September 13, 2010, accessed September 13, 2010 at: http://www.ft.com/cms/s/0/841b6bd6-bf46-11df-a789-00144feab49a.html

[57] "Hu Jintao talks to netizens via People's Daily Online" *People's Daily Online*, June 20, 2008, accessed September 13, 2010 at: http://english.people.com.cn/90001/90776/90785/6433952.html; and "Premier Wen talks online with public," *China Daily*, February 28, 2009, accessed September 13, 2010 at: http://www.chinadaily.com.cn/china/2009-02/28/content_7522765.htm

National People's Congress was launched in 2009.[58] In an editorial published in German newspapers, the Chinese Ambassador to Germany recently wrote: "opinions have always remained particularly active on the Internet, some of which hold a critical attitude toward the government. The Chinese government has long paid high attention to various kinds of criticisms and proposals, especially those over the Internet."[59] The official government Whitepaper lists a variety of ways in which the Chinese government solicits public feedback through the Internet. It states: "According to a sample survey, over 60 percent of netizens have a positive opinion of the fact that the government gives wide scope to the Internet's role in supervision, and consider it a manifestation of China's socialist democracy and progress."[60]

All of these things are taking place in the context of the Chinese government's broader policies on information and news control. In December 2009 the Committee to Protect Journalists listed China as the world's top jailer of journalists.[61] In recent Congressional testimony, Joshua Rosenzweig of the Dui Hua Foundation, a human rights advocacy organization, presented an array of statistics to support a grim conclusion: "Over the past 2½ years in particular, roughly since the beginning of 2008, there has been a palpable sense that earlier progress towards rule of law in China has stalled, or even suffered a reversal, and there is mounting evidence that a crackdown is underway, one

---

[58] Mo Huaying and Wu Liming, "World perceives new pulses of China's development through NPC sessions," Xinhua, March 12, 2010, accessed September 13, 2010 at: http://news.xinhuanet.com/english2010/indepth/2010-03/12/c_13208553.htm

[59] Wu Hongbo, "View China Objectively," *China Daily*, July 6, 2010, accessed September 13, 2010 at: http://www.china.org.cn/opinion/2010-07/06/content_20430456_2.htm

[60] "III. Guaranteeting Citizens' Freedom of Speech on the Internet," *The Internet in China,* Information Office of the State Council of the People's Republic of China, June 8, 2010, accessed September 13, 2010 at: http://www.china.org.cn/government/whitepaper/2010-06/08/content_20207994.htm

[61] "2009 Prison Census," Committee to Protect Journalists, (as of December 1, 2009), accessed September 13, 2010 at: http://cpj.org/imprisoned/2009.php

particularly targeting members of ethnic minorities, government critics, and rights defenders."[62]

Thus, online public discourse is indeed expanding – with government encouragement. The government is creating and promoting the impression both at home and abroad that China is moving in the direction of greater democracy. At the same time, the Chinese people's ability to engage in serious political dissent or to organize political movements that might effectively challenge the Chinese Communist Party's legitimacy has actually diminished, and the consequences for attempting such activities are more dire than they were ten years ago.

Networked authoritarianism beyond China

In their most recent book surveying Internet censorship and control around the world, Ron Diebert and Rafal Rohozinski warn of a global trend: "the center of gravity of practices aimed at managing cyberspace has shifted subtly from policies and practices aimed at denying access to content to methods that seek to normalize control and the exercise of power in cyberspace through a variety of means."[63] This paper has described a range of ways in which China is clearly near the forefront of this trend. Diebert and Rohozinski divide the techniques used by governments for Internet censorship and control into three "generations:" The first generation of techniques focuses on "Chinese style" Internet filtering and Internet café surveillance. Second generation techniques

---

[62] Joshua Rosenzweig, "Political Prisoners in China: Trends and Implications for U.S. Policy," Testimony to the Congressional-Executive Committee on China, August 3, 2010, accessed September 13, 2010 at: http://www.cecc.gov/pages/hearings/2010/20100803/statement5.php

[63] Ronald Deibert and Rafal Rohozinski, "Beyond Denial: Introducing Next-Generation Information Access Controls," in Diebert, Palfey, Rohozinski, and Zittrain, eds., *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace,* (MIT Press, 2010), p.6

include the construction of a legal environment legitimizing information control, informal requests made by authorities to companies for removal of information, technical shutdowns of websites and computer network attacks. Third generation techniques include warrantless surveillance, the creation of "national cyberzones," state-sponsored information campaigns, and direct physical action to silence individuals or groups.[64]

While Diebert and Rohozinski characterize Chinese cyber-controls as being largely "first generation," this paper has shown how the Chinese government aggressively utilizes all of the "second" and "third" generation techniques, and has been doing so for quite some time. Indeed, the second and third generation techniques are essential because the "great firewall" alone is ineffective and permeable.

Importantly, however, Diebert and Rohozinski point out that a number of governments, particularly those in Russia and a number of former Soviet republics, have bypassed the "first generation" controls almost completely and instead are concentrating their energies on second and third-generation controls, which are more subtle, more difficult to detect, and more compatible with democratic or pseudo-democratic institutions. The Russian-language Internet, known by its denizens as "RUNET," is thus on the cutting edge of techniques aimed to control online speech with little or no direct filtering.[65]

Research in the Middle East and North Africa shows that while Internet filtering is increasingly common and pervasive throughout the region, governments are stepping

[64] *Ibid.,* p. 23
[65] Diebert and Rohozinski, "Control and Subversion in Russian Cyberspace," *op. cit.*, pp. 15-34

up the use of second and third generation techniques.[66] Tunisia has proven to be particularly sophisticated in that regard, deploying deep packet inspection (technology that enables the identification, analysis, and potentially blockage or alteration of specific content passing through a network), cyber-attacks, and increasingly sophisticated approaches toward surveillance and targeted intimidation.[67] Many governments in the region have beefed up their crackdowns against online dissent through the skillful use of family safety measures and anti-terrorism laws, while at the same time making substantial investments in Internet and telecommunications infrastructure, recognizing that connectivity is essential for economic success.[68]

Some second and third generation controls are also used by democratically elected governments, including South Korea and India.[69] Intermediary liability, the legal mechanism whereby Internet service providers and online service providers are held legally responsible for content posted and transmitted by users, is deployed in a range of political systems to silence anti-regime speech in addition to other objectives such as fighting crime or protecting children.[70] The concept of holding service providers liable

---

[66] "MENA Overview" *op.cit.,* pp. 523-535.;

[67] Sami Ben Gharbia, "Silencing online speech in Tunisia," *Global Voices Advocacy,* August 20, 2008, accessed September 17, 2010 at: http://advocacy.globalvoicesonline.org/2008/08/20/silencing-online-speech-in-tunisia/

[68] *False Freedom: Online Censorship in the Middle East and North Africa*, Human Rights Watch, November 14, 2005, accessed September 13, 2010 at: http://www.hrw.org/en/reports/2005/11/14/false-freedom

[69] Michael Fitzpatrick, "South Korea wants to gag the noisy internet rabble," *Guardian.co.uk* , October 8, 2008, accessed September 13, 2010 at: http://www.guardian.co.uk/technology/2008/oct/09/news.internet and John Ribeiro, "India's new IT law increases surveillance powers," IDG News Service, October 27, 2009 accessed September 13, 2010 at: http://www.networkworld.com/news/2009/102709-indias-new-it-law-increases.html

[70] "Intermediary Liability: Protecting Internet Platforms for Expression and Innovation," Center for Democracy and Technology policy paper, April 27, 2010, accessed September 13, 2010 at: http://www.cdt.org/paper/intermediary-liability-protecting-internet-platforms-expression-and-innovation

has become increasingly popular among lawmakers around the world, including Western Europe – where the objective is primarily to combat intellectual property theft and protect children.[71] Drafts of the Anti-Counterfeiting Treaty Agreement, currently being negotiated by the United States, the European Union, and eleven other countries, until recently contained provisions that would strengthen intermediary liability for Internet service providers; these provisions were finally removed in the wake of strong civil society protest.[72] As recently demonstrated in Russia, allegations of intellectual property violation can easily be used as an excuse to crack down on human rights activists.[73] In the United States, activists are concerned about the weakening of due process in government access to corporate-owned and operated networks, all in the name of combating cyber-crime and cyber-warfare.[74] Even the Chinese government has adopted a very similar language of cyber-security to justify its internet control structures and procedures.[75] Diebert and Rohozinski are right to warn that "many of the legal mechanisms that

[71] Rebecca MacKinnon, "Will Google Stand Up to France and Italy Too?" *The Guardian*, January 13, 2010, accessed September 13, 2010 at: http://www.guardian.co.uk/commentisfree/libertycentral/2010/jan/13/google-china-western-internet-freedom

[72] Peter Sayer, "Secret Copyright Treaty Draft Leaked After Washington Talks," *PC World,* September 6, 2010, accessed September 13, 2010 at: http://www.pcworld.com/businesscenter/article/204915/secret_copyright_treaty_draft_leaked_after_washington_talks.html

[73] Clifford J. Levy, "Russia Uses Microsoft to Suppress Dissent," *The New York Times*, September 11, 2010, accessed September 13, 2010 at: http://www.nytimes.com/2010/09/12/world/europe/12raids.html

[74] "EFF Obtains Records from Behind-the-Scenes Negotiations on Telecom Immunity," EFF.org, November 12, 2009, accessed September 13, 2010 at: http://www.eff.org/press/archives/2009/11/12

[75] "U.S.-China Internet forum highlights need to step up online security," Xinhua News Agency, December 11, 2009, accessed September 13, 2010 at: http://news.xinhuanet.com/english/2009-12/11/content_12631544.htm

legitimate control over cyberspace, and its militarization, are led by the advanced democratic countries of Europe and North America"[76]

Policy implications

This paper has described how Chinese authoritarianism has adapted to the Internet age, not merely through the deployment of Internet filtering but also through the skilled use of second and third generation controls. Chinese networked authoritarianism serves as a model for other regimes – such as Iran – that seek to maintain power and legitimacy in the Internet age. In Russia and elsewhere, however, we are seeing a further disturbing trend: strong governments in weak or new democracies are using second and third generation Internet controls in ways that contribute to the erosion of democracy and slippage back toward authoritarianism. This situation is enabled by weak rule of law, lack of independent judiciary, weak guarantees for freedom of speech and other human rights protections, heavy or un-transparent regulation of industry – particularly the telecommunications sector – and weak political opposition that is rendered even weaker by clever manipulation of the media, legal system, and commercial regulatory system.

Thus it is clear that simply helping activists circumvent first-generation censorship and training them in the use of new technologies for digital activism, without also addressing the second and third generation controls deployed by their governments, is insufficient, sometimes counterproductive, and potentially dangerous for the individuals involved. Most second and third generation controls are enabled by weak rule of law and lack of accountability and transparency in the regulation of privately owned

[76] Diebert and Rohozinski, *op.cit.,* p.6

and operated Internet platforms and telecommunications networks. Therefore, strong advocacy work at the policy and legislative level aimed at improving rule of law, transparency and accountability – in government as well as the private sector – is more important than ever.

The business and regulatory environment for telecommunications and Internet services must become a new and important focus of human rights activism and policy. Free and democratic political discourse requires Internet and telecommunications regulation and policymaking that is transparent, accountable, and open to reform both through the courts and the political system. Without such baseline conditions, opposition, dissent, and reform movements will face an increasingly uphill battle against increasingly innovative forms of censorship and surveillance, assisted by companies that operate and shape activists' digital environment.

Finally, citizens and policymakers of democratic nations must not forget that global Internet freedom begins at home. One of the most urgent tasks of the world's democracies is to develop best practices for openness, accountability, rule of law, and transparent governance of their own digital networks. That is the best possible long-term weapon against the spread of networked authoritarianism. It is also essential in order to ensure the long-term health of the world's existing democracies.