China's "Networked Authoritarianism"

Rebecca MacKinnon

Journal of Democracy, Volume 22, Number 2, April 2011, pp. 32-46 (Article)

JOURNAL OF DEMOCRACY

Islamists and the "Arab Spring"

Why Greece Failed

The Freedom House Survey for 2012

Lessons from Latin America

Published by The Johns Hopkins University Press
DOI: 10.1353/jod.2011.0033

Liberation Technology

CHINA'S "NETWORKED AUTHORITARIANISM"

Rebecca MacKinnon

Rebecca MacKinnon *is a Bernard L. Schwartz Senior Fellow at the New America Foundation. She is cofounder of Global Voices Online* (www.globalvoicesonline.org)*, a global citizen-media network. This essay draws on testimony that she gave before the U.S. Congressional-Executive Commission on China* (www.cecc.gov) *on 24 March 2010.*

To mark the twentieth anniversary of the fall of the Berlin Wall, a German arts organization launched a website called the "Berlin Twitter Wall." Anyone anywhere on the Internet could use Twitter to post a comment into one of the speech bubbles. Within a few days of its launch, the website was overrun by messages in Chinese. Instead of talking about the end of the Cold War and the fall of communism in Europe, Chinese Twitter users accessed 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." Twitter is blocked in China. Still, a growing community is so determined to gain access to the widely used social-networking service and hold uncensored conversations with people around the world that these Chinese Internet users have acquired the technical skills to circumvent this censorship system—widely known as the "Great Firewall of China," a filtering system that blocks websites on domestic Internet connections.

In late January 2010, U.S. secretary of state Hillary Clinton—who two months earlier had stood at Berlin's Brandenburg Gate with other world leaders to celebrate the twentieth anniversary of the fall of the 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."[1]

Journal of Democracy Volume 22, Number 2 April 2011

But can we assume that Chinese authoritarianism will crumble just as the Iron Curtain crumbled two decades ago? It is unwise to make the assumption that the Internet will lead to rapid democratization in China or in other repressive regimes. There are difficult issues of government policy and corporate responsibility that must be resolved in order to ensure that the Internet and mobile technologies can fulfill their potential to support liberation and empowerment.

When an authoritarian regime embraces and adjusts to the inevitable changes brought by digital communications, the result is what I call "networked authoritarianism." In the networked authoritarian state, the single ruling party remains in control while a wide range of conversations about the country's problems nonetheless occurs on websites and social-networking services. The government follows this online chatter, and sometimes people are 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 feel that he has the ability to speak and be heard—in ways that were not possible under classic authoritarianism. At the same time, in the networked authoritarian state, there is no guarantee of individual rights and freedoms. Those whom the rulers see as threats are jailed; truly competitive, free, and fair elections are not held; and the courts and the legal system are tools of the ruling party.

As residents of a networked authoritarian society, China's more than four-hundred million Internet users are managing to have more fun, feel more free, and be less fearful of their government than was the case even a mere decade ago. At the same time, however, the government has continued to monitor its people and to censor and manipulate online conversations to such a degree that no one has been able to organize a viable opposition movement. According to the Dui Hua Foundation, a human-rights advocacy organization, 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 in 2008 for the second time in three years.[2] Average Chinese citizens, however, rarely hear of such trends—an "information gap" which makes it much less likely that a critical mass of them will see the need for rapid political change. The system does not control all of the people all of the time, but it is effective enough that even most of China's best and brightest are not aware of the extent to which their understanding of their own country—let alone the broader world—is being blinkered and manipulated. All university students in China's capital now have high-speed Internet access. But when a documentary crew from U.S. public television recently went onto Beijing university campuses and showed students the iconic 1989 photograph of a man standing in front of a tank in Tiananmen Square, most did not recognize the picture at all.

The Chinese experience teaches us a globally applicable lesson: Independent activists and prodemocracy movements may have won some early skirmishes against censorship, 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 and pouring unprecedented resources into building their capacity to influence and shape digital communications networks in direct and indirect ways. As Larry Diamond put it: "It is not technology, but people, organizations, and governments that will determine who prevails."[3]

In the public discourse about the Internet and repressive regimes, Western policy makers and activists frequently use Cold War–era metaphors in ways that are similar to Clinton's likening of blogs to Soviet-era *samizdat*. Such metaphors are strongest in the policy discourse about the Great Firewall of China. 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. "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." Tsui argues that this framework for understanding the impact of the Internet on Chinese politics is not consistent with the growing body of empirical research and is therefore likely to result in failed policy and activism strategies.[4]

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. 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."[5] Note that the revolution he describes is being waged mainly by Chinese people posting and accessing information on websites and services operated by Chinese companies—in other words, acting *inside* 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-phone 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 people with tools for mobility, empowerment, and self-betterment. Yet he also describes how "working-class ICTs" provide new levers for government and corporations to organize and control a new class of "programmable labor." While Chinese workers have been able to use Internet and mobile technologies to organize strikes and share information about factory conditions in different parts of the country, Qiu concludes that "working-class ICTs by themselves do not constitute a sufficient condition for cultural and political empowerment."[6]

Can Online Activism Help Authoritarians?

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 that which is at the local level or targets specific policy issues over which there are divisions or turf wars between different parts of the government—can actually serve to bolster regime legitimacy. The least successful online movements tend to be those that advocate various forms of political "exit," including calls for an end to one-party rule by the Chinese Communist Party (CCP) and greater political autonomy or independence for particular ethnic or religious groups. "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." On the other hand, successful online movements in China are usually characterized by what Zheng (following Albert O. Hirschman) calls the "voice" option, or what other 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.[7]

Thus, rising levels of online activism in China cannot automatically be interpreted as a sign of impending democratization. One must examine what kind of online activism is succeeding and what kind 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 conclude that the CCP 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 policy makers, 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."[8] Zheng's analysis, however, supports the opposite conclusion: The Internet may actually prolong the CCP's rule, bolstering its domestic power and legitimacy while the regime enacts no meaningful political or legal reforms.

Public-policy discourse and deliberation are not exclusive features of democracies. 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 uses "deliberative venues" to bolster regime legitimacy. While it is possible that the deliberation now taking place within Chinese authoritarianism might bring about eventual democratization, Baogang He and Warren believe that this is only one of two possibilities. The other is that the deliberative practices embraced by the state could stabilize and extend the CCP's authoritarian rule.[9]

Min Jiang applies the concept of authoritarian deliberation specifically to Chinese cyberspace, identifying four main deliberative spaces: 1) "central propaganda spaces," meaning websites and forums built and operated directly by the government; 2) "government-regulated commercial spaces," meaning 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," meaning websites run by nongovernmental organizations and noncommercial individuals, which are censored less systematically than commercial spaces but are nonetheless subject to registration requirements as well as intimidation, shutdown, or arrest when authors cross the line or administrators fail to control community conversations; and 4) "international deliberative spaces," meaning websites and services that are hosted beyond 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.

It is important to note that the Great Firewall is meant to control only the fourth category of deliberative space, the one that is located outside China. Yet it is the first two categories, as Jiang points out, that have the greatest impact on Chinese public opinion. The state uses much more direct and proactive means to control the first three deliberative spaces, all of which operate within the jurisdiction of the Chinese government. Undesirable or "sensitive" content is either deleted from the Internet altogether or blocked from being published.[10]

The Web as Waterworks

Chinese scholar Li Yonggang has suggested that, instead of using a "firewall" metaphor, it is more helpful to think of Chinese Internet controls—which include not only censorship but surveillance and manipulation of information—as something like a hydroelectric 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, and running it requires flexibility. It is impossible for the central government to have total control over every detail of water level or pressure at any given time. The system's managers learn and innovate as they go along.[11]

Recent Chinese-government statements show that, like water, the Internet is viewed as simultaneously vital and dangerous. According to the 2010 government white paper "The Internet in China," rapid, nationwide expansion of Internet and mobile-device penetration is a strategic priority. The Internet is seen as indispensible for education, poverty alleviation, and the efficient conveyance of government information and services to the public. The development of a vibrant, indigenous Internet and telecommunications sector is also considered critical for China's long-term global economic competitiveness.[12] Globally, the Internet is rapidly evolving away from personal computers and toward mobile devices, appliances, and vehicles, with the most rapid rate of growth in Internet and mobile-phone 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 government has designated as a strategic industry.[13]

Although the government has direct control over websites run by state-operated media as well as its own national- and provincial-level websites, by far the largest portion of the Chinese Internet is run by the private sector (or "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 the origin of their financing or where they are headquartered. Every year a group of Chinese Internet executives is chosen to receive the government's "China Internet Self-Discipline Award" for fostering "harmonious and healthy Internet development."

In Anglo-European legal parlance, the legal mechanism used to implement such a "self-discipline" system is "intermediary liability." It is the mechanism by which Google's Chinese search engine, Google.cn, was required to censor itself until Google redirected its simplified Chinese search engine offshore to Hong Kong. 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, the government hands many censorship and surveillance tasks to private companies that face license revocations and forced shutdowns should they fail to comply. Every one of China's large Internet companies has a special department full of employees whose sole job is to police users and censor content.

In 2008, I conducted a comparative study examining how fifteen different Chinese blog-hosting services censored user-created content. The tests revealed that each company used slightly different methods and approaches in its censorship. 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 Tiananmen Square, or a recent clash in a remote town in Western China, internal site software would block publication of the post entirely. Other posts could be saved as drafts but were "held for moderation" until a company staffer could make a decision about whether they should be allowed. Other postings simply disappeared within hours of publication.

Lifting the Veil

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 Chen Tong, the editor of Sina's Twitter-like microblogging service, who described his company's censorship system in some detail: round-the-clock 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 report problematic content and bring it to the attention of company censors.[14] 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 confirming the company's longstanding reputation as an 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; lists of specific 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.[15]

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

Cyber-attacks: The sophisticated, military-grade cyber-attacks launched against Google in late 2009 were targeted specifically at the Gmail accounts of human-rights activists who are either from China or work on China-related issues. Websites run by Chinese exiles, dissidents, and human-rights defenders (most of whom lack the training or resources to protect themselves) have been the victims of increasingly aggressive cyber-attacks over the past few years—in some cases, compromising 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, with efforts to expose their sources, making it much more risky to work on politically sensitive topics.

Device and network controls: In May 2009, the Ministry of Industry and Information Technology (MIIT) mandated that by July 1 of that year a specific software product called Green Dam Youth Escort was to be preinstalled on all computers sold in China. While Green Dam was ostensibly aimed at protecting children from inappropriate content, researchers outside and within China quickly discovered that it not only censored political and religious content but also logged user activity and sent this information back to a central computer server belonging to the software developer's company. The software had other problems that created opposition to it within U.S. companies. It contained serious programming flaws that increased the user's vulnerability 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.

The defeat of Green Dam, however, did not diminish other efforts to control and track Internet-user behavior at more localized levels—schools, universities, apartment blocks, and citywide Internet Service Providers (ISPs). In September 2009, news reports circulated that local governments were mandating the use of censorship and surveillance products with names such as "Blue Shield" and "Huadun." The purpose of these products appeared similar to Green Dam's, though they involved neither the end user nor foreign companies.[16] 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 2009, 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." 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 webmasters protested that it also violated individual rights. Authorities announced that more than 130,000 websites had been shut down in the cleanup. In January 2010, a Chinese newspaper reported that self-employed individuals and freelancers conducting online business had been badly hurt by the measure.[17] In February, CNNIC backtracked somewhat, announcing that individuals would once again be allowed to register .cn domains, but all applicants would have to appear in person to confirm their registration, show a government ID, and submit a photo of themselves with their application. This eliminated the possibility of anonymous domain-name registration under .cn and has made it easier for authorities to warn or intimidate website operators when "objectionable" content appears.

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 in the far-northwestern province of Xinjiang, a traditionally Muslim region that borders Pakistan, Kazakhstan, and Afghanistan. After ethnic riots took place in July 2009, the Internet was cut off in the entire province for six months, along with most mobile text messaging and international phone service. No one in Xinjiang could send e-mail or access any website—domestic or foreign. Business people had to travel to the bordering province of Gansu to communicate with customers. Internet access and phone service have since been restored, but with severe limitations on the number of text messages that people can send on their mobile phones per day, no access to overseas websites, and very limited access even to domestic Chinese websites. Xinjiang-based Internet users can only access watered-down versions of official Chinese news and information sites, with many of the functions such as blogging or comments disabled.[18]

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 have transgressed certain standards. Detention, arrest, or imprisonment of selected individuals serves as an effective warning to others that they are being watched. Surveillance techniques include:

"Classic" monitoring: While surveillance measures are justified to the public as antiterrorism measures, they are also broadly used to identify and harass or imprison peaceful critics of the regime. Cybercafés—the cheap and popular option for students and the less affluent—are required to monitor users in multiple ways, including identity registration upon entry to the café or upon login, surveillance cameras, and monitoring software installed on computers.

"Law-enforcement compliance" : In 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 wrong was when Yahoo's local Beijing staff gave Chinese police account information of activist Wang Xiaoning in 2002 and journalist Shi Tao in 2004, leading to their imprisonment. In 2006, Skype partnered with a Chinese company to provide a localized version of its Internet-based phone-calling service, then found itself being used by Chinese authorities to track and log politically sensitive chat sessions by users inside China. Skype had delegated law-enforcement compliance to its local partner without sufficient attention to how the compliance was being carried out.[19]

"Astroturfing" and public outreach: The government increasingly combines censorship and surveillance measures with proactive efforts to steer online conversations. 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 posts that show their employers in a favorable light in online chatrooms, social-networking services, blogs, and comments sections of news websites.[20] Many more people do similar work as volunteers—recruited from the ranks of retired officials as well as college students in the Communist Youth League who aspire to become Party members. This approach is similar to a tactic known as "astroturfing" in U.S. parlance, now commonly used by commercial advertising firms, public-relations companies, and election campaigns around the world in order to simulate grassroots enthusiasm for a product or candidate. In many Chinese provinces, it is now also standard practice for government officials—particularly at the city and county level—to coopt and influence independent online writers by inviting them to special conferences and press events.

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. In September 2010, the CCP launched an online bulletin board called "Direct to Zhongnanhai," through which the public was invited to send messages to China's top leaders. Since 2008, President Hu Jintao and Premier Wen Jiabao have held annual "web chats" with China's "netizens." An official "E-Parliament" website, on which citizens are invited to post policy suggestions to the National People's Congress, was launched in 2009. The 2010 official government white paper 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."[21]

All of this is 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 worst jailer of journalists. In recent testimony before the U.S. Congress, Joshua Rosenzweig of the Dui Hua Foundation presented an array of statistics to support a grim conclusion:

> Over the past two-and-a-half 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 particularly targeting members of ethnic minorities, government critics, and rights defenders.[22]

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 CCP'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 Deibert and Rafal Rohozinski warn that "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." This article has described a range of ways in which China is near the forefront of this trend. Deibert 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 include the construction of a legal environment legitimizing information control, authorities' informal requests to companies for removal of information, technical shutdowns of websites, and computer-network attacks. "Third-generation" techniques include warrantless surveillance, the creation of "national cyber-zones," state-sponsored information campaigns, and direct physical action to silence individuals or groups.[23]

While Deibert and Rohozinski characterize Chinese cyber-controls as being largely first generation, the Chinese government aggressively uses all 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.

Deibert and Rohozinski point out that a number of governments, particularly those in Russia and several former Soviet republics, have bypassed the first-generation controls almost completely and instead are concentrating their energies on second- and third-generation controls, most of which (with the jarring exception of "direct physical action to silence individuals or groups") are more subtle, more difficult to detect, and more compatible with democratic or pseudodemocratic 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.[24]

Research in the Middle East and North Africa shows that while Internet filtering is more common and pervasive throughout that region, governments are increasing the use of second- and third-generation techniques. Many governments in the region have cracked down on online dissent through the skillful use of family-safety measures and antiterrorism laws. At the same time, they have made substantial investments in Internet and telecommunications infrastructure, recognizing that connectivity is essential for economic success.[25]

Some second- and third-generation controls are also used by democratically elected governments, including those of South Korea and India.[26] Intermediary censorship is deployed in a range of political systems to silence antiregime speech, fight crime, or protect children. The concept of holding service providers liable has become increasingly popular among lawmakers around the world, including in Western Europe—where the main goals are to combat intellectual-property theft and protect children. In the United States, activists are concerned about the weakening of due process, which has allowed government access to networks owned and run by corporations, all in the name of combating cyber-crime and cyber-warfare. Even the Chinese government has adopted a very similar language of cyber-security to justify its Internet-control structures and procedures. Deibert and Rohozinski are right to warn that "many of the legal mechanisms that legitimate control over cyberspace, and its militarization, are led by the advanced democratic countries of Europe and North America."[27]

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. China's brand of networked authoritarianism serves as a model for other regimes, such as the one in Iran, that seek to maintain power and legitimacy in the Internet Age. In Russia and elsewhere there is 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 a weak rule of law, lack of an independent judiciary, weak guarantees for freedom of speech and other human-rights protections, heavy or untransparent 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.

It is clear that simply helping activists to 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. Weak rule of law and lack of accountability and transparency in the regulation of privately owned and operated Internet platforms and telecommunications networks facilitate the use of second- and third-generation controls, which pose a great threat to activists. 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 policy making that are transparent, accountable, and open to reform both through independent courts and the political system. Without such baseline conditions, opposition, dissent, and reform movements will face an increasingly uphill battle against progressively more innovative forms of censorship and surveillance.

NOTES

1. Hillary Rodham Clinton, "Remarks on Internet Freedom," Washington, D.C., 21 January 2010; available at *www.state.gov/secretary/rm/2010/01/135519.htm.*

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

3. Larry Diamond, "Liberation Technology," *Journal of Democracy* 21 (July 2010): 82.

4. 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 presented at the sixth annual Chinese Internet Research Conference, Hong Kong University, 13–14 June 2008; available at *http://jmsc.hku.hk/blogs/circ/files/2008/06/tsui_lokman.pdf.*

5. Guobin Yang, *The Power of the Internet in China: Citizen Activism Online* (New York: Columbia University Press, 2009), 213.

6. Jack Linchuan Qiu, *Working-Class Network Society: Communication Technology and the Information Have-Less in Urban China* (Cambridge: MIT Press, 2009), 243.

7. Yongnian Zheng, *Technological Empowerment: The Internet, State, and Society in China* (Stanford: Stanford University Press, 2008), 164–65.

8. Nicholas D. Kristof, "Death by a Thousand Blogs," *New York Times,* 24 May 2005; available at *www.nytimes.com/2005/05/24/opinion/24kristoff.html.*

9. Baogang He and Mark Warren, "Authoritarian Deliberation: The Deliberative Turn in Chinese Political Development," paper presented at the Annual Meeting of the American Political Science Association, Boston, 28–31 August 2008; forthcoming, *Perspectives on Politics,* June 2011.

10. Min Jiang, "Authoritarian Deliberation on Chinese Internet," *Electronic Journal of Communication* 20 (2010); available at *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1439354.*

11. Rebecca MacKinnon, "Chinese Internet Research Conference: Getting Beyond 'Iron Curtain 2.0,'" *RConversation*, 18 June 2008; available at *http://rconversation.blogs.com/rconversation/2008/06/chinese-inter-1.html.*

12. "The Internet in China," Information Office of the State Council of the People's Republic of China (SCIO), 8 June 2010; available at *http://china.org.cn/government/whitepaper/node_7093508.htm.*

13. Robert McManus, "Chinese Premier Talks Up Internet of Things," *ReadWriteWeb,* 19 January 2010; available at *www.readwriteweb.com/archives/chinese_premier_internet_of_things.php.*

14. Jonathan Ansfield, "China Tests New Controls on Twitter-Style Services," *New York Times,* 16 July 2010; available at *www.nytimes.com/2010/07/17/world/asia/17beijing.html.* The full Chinese-language text of the report (which was deleted by censors from the original source) was reproduced by Radio France Internationale at *www.chinese.rfi.fr.*

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

[16] Owen Fletcher, “China Clamps Down on Internet Ahead of 60th Anniversary,” IDG News Service, 25 September 2009; available at *www.pcworld.com/article/172627/china_clamps_down_on_internet_ahead_of_60th_anniversary.html*; and Oiwan Lam, “China: Blue Dam Activated,” *Global Voices Advocacy,* 13 September 2009; available at *http://advocacy.globalvoicesonline.org/2009/09/13/china-blue-dam-activated.*

[17] Oiwan Lam, “China: More than 100 Thousand Websites Shut Down,” *Global Voices Advocacy,* 3 February 2010; available at *http://advocacy.globalvoicesonline.org/2010/02/03/china-more-than-100-thousand-websites-shut-down.*

[18] Josh Karamay, “Blogger Describes Xinjiang as an ‘Internet Prison,’” BBC News, 3 February 2010; available at *http://news.bbc.co.uk/2/hi/asia-pacific/8492224.stm.*

[19] Nart Villeneuve, “Breaching Trust: An Analysis of Surveillance and Security Practices on China’s TOM-Skype Platform,” Open Net Initiative and Information Warfare Monitor, October 2008; available at: *www.nartv.org/mirror/breachingtrust.pdf.*

[20] David Bandurski, “China’s Guerilla War for the Web,” *Far Eastern Economic Review*, July 2008.

[21] SCIO, “The Internet in China.”

[22] Joshua Rosenzweig, “Political Prisoners in China: Trends and Implications for U.S. Policy,” Testimony to the Congressional-Executive Committee on China, 3 August 2010; available at *www.cecc.gov/pages/hearings/2010/20100803/statement5.php.*

[23] Ronald Deibert and Rafal Rohozinski, “Control and Subversion in Russian Cyberspace,” in Ronald Deibert et al., eds., *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge: MIT Press, 2010), 23.

[24] Deibert and Rohozinski, “Control and Subversion in Russian Cyberspace,” in *Access Controlled,* 15–34.

[25] “MENA Overview,” *Access Controlled,* 523–35.

[26] Michael Fitzpatrick, “South Korea Wants to Gag the Noisy Internet Rabble,” *Guardian.co.uk,* 9 October 2008; available at *www.guardian.co.uk/technology/2008/oct/09/news.internet*; and John Ribeiro, “India’s New IT Law Increases Surveillance Powers,” IDG News Service, 27 October 2009; available at *www.networkworld.com/news/2009/102709-indias-new-it-law-increases.html.*

[27] Deibert and Rohozinski, “Beyond Denial: Introducing Next-Generation Information Access Controls,” 6.