

Breaching the Great Firewall?

Beijing's Internet Censorship Policies and U.S.-China Relations

James Mulvenon

The growth of the Internet in China has been remarkable by any measure. Conservative estimates place the number of users at more than 100 million, and it is widely expected that in the next couple of years China will surpass even the United States in total numbers of users. Yet the nature and implications of this astonishing growth are a controversial issue in the U.S.-China relationship, with many different sectors and constituencies projecting their own hopes and fears onto the medium.

The authorities in Beijing clearly see the Internet as an engine of economic progress, but fear its subversive power. China's online population has enthusiastically embraced the Web and the blogosphere, but only a brave few dare to reject the built-in incentives for self-deterrence and self-censorship. Some elements in the American political class, allied with human rights and other nongovernmental organizations, see the rise of the Internet in China as one of the best hopes for political reform and even regime change in Beijing, while the business community seeks to depoliticize China's information revolution, fearing the loss of market share or that their firms will be branded as collaborating with the censors.

Although the ultimate impact of the Internet in China remains to be seen, it is already testing Beijing's ability to balance the competing imperatives of modernization and control.¹ From public statements, policies, and actions, it is

¹ The Chinese government is not the only global sovereign confronting this dilemma, since similar arguments could be made about many countries around the world, including erstwhile U.S. allies like Saudi Arabia. In response to this paper, one thoughtful observer pointed out: "All countries have subject areas of content deemed especially sensitive and restricted (sex, violence, guns and weapons, birth control, ethnic references, etc.—not just politics or crime). Countries

clear that the Chinese regime is anxious about the consequences of the country's information technology modernization, in particular the challenge of confronting an increasingly complex global information security environment. On the one hand, the regime believes that information technology is a key engine of economic development and that future economic growth in China will depend in large measure on the extent to which the country is integrated with the global information infrastructure. At the same time, however, China is still an authoritarian state run by a Leninist party, whose continued rule relies on the suppression of anti-regime activities. The installation of an advanced telecommunications infrastructure to facilitate economic reform greatly complicates the state's internal security goals. Faced with these contradictory forces of openness and control, Beijing has sought to strike a balance between the information-related needs of economic modernization and the security requirements of internal stability—actively promoting the growth of the Internet even as it imposes significant restrictions on online content and the political use of information technology.

The Internet in U.S.-China Relations: Why Should We Care?

Before diving into detailed analysis of Chinese Internet censorship practices and their policy implications, it is important to place the issue in a broader strategic context. Indeed, the development of the Internet in China is a reflection of the bilateral relationship in many ways, containing elements of both cooperation and contention:

- n **Communication.** The Internet is first and foremost a platform for communication between residents of the two countries. Optimists hope that this communication will dispel misperceptions and narrow the cultural divide, while pessimists point out that the medium can help create misperceptions as well.
- n **Cooperation.** The Internet's development as a global, transnational infrastructure also offers the possibility of mutually beneficial cooperation between the two countries, driven in large measure by economic imperatives. Cooperation has ranged from the relatively mundane, such as participation in multilateral bodies charged with standards development, to core national interests, such as the tracking of illicit terrorist financing over networks. Yet here again, China's rising clout and assertiveness have injected elements of conflict with the United States and other powers. The most telling examples are China's aggressive use of market access as leverage to support the adoption

share little consensus in applying international principles of human rights (e.g., freedom of expression) to contexts involving the Internet, and strike different balances among the competing values inherent in these principles.”

of home-grown IT standards like the WAPI wireless security standard, as well as the fights in ICANN over control of Chinese-language domain names.²

- n **Commerce.** The Internet is an increasingly important facilitating mechanism for bilateral trade, permitting entrepreneurs to conduct business at the speed of light. But the combination of censorship and technical problems associated with the unprecedented rapid growth of China's networks also creates barriers to the free flow of trade.
- n **Change.** The most controversial aspect of the role of the Internet in U.S.-China relations is its perceived capacity to effect political change in China. The importance of cyberspace as a battlefield in the struggle between the Chinese government and foreign and domestic critics of its censorship policies has been magnified as a result of the exponential growth of Internet access in China since personal accounts were made available in 1995. China's international connectivity and the number of computers with Internet access are also expanding impressively. Along with the rapid diffusion of Internet connectivity in China, many commentators, politicians, and pundits in the United States and elsewhere have speculated about its potential to facilitate political change and undermine the dominance of the Chinese Communist Party (CCP).

Especially in the early years of China's IT revolution, many observers argued that the Internet would dramatically shift power to the Chinese people by allowing them to organize and by channeling uncensored information from outside, especially about democracy and human rights. To be sure, the Internet has degraded the regime's ability to control the flow of information, both within China and across its borders. Yet, the Chinese government has managed to stifle most attempts to use the Internet to promote political change and has proven remarkably nimble in responding to the rapidly changing technological environment.

The regime has imprisoned dozens of Web surfers for "subversive" use of the Internet and erected a technologically complex set of monitoring and control mechanisms, widely referred to as the "Great Firewall," to limit access to information it deems harmful to its interests. Online freedom of speech advocates and exiled Chinese democracy activists have mounted numerous attempts to breach the Great Firewall, achieving limited results. Meanwhile, in response to these challenges, the Chinese government has increased the sophistication of its Internet controls.

These trends strongly suggest that the Internet in China is a platform for *evolutionary*—rather than *revolutionary*—political change in China, with the most important metric being the lack of any organized (much less networked)

² ICANN is the Internet Corporation for Assigned Names and Numbers. Headquartered in Marina Del Rey, California, ICANN is a California non-profit corporation that was created on September 18, 1998 in order to oversee a number of Internet-related tasks, including managing the assignment of domain names and IP addresses. To date, much of its work has concerned the introduction of new generic top-level domains. See <http://en.wikipedia.org/wiki/ICANN>.

opposition to the present regime. Although modernization always creates new social forces that are difficult for atavistic bureaucracies to accommodate, the regime appears to be aggressively using the Internet not only to monitor and disrupt threats to continued CCP rule, but also to implement an effective e-government policy designed to improve its governance through greater public involvement in policymaking.³ Thus, although most media articles on the Chinese Internet focus on either regime censorship or the cultural mores of young bloggers, the Internet has improved both governance and popular participation in governance.

Finally, although the prospects for political change may be developing slower than expected, the Internet is clearly creating revolutionary *social* change in China, as even a casual tour through the vibrant Chinese blogosphere reveals. It is also worth noting that Chinese efforts to censor the Internet are likely agitating future generational elites, who will be drawn from the core of China's young, urban, educated, Internet-savvy citizens.

How Does China's Internet Censorship Regime Work?

The implementation of this strategy includes low-tech and high-tech countermeasures.⁴ The low-tech countermeasures draw upon the state's Leninist roots and tried-and-true organizational methods, while the high-tech countermeasures embrace the new information technologies as an additional tool of state domination. Together, they have proven a potent combination in deterring the majority of anti-regime behavior and neutering most of what remains.

On the low-tech front, the Chinese authorities have issued a series of broad regulations that forbid online activities seen as detrimental to the Communist Party's interests. These bureaucratic regulations, such as the Internet Service Provider laws that make providers responsible for the activities of their subscribers, are among the most effective lines of defense in China's Internet security strategy, shaping the market environment and the incentives of key participants in ways conducive to the state's interest. In other words, the government has "outsourced" Internet policing, forcing ISPs to deploy their own (often overly conservative) censors (known colloquially as *damama* or "big mammas") to protect the companies from government reprisal.⁵ To complement

³ For a recent example, see "Officials Enter China's Blogosphere," *Reuters*, November 27, 2006.

⁴ For example, Internet "censorship" needs to be disaggregated into different layers. One reviewer of the paper offered four dimensions: (1) censorship/restrictions on content; (2) government imposition of self-policing on Internet Service Providers as a condition of getting and retaining a license to serve customers within their jurisdiction; (3) government use of Internet surveillance to monitor political & criminal activities (with or without ISP involvement); and government access to Personally Identifying Information (PII) maintained by the ISPs.

⁵ One reviewer of the paper correctly offered the following important caveats about the role of ISPs in censorship: "All ISPs do have terms of use that place restrictions on customer use and justify denial of service by the companies themselves (child pornography, fraud, IP infringements,

the regulations, the authorities have also elicited further pledges of cooperation from key industry players.

Another important part of the low-tech counterstrategy is making examples of dissidents and other Internet users who violate the regime's rules. So far, at least 35 Chinese Internet users have been arrested for "subversive" use of the Internet. In addition to selectively publicizing some of these arrests, the regime occasionally highlights the monitoring capabilities of its "Internet police" in the official media, though the commercial censors described above often perform the task on their behalf. In some cases, official media reports may deliberately exaggerate authorities' ability to monitor the activities of ordinary Chinese Web surfers to deter Internet users from engaging in "subversive" online activities. The desired result is a climate in which the vast majority of Internet users are either disinterested in or deterred from undertaking any online activities that might risk punishment by running afoul of the censors.

More recently, however, the regime has supplemented its strategy with an array of increasingly sophisticated and effective high-tech countermeasures, apparently reflecting a substantial investment by the Chinese authorities in enhanced blocking, filtering, and monitoring capabilities. The centerpiece of this high-tech component system of high-tech Internet controls, dubbed "the Great Firewall" by the regime's critics.

Although the Great Firewall remains far from impenetrable, technical analysis indicates extensive deployment of sophisticated equipment capable of blocking access to prohibited sites and proxy servers as well as filtering the content of accessed sites and e-mail. In particular, technical analysis reveals the widespread use of transparent proxies to perform inline content filtering, proxy server hunting, and POP3 e-mail filtering, as well as rampant hijacking of domain name service (DNS) queries, including the capturing of requests to foreign servers and spoofing responses.⁶

national security, public order, etc.). However, companies cannot affirmatively monitor all customer behavior and must rely on a complaint process to identify unacceptable behaviors. Criminal authorities seeking customer information often do not do so in writing and seldom provide information about the grounds or purpose for their requests or investigations. (It is typically illegal in all countries to notify customers that they are under criminal investigation.) Therefore, the basis for resisting such requests may be limited to insisting on written process and competent authorities, subject to further challenge in administrative or judicial proceedings that are not always available, fair or transparent."

⁶ Domain Name Servers are computers that work to tell each computer the IP address for any Web site. If someone types in the domain name for a site, such as <http://www.google.com/>, then the network searches for a DNS server that can resolve the URL into a numerical IP address associated with the URL. Once the computer has the IP address, it can route the user's traffic to the Web site, and the connection is made. The Chinese Internet censorship infrastructure interferes with this core network protocol to prevent domestic users from reaching sensitive sites.

What Are Some Examples of Chinese Internet Censorship?

Chinese attempts to censor the Internet as early as the late 1990s are well-documented by both domestic and international observers.

The Blocking of Wikipedia

Chinese authorities first began blocking the Chinese-language version of the online encyclopedia Wikipedia (<http://zh.wikipedia.org>) on June 3, 2004, one day before the politically sensitive anniversary of the Tiananmen Massacre. The site was accessible again a short time later, only to have the Chinese and English versions of the site blocked again in October 2005, without explanation. Wikipedia founder Jimmy Wales refused to remove the objectionable entries from the sites, claiming that censorship was “antithetical to the philosophy of Wikipedia.” After more than a year of inaccessibility, the block on the English version of the site was lifted in October 2006, and Chinese Wikipedia was briefly reopened in mid-November. Activist Andrew Lih speculated that the Chinese authorities ended the ban because the Wikipedia community “has a neutral point of view at its core, with no activist or subversive agenda.” But the access was short-lived, with the ban restored within a week.⁷ As of December 17, both the English and Chinese versions of Wikipedia continued to be blocked to Chinese users.

Introduction of the Censored Google.cn

Google was one of the first Western search engine companies to offer a Chinese-language version of its portal. Since 2001, Western users capable of reading Chinese had the option to use the site (<http://www.google.com/intl/zh-CN/>), and users located in China were automatically directed to it. As Google gained global search dominance and captured 25 percent of the Chinese market, it quickly became the target of attention by the Chinese censors, who were particularly concerned that Chinese users could indirectly access banned overseas content using the search engine’s “cache” feature.

On September 3, 2002, Google was blocked in China,⁸ and Google queries originating within China were redirected via DNS hijacking to a domestic Chinese search engine, Baidu (baidu.com), whose front end looked remarkably similar to the simplified Chinese version of Google.⁹ After the redirection was publicized in the media and Google complained to authorities in Beijing, the redirecting

⁷ “Chinese Censors Block Access to Wikipedia,” *IDG News Service*, June 14, 2004; “Wikipedia Defies China’s Censors,” *The Observer*, September 10, 2006; “Wikipedia Defies China’s Censors,” *The Observer*, September 10, 2006; “China ‘Unblocks’ Wikipedia Site,” *BBC News*, November 16, 2006; Hiawatha Bray, “China Allows Full Access to Wikipedia: Other Websites Still Censoring Content,” *Boston Globe*, November 16, 2006; Clive Thompson, “Google’s China Problem (and China’s Google Problem),” *New York Times Magazine*, April 23, 2006, p.64; “Chinese Web Censors Unblock Wikipedia, Then Block It Again,” *Associated Press*, November 17, 2006.

⁸ Thompson, “Google’s China Problem,” p.64.

⁹ Peter S. Goodman and Mike Musgrove, “China Blocks Web Search Engines: Country Fears Doors to Commerce Also Open Weak Spots,” *Washington Post*, September 12, 2002, p. E01.

stopped, but it appears that the company adopted the strategy “if you can’t beat ‘em, join ‘em.”

In 2004, Google invested a \$5 million stake in Baidu¹⁰ and in January 2006 launched a new Web site (google.cn) that was registered in China,¹¹ though tracerouting of queries revealed that traffic was routed to servers in California. Users immediately noticed significant differences between search results for identical queries, depending on geographic location of the user and language of the query. Users based in the United States who entered “Tiananmen” in English into google.com or the simplified Chinese google.com received the most complete results, starting with the Wikipedia entry on the Tiananmen Massacre. Users based in the United States who entered “Tiananmen” in Chinese into the simplified Chinese google.com receive similar content in the vernacular. Users based in China, however, are automatically redirected to google.cn, where queries on Tiananmen in both English and Chinese produce only tourist information with no political content whatsoever.

Criticism of Google for creating a censored version of its search engine in China was swift and withering. Company executives, along with counterparts from Microsoft, Yahoo!, and Cisco were subpoenaed to appear at a congressional hearing in February 2006, where they were criticized by members for collaborating with the Beijing authorities to silence dissidents.¹² In response, Google decided in March 2006 to store search records from the site outside of China, so the Beijing government could not access the data without Google’s consent.¹³ The data include both the information sought in the search as well as the IP addresses associated with the queries.¹⁴ In addition, Google announced that it would not introduce its popular Gmail or Blogger products in China, fearing that it would have to turn over user data to the government. At the same time, the company’s CEO, Eric Schmidt, told journalists during an April 2006 visit to Beijing that it would be “arrogant” for Google to try and change the country’s Internet censorship regulations.¹⁵

Yahoo! and Collaboration with the Beijing Police

When Yahoo! entered the Chinese market in 2002, it voluntarily signed the government’s “Public Pledge on Self-Discipline for the China Internet Industry,” agreeing to abide by the country’s Internet censorship regulations. Jerry Yang and the Yahoo! leadership were roundly criticized, but they insisted that the decision was consistent with a general principle to obey the domestic laws of any country in which they provided services. It was assumed that this policy would be passive in implementation, denying access to information but not actively cooperating with the government.

¹⁰ Mure Dickie, “Google Takes Stake in Baidu,” *Financial Times*, June 15, 2004.

¹¹ Robert McMillan, “Google Moving Search Records Out of China,” *InfoWorld*, March 1, 2006.

¹² Jim Yardley, “Google Chief Rejects Putting Pressure on China,” *New York Times*, April 13, 2006.

¹³ McMillan, “Google Moving Search Records Out of China.”

¹⁴ *Ibid.*

¹⁵ Thompson, “Google’s China Problem,” p. 64.

In 2005, however, Yahoo! was the first to be accused of collaborating with the Chinese regime to aid in the prosecution of dissidents. On April 30, 2005, Shi Tao, a reporter for *Dangdai Shang Bao* (Contemporary Business News), was convicted of sending the text of an internal message to foreign Web sites. The message was reportedly an internal document from the government, warning journalists about the dangers of dissidents and social destabilization in the run-up to the fifteenth anniversary of the Tiananmen Massacre. Shi admits forwarding the document, but disputes that it was classified. State security officials insist that the classification of the document was “top secret” (*juemi*).

Shi was arrested in 2004 in Taiyuan and moved to a prison in Changsha. The text of the 2005 verdict against Shi Tao, sentenced to 10 years in prison for “divulging state secrets abroad,” reveals that Yahoo’s Hong Kong subsidiary provided Chinese authorities with details that helped identify and convict him.¹⁶ Yahoo! Holdings (Hong Kong) apparently responded to requests from Chinese authorities to provide more details about an IP address, facilitating their ability to link Shi Tao to material posted online. Specifically, the verdict reveals that Yahoo! Holdings (Hong Kong) gave the authorities information that allowed them to link Shi Tao’s e-mail address and the message containing the alleged “state secret” to the IP address of Shi’s computer. Shi’s appeal was denied.

Yahoo! responded to the international media firestorm over Shi’s case by claiming that the company was legally obligated to comply with a valid and legal demand for information according to Chinese law. Company statements argued that the firm’s active involvement in China contributed to the continued modernization of the country, even if this meant complying with national laws that violate human rights.

Much to Yahoo!’s chagrin, however, the Shi Tao case was only the first of a series of Chinese cyber dissident cases implicating the company. In February 2006, Reporters Without Borders obtained the text of the December 2003 verdict against Li Zhi, an official sentenced to eight years in prison for posting “anti-regime” messages and interacting with the banned China Democracy Party. The text confirmed that Yahoo! Hong Kong and Sina.com had both responded to official queries about Li Zhi, verifying that he had set up email accounts on their respective services. The verdict did not confirm, however, that the content of any of his messages had been turned over to the courts, though a telecommunications company was able to find Li Zhi’s address and telephone number based on the IP address used to set up the Yahoo! and Sina accounts.

In April 2006, Reporters Without Borders obtained a copy of the verdict against Jiang Lijun, sentenced to four years in prison for writing pro-democracy articles. In a section entitled “physical and written evidence,” Yahoo! Hong Kong reportedly confirmed that the account name “ZYMZd2002,” which contained a “declaration,” was used jointly by Jiang Lijun and another dissident. Jiang was freed after completing all four years of his sentence.

¹⁶ “Information Supplied by Yahoo! Helped Journalist Shi Tao Get 10 Years in Prison,” press release by Reporters Without Borders, September 6, 2005.

Censorship of MSN Spaces

China's most famous blogger, Zhao Jing, started his blog in December 2004, using the pseudonym Michael Anti. His blog was originally hosted on a UK-based service, but in August 2005 the Chinese government reportedly blocked access to his site. Zhao then moved the site to MSN Spaces, which was China's leading blog service provider even though its servers were located in the United States.¹⁷ In December 2005, Microsoft shut down Zhao's site at the request of the Chinese government, which objected to a posting supporting a newspaper strike at the *Beijing News*. The move effectively allowed "Chinese censors to reach across the ocean and erase data stored on American territory."¹⁸ Granted, the fine print of the user "code of conduct" clearly prohibits the uploading, posting, or distribution of any content that "violates any local and national laws that apply to your locations," but Zhao's case was the first public enforcement of the rules.¹⁹

Reacting to the resulting media firestorm, Microsoft's director of government relations told a congressional hearing in February 2006 that the company had saved the deleted postings and sent them to Zhao. An interview with the blogger, however, revealed that Microsoft refused to e-mail the logs to China or even mail a CD to China, insisting instead on mailing a CD of the data to any address in the United States but not China.²⁰

What Are the Key Policy Issues at Stake?

Chinese Internet censorship has significant implications for China's domestic development, its bilateral relations with the United States, and even its international integration into the global economy. Beijing's successful adaptation to a rapidly changing technological environment has effectively precluded the Chinese people from enjoying the full benefits of the Internet, especially the ability to freely communicate and cooperate with an increasingly global community of users. By creating a form of "cyber apartheid," the Chinese Communist Party has protected its monopoly on power at the expense of individual freedom, directly challenging the Bush administration's stated intent "to seek and support democratic movements and institutions in every nation and culture, with the ultimate goal of ending tyranny in our world."²¹ And given Chinese efforts to filter content and hijack DNS requests, it is no hyperbole to say that China is undermining some of the core, trusted protocols of the global Internet.

Since the regime believes that information technology is a key engine of economic development and that future economic growth in China will depend in large measure on the extent to which the country is integrated with the global

¹⁷ "MSN Spaces Rated the Leading Blog Service Provider in China," *People's Daily Online*, December 20, 2005.

¹⁸ Thompson, "Google's China Problem," p.64; "Yahoo Accused of Helping China to Jail User; Draft E-Mail Given to Authorities, Rights Group Says," *Associated Press*, April 20, 2006.

¹⁹ "Microsoft Censors Chinese Blogs," *BBC News*, June 14, 2005.

²⁰ Thompson, "Google's China Problem," p.64.

²¹ *The National Security Strategy of the United States of America*, March 2006.

information infrastructure, overzealous application of DNS hijacking and content filtering could spill over into nonpolitical transactions as well.

Yet, despite the success of the censors in China thus far, there are some reasons for optimism and hope. A 2003 Chinese Academy of Social Sciences (CASS) report on the social impact of the Internet in China found that Chinese Web surfers expect the Internet to enhance freedom of speech and increase opportunities for political participation.²² According to the report, “The Internet is changing the Chinese political landscape. It provides people a platform to express their opinions and a window to the outside world as never before.”²³ As a professional Chinese middle class emerges, it will likely seek to leverage its growing economic clout in the political arena, at least to influence state economic policies. With the media under state supervision, the Internet is an attractive forum for organizing and articulating these preferences and could thus serve as the medium for the pluralization of the Chinese political system, either within a co-opted space permitted by the Chinese Communist Party or in direct opposition. In this way, the Internet in China could facilitate political change in the same way that audiotapes of Khomeini’s speeches helped overthrow the Shah in 1979 and fax machines almost brought down the Beijing government in 1989.

To facilitate a more open Internet in China, however, U.S. policymakers and business leaders confront some difficult questions:

1. Should companies that help the CCP censor the Internet be penalized?

The current economic environment in China encourages the Internet’s commercialization, not its politicization. As one Internet executive put it, for Chinese and foreign companies, “the point is to make profits, not political statements.”²⁴

Even so, American companies involved in the Chinese information revolution have come under increasing scrutiny from NGOs and the Congress for their possible collaborative role in the construction and maintenance of the Great Firewall. On the software and services side, the controversial practices of Yahoo!, Google, Microsoft and others have already been documented above. On the hardware side, companies like Cisco and Nortel have been accused of designing, selling, installing, and maintaining equipment used to censor the Chinese Internet. Cisco has even been accused of producing a custom “censorware” box

²² Guo Liang, *The CASS Internet Report 2003: Surveying Internet Usage and Impact in Twelve Chinese Cities* (Beijing: Chinese Academy of Social Sciences Research Center for Social Development, 2003), 55–57. About 72 percent of Internet users surveyed agreed that the Internet would provide people in China greater opportunities to express their political views, approximately 61 percent stated that it would make it easier to criticize government policies, some 79 percent indicated it would improve people’s understanding of political issues, and 72 percent said they believed the Internet would allow government officials to enhance their understanding of the public’s views.

²³ Guo Liang, 2003, p. 55.

²⁴ Interview with U.S. businessperson, 2001.

for China,²⁵ though the company's CEO in February 2006 denied the charge before the House International Relations Committee. Indeed, much if not all of the functionality ascribed to a custom censorware box is available from off-the-shelf Cisco equipment like the PIX Firewall. At the same time, the company has not explicitly denied that it provides customized training to use Cisco equipment for censorship purposes, nor has it denied that in China, Cisco products are marketed explicitly for Internet policing.

Even if some U.S. software and hardware companies are complicit in Chinese Internet censorship, however, there are very few attractive policy options to deal with the situation, given the domestic Chinese competition faced by U.S. companies and the inherently dual-use nature of the technologies involved. Google's introduction of the censored google.cn, for example, was largely a response to its dramatic loss of market share to a domestic Chinese search engine, Baidu, which is known as "China's Google." Yahoo! and Microsoft also confront successful and dynamic domestic competitors in the e-mail and blog market spaces. Penalizing these companies for their role in censorship would only further erode their market share and cede more of the market to Chinese companies that have few if any qualms about collaborating with the Beijing government to control Internet information. Similarly, penalizing companies like Cisco for selling routers and firewalls to China would simply drive the authorities to purchase their equipment from competing vendors in Europe, Japan, Korea, and elsewhere.

2. Should more resources be devoted to programs designed to subvert China's Internet controls?

Various parties outside of China—ranging from Chinese exiles seeking to promote human rights and democratization in China specifically to international "hacktivists" focused on undermining online censorship worldwide—have responded to Beijing's censorship regime by developing technologies designed to breach the Great Firewall. To date, however, only a few groups have managed to deploy programs that have generated substantial levels of traffic. Many of the circumvention programs are not user-friendly or require sophisticated computer skills to install and operate and therefore appeal to only a small core group of technical experts. Those technologies that are explicitly designed to be as user-friendly as possible still face significant technical obstacles, especially the determined countermeasures of an increasingly sophisticated content filtering and blocking regime.

For many groups, the inability to produce user-friendly software stems from the shortage of manpower and the inadequacy of financial resources. Most of the groups developing anti-censorship programs have only a handful of full-time programmers, and a few are effectively one-man operations. With no commercial applications for their programs, many say private foundations and governments are their only potential sources of financing. Architectural flaws also pose serious concerns; most of the mechanisms designed to breach the Great Firewall suffer to

²⁵ Ethan Guttman, *Losing the New China: A Story of American Commerce, Desire and Betrayal* (New York: Encounter Books, 2004).

from architectural shortcomings that render them vulnerable to several blocking or exploitation measures, including IP blocking, port blocking, packet sniffing, virus attacks, and infiltration by Chinese security agents.²⁶

Even if pro-democracy activists and computer engineers managed to wrest the technological advantage from China's Internet censors, they still would still need to contend with a core fundamental strategic problem: Devising a workable plan for using technology to promote political change in China. It has not been enough simply to make a variety of sources of outside information accessible to Chinese Internet users. There are now many more internal sources of information in China, including an increasingly vibrant traditional media and a dynamic Internet news environment, and these trends reduce the demand for external sources of information, particularly given the possible risks.

Widespread disinterest, apathy, and mistrust of outside sources of information have also limited the Internet's power to spark political change. As digital freedom advocate Bobson Wong has written:

Improving the ability of people in China to access banned material online is certainly necessary and important, but there is no guarantee that Chinese users will want to take advantage of this privilege . . . simply "liberating" China's Internet from government censors may not lead to a dramatic change in popular attitudes. Turning the Internet into an effective tool for social change in China involves not only solving the technological problem of reducing online censorship, but also providing a balanced forum for communication that Chinese users can trust.²⁷

Thus, many anti-censorship activists are faced with a difficult tradeoff: The U.S. government is likely their most attractive source of funding, yet association with a foreign government might compromise their credibility as an unbiased source of information in the eyes of Chinese Internet users.

Is There Any Reason for Hope?

So far, Beijing's countermeasures to outside efforts to undermine the Great Firewall have been relatively successful. The current lack of credible challenges to the regime, however, does not inexorably lead to the conclusion that the regime will forever be immune from the forces unleashed by the flood of information across its borders. To the contrary, the scale of China's information technology modernization suggests that time is ultimately on the side of the regime's opponents. As RAND scholar Nina Hachigian predicts, "Control over information

²⁶ IP blocking refers to measures that block user access to specific numeric IP addresses. Port blocking refers to measures that block specific Internet service protocols (such as Port 80 for Web browsing). Packet sniffers are computer software or computer hardware that can intercept and log traffic passing over a digital network or part of a network. As data streams travel back and forth over the network, the sniffer captures each packet and eventually decodes and analyzes its content according to the appropriate RFC or other specifications.

²⁷ Bobson Wong, "A Matter of Trust: The Internet and Social Change in China," *China Rights Forum*, no. 3 (2003): 41-43.

will slowly shift from the state to networked citizens,” leading to potentially “seismic” changes.²⁸ In the words of a Chinese researcher, “It will be impossible to control this technology completely, even with filters and an army of trained digital agents.”²⁹

U.S. policymakers should therefore keep their eyes on the horizon—encouraging the transfer of information communications technologies to China, even though some of the technologies can be used to constrain information flow. Although no one can predict the course of China’s Internet revolution, we can be comforted by the fact that the transformation is under way.

²⁸ Nina Hachigian, “China’s Cyber-Strategy,” *Foreign Affairs* 80, no. 2 (March/April 2001): 118–133.

²⁹ Interview with Chinese researcher, January 2001.