Backgrounder

Published by The Heritage Foundation

No. 1806
October 8, 2004

China's Orwellian Internet

John J. Tkacik, Jr.

The Internet once promised to be a conduit for uncensored information from beyond China's borders, and for a brief, shining instant in modern Chinese history, it was a potential catalyst for political and human rights reform in China. However, for China's 79 million Web surfers—the most educated and prosperous segment of the country's population—the Internet is now a tool of police surveillance and official disinformation. If a stable, democratic China remains a key goal of America's global strategy, the Bush Administration and Congress must consider ways to penetrate China's "Great Firewall." The United States must restrain the transfer of sensitive and often proprietary cybertechnology from Western—including American—firms to Chinese police agencies. Just as the United States established Radio Free Asia to provide a source of uncensored news, so too must the U.S. minimize the obstructions that the Chinese face in acquiring and disseminating news and information via the Internet.

The Democratic Imperative

In 2003, President George W. Bush declared, "We welcome the emergence of a strong, peaceful, and prosperous China. The democratic development of China is crucial to that future."[1] This imperative of a democratic China has been a feature of America's strategic plan for nearly six decades. President Harry S. Truman said that a "strong, unified and *democratic* China" is "of the utmost importance to world peace" and consequently "in the most vital interests of the United States."[2] Yet two out of three is not good

Talking Points

- President Truman declared that it is "in the most vital interests of the United States" to have a "strong, unified and democratic China." But two out of three is not good enough. A strong, unified, and undemocratic China is a greater potential threat to the region and to America than a weak, undemocratic one.
- China's Internet, once a conduit for uncensored information, is now a tool of police surveillance, propaganda, and official disinformation.
- If a democratic China remains a key goal of America's global strategy, the Administration and Congress must consider ways to penetrate the "Great Firewall of China."
- The United States should restrain the transfer of sensitive and often proprietary cybertechnology from American firms to Chinese police agencies.
- Congress should create an Office of Global Internet Freedom to coordinate U.S. efforts to develop counter-censorship technologies.

This paper, in its entirety, can be found at:
www.heritage.org/research/asiaandthepacific/bg1806.cfm

Produced by the Asian Studies Center

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

enough. A strong, unified, and *undemocratic* China is a greater potential threat to the region and to America than a weak and undemocratic one.

If the U.S. truly believes that a peaceful China evolving along democratic lines is in America's interest—as well as in the interest of the Chinese people—then the U.S. should recognize that the Internet could be a most effective tool. Moreover, it requires no special informational input from the U.S. government. Key elements of democratic thought, free market economics, and concepts of a civil society are all freely available on the Internet. Yet regrettably, the Internet has an even greater potential as an instrument of Orwellian thought control. With the help of foreign—including American—high-tech companies, Internet technologies have enabled China's Big Brother to keep a close eye on its citizens and to identify and arrest those who spread democratic ideals.

Democratic reform in China is highly unlikely to come from the top down, that is, from the Chinese Communist Party. It will have to emerge from the grass roots. If the Internet is to be a medium of that reform, ways will need to be found to counter China's official censorship and manipulation of digital communications. The cultivation of democratic ideals in China therefore requires that the U.S. adopt policies that promote freedom of information and communication by funding the development of anti-censorship technologies and restricting the export of Internet censoring and monitoring technologies to police states.[3]

Naïve optimism about China's Internet fills the pages of America's leading papers and scholarship, giving the impression that an increasingly wired China will necessarily evolve into an open and free society. One recent editorial in *The Wall Street Journal* optimistically claimed, "By searching for new measures to clamp down on its increasingly high-tech citizens, the Communist Party has taken on a battle it is bound to lose."[4]

For Chinese Communist Party leaders, domestic "stability" is a prerequisite to national goals, but by stability they mean unchallenged Party rule. Thus while cosmopolitan urban Chinese—who perhaps number as many as 50 million (out of China's 1.3 billion people) and have an average annual family income in excess of $5,000—increasingly enjoy the electronic gadgetry of modern life, they have learned that the price to be paid is the unquestioned rule of the Party. As the central propaganda organs and police agencies maintain and tighten their grips on information flow and private digital communications, the average Chinese citizen now realizes that political speech on the Internet is no longer shrouded in anonymity: Private contacts with like-minded citizens in chat rooms, or even via e-mail text messaging, are not likely to escape police notice.

Big Brother Is Watching

For several years during the 1990s, Chinese Internet users gained increasing amounts of information from the Internet. By 1998, according to an insider's account of China's Internet development, the Chinese Public Security Ministry and its police stations around the country found that their resources for monitoring the Internet were becom-

1. The White House, *The National Security Strategy of the United States of America*, September 2002, p. 27, at *www.whitehouse.gov/nsc/nss.html* (October 4, 2004).
2. See President Truman's instructions to General George C. Marshall in U.S. Department of State, *United States Relations with China, with Special Reference to the Period 1944–49* (Washington, D.C.: U.S. Government Printing Office, 1949), p. 133 (emphasis added). This document is also known as the China White Paper.
3. For a comprehensive discussion of policy options, see *Report to Congress of the U.S.–China Economic and Security Review Commission* (Washington, D.C.: U.S. Government Printing Office, June 2004), pp. 213–223. For several technical briefings on this issue, see Hearings, *SARS in China: Implications for Information Control, Internet Censorship, and the Economy*, U.S.–China Economic and Security Review Commission, 108th Cong., 1st Sess., June 5, 2003, at *www.uscc.gov/hearings/2001_02hearings/transcripts/02_06_05tran.pdf* (October 4, 2004).
4. Op-ed, "China's Cyber Censors," *The Wall Street Journal*, July 6, 2004, at *online.wsj.com/article/0,,SB108906627345855454,00.html* (September 24, 2004, subscription required).

ing overwhelmed.[5] Several major U.S. firms came to the aid of the Chinese security services by constructing a new Internet architecture that enabled China's cyberpolice to monitor Internet sites in real time and identify both the site owners and visitors.

The inevitable result is that suppression of Internet dissent has increased in recent years. China is said to have the largest prison population of "cyberdissidents" in the world. As of June 2004, the Reuters news service reported there were 61 cyberdissidents in jail for criticizing the Chinese government.[6] In January 2004, Amnesty International documented 54 cases of individuals arrested for "cyberdissent," but concluded that the 54 cases were probably just "a fraction" of the actual number detained.[7] According to another report, 13 Internet essayists were tried, sentenced, and denied appeals between October and December of 2003 alone.[8]

In April 2004, *The Washington Post* described a typical cyberdissidence case involving a group of students who were arrested for participating in an informal discussion forum at Beijing University. It was a chilling report that covered the surveillance, arrest, trial, and conviction of the dissidents and police intimidation of witnesses.

Yang Zili, the group's coordinator, and other young idealists in his Beijing University circle were influenced by the writings of Vaclav Havel, Friedrich Hayek, and Samuel P. Huntington. Yang questioned the abuses of human rights permitted in the "New China." His popular Web site was monitored by police, and after letting him attract a substantial number of like-minded others, China's cyberpolice swept up the entire group. Relentlessly interrogated, beaten, and pressured to sign confessions implicating each other, the core members nevertheless withstood the pressure. The case demonstrated that stamping out cyberdissent had become a priority state function. According to the *Post*, Chinese leader Jiang Zemin considered "the investigation as one of the most important in the nation." In March 2003, the arrestees were each sentenced to prison terms of between eight and ten years—all for exchanging opinions on the Internet.[9]

Then there is the case of Liu Di, a psychology student at Beijing Normal University who posted Internet essays under the screen name of Stainless Steel Mouse. She is an exception among cyberdissidents—after a year behind bars, she is now out of jail. The then 23-year-old Liu was influenced by George Orwell's *1984* and became well known for her satirical writing and musings on dissidents in the former Soviet Union. She defended other cyberdissidents, supported intellectuals arrested for organizing reading groups, attacked Chinese chauvinists, and, in a spoof, called for a new political party in which anyone could join and everyone could be "chairman." Arrested in November 2002 and held for nearly one year without a trial, she became a *cause célèbre* for human rights and press freedom groups overseas and apparently gained some notoriety within China as well. Although she had been held without trial and was never formally charged, she was imprisoned in a Beijing jail cell with three criminals. In December 2003, she was released in anticipation of Premier Wen Jiabao's visit to the U.S. Yet nine months after returning to the Beijing apartment that she shares with her grandmother, Liu still finds police security officers posted at her home. She has found it impossible to find a regular job, and police moni-

5. Ethan Gutmann, *Losing the New China: A Story of American Commerce, Desire and Betrayal* (San Francisco: Encounter Books, 2004), p. 130.
6. Reuters, "China Is Largest Jailer of Cyber Dissidents," June 24, 2004, at *www.abc.net.au/news/newsitems/200406/s1139911.htm* (October 6, 2004).
7. Amnesty International Report, "People's Republic of China, Controls Tighten As Internet Activism Grows," January 28, 2004, at *web.amnesty.org/library/Index/ENGASA170012004* (September 24, 2004).
8. Liu Di, "The Powerful Voice of a Mouse," *The Washington Post*, December 7, 2003, p. B02, at *www.washingtonpost.com/wp-dyn/articles/A40194-2003Dec5.html* (September 24, 2004).
9. Philip P. Pan, "A Study Group Is Crushed in China's Grip," *The Washington Post*, April 23, 2004, p. A1, at *www.washingtonpost.com/wp-dyn/articles/A34768-2004Apr22.html* (September 24, 2004).

tors block her screen name Stainless Steel Mouse from Web sites.[10]

One reason Ms. Liu was released was the incessant prodding of another Internet essayist, Du Daobin (identified only as a 39-year-old civil servant from Hubei province), who condemned Liu's jailing. In turn, at least 1,000 people signed a petition in support of Du that urged the government to stop using anti-subversion laws to hinder free speech. Of course, Du was charged with subversion and jailed. In June 2004, a Chinese court announced that Du would get a suspended sentence instead of a long prison term. Du's case, says *The New York Times*, may not be one of government magnanimity, but rather an example of what can happen to other cyberdissidents in "a quiet but concerted push to tighten controls of the Internet and surveillance of its users even though China's restrictions on the medium are already among the broadest and most invasive anywhere."[11]

On July 31, 2004, hundreds of villagers of Shijiahecun hamlet in rural Henan province demonstrated against local corruption. Provincial police from the capital at Zhengzhou dispatched a large anti-riot unit to the village, which attacked the crowd with rubber bullets, tear gas, and electric prods.[12] Propaganda officials immediately banned media coverage of the incident, and the outside world might not have learned of the clash if an intrepid local "netizen" had not posted news of it on the Internet. The Web correspondent was quickly identified by Chinese cybercops and arrested during a telephone interview with the Voice of America on August 2. While the informant was on the phone with VOA interviewers in Washington, D.C., he was suddenly cut short, and the voice of a relative could be heard in the background shouting that authorities from the Internet office of the Zhengzhou public security bureau (*Shi Gonganju Wangluchu*) had come to arrest the interviewee. After several seconds of noisy struggle, the telephone connection went dead.[13]

Popular Web Sites Shut Down

In other cases, when it is difficult for the state to discern whether or not certain Internet activity is a clear and present danger, the cyberpolice simply shut down Web sites. For example, on September 13, 2004, officials from the State Council News office, the ministry of information industry, and the ministry of education suddenly appeared at Beijing University to announce the closure—for no stated reason—of *Yi Ta Hutu* (One Big Mess), a popular university bulletin board system (BBS). It was understood that the BBS was shut down for "disseminating political rumors." At the same time, the government ordered all Web sites in China to delete Internet links to One Big Mess. Six days later, three Beijing University law instructors wrote an open letter to Chinese President Hu Jintao and Premier Wen Jiabao praising the closed BBS site as "an important channel by which the party and government can understand the feelings of the people." The professors then condemned the BBS closure as "suppressing freedom of speech" and decried the state action as "illegal" and "regrettable." Needless to say, the professors' open letter was not published on Chinese sites and had to be e-mailed to correspondents outside China.[14]

10. Jim Yardley, "A Chinese Bookworm Raises Her Voice in Cyberspace," *The New York Times*, July 24, 2004, at *www.nytimes.com/2004/07/24/international/asia/24prof.html* (September 24, 2004).
11. See Jennifer Chou, "China's Cyber-Crackdowns," *The Washington Times*, January 1, 2004, at *www.washingtontimes.com/op-ed/20031231-083459-2999r.htm* (September 30, 2004). For information on Mr. Du's trial, see Howard W. French, "Despite an Act of Leniency, China Has Its Eye on the Web," *The New York Times*, June 27, 2004, at *www.nytimes.com/2004/06/27/international/asia/27chin.html* (September 24, 2004).
12. Philip P. Pan, "Farmer's Rising Anger Erupts in China Village," *Washington Post*, August 7, 2004, p. A1, at *www.washingtonpost.com/wp-dyn/articles/A46778-2004Aug6.html* (September 24, 2004).
13. "Zhengzhou Zhenya shangfang cunminde wangmin zhuan bei bu, Jiazhong jieshou dianhua fangwen shi zhuanchu zhuaren sheng, gunagfang dui ci fengkou" (netizen who reported Zhengzhou crackdown said to have been arrested, sounds of police seizure during telephone interview at home, official silence on case), *World Journal* (New York, in Chinese), August 4, 2004, p. A8.

One Big Mess was host to over 800 separate discussion boards, boasted an average of 20,000 page viewers at any one time, and had over 300,000 regular viewers on its list.[15] Instead of being a vehicle for democratic reform, Chinese security services now use the Internet to identify and eliminate networks of dissent.

Surveys conducted by the Chinese Academy of Social Sciences show that in metropolitan areas more than one in three people has Internet access.[16] Even in small cities, 27 percent of residents have access to the Internet.[17] Given these numbers and the determination of the Chinese Communist Party to stamp out each and every vestige of dissent and opposition, it is not surprising that China has the most extensive Internet censorship in the world.[18] At last estimate, access was blocked to 19,000 political Web sites considered threatening.[19] These blocked sites include popular foreign news, political, religious, and educational Web sites, including fairly innocuous Web sites of church and religious organizations serving foreign businessmen and residents.[20]

Clampdown Aided by U.S. Firms

In addition to blocking sensitive Web sites, the government also controls the sites that appear in popular global search engines such as Yahoo and Google. For instance, a search for "Jiang" in the Chinese version of Yahoo returns only 24 sites, all of which are flattering to Chinese leader Jiang Zemin. Moreover, e-mail subscription services are blocked and the government can and does monitor personal e-mail and "erase online content considered undesirable."[21]

Some American Internet portal companies assist the Chinese government in limiting information available to the Chinese people. In 2001, Yahoo signed an agreement with Chinese security authorities to block critical content from its Chinese language servers. Yahoo further promised to avoid "producing, posting or disseminating pernicious information that may jeopardize state security and disrupt social stability."[22] By contrast, the search engine Google, which has not signed such an agreement, has been deemed "unselective" and "unsupervised" by the security authorities and has

14. "San Jiaoshou shangshu Hu Wen, Kangyi Beida Wangzhan bei feng, Gongkaixin dui 'yi ta hutu' BBS zhan cao mouming jiangzui biao yihan, tongchen zhengfu weifa, daya yanlun ziyou" (three professors petition Hu Jintao and Wen Jiabao, protest closure of Beijing University Web site, open letter expresses regret at unspecified accusation against "One Big Mess" BBS site, decry government illegal suppression of freedom of expression), *World Journal* (New York, in Chinese), September 24, 2004, p. A8.
15. *Ibid*.
16. Charles Hutzler, "Social, Economic Impact Is Expected As Internet Use Spreads Beyond Big Cities," *The Wall Street Journal*, Nov. 18, 2003, at *online.wsj.com/article/0,,SB106909460599389 00,00.html* (September 24, 2004, subscription required).
17. *Ibid*.
18. Amnesty International, "People's Republic of China: State Control of the Internet in China," January 28, 2004, at *web.amnesty.org/library/index/engasa170072002* (September 24, 2004).
19. Associated Press and *New York Times* News Service, "China's Internet Censorship World's Most Extensive," *The Taipei Times,* December 5, 2002, at *www.taipeitimes.com/News/front/archives/2002/12/05/185937* (September 24, 2004).
20. Associated Press, "Officials in Shanghai to 'Update' Rules on Religion," reprinted in *The Taipei Times*, July 21, 2004, p. 5, at *www.taipeitimes.com/News/world/archives/2004/07/21/2003179804* (September 24, 2004).
21. Associated Press, "Beijing Blocks Access to Google," *The Taipei Times*, September 4, 2002, at *www.taipeitimes.com/news/2002/09/04/story/0000166786* (September 24, 2004). See also Charles Hutzler, "China Finds New Ways to Restrict Access to the Internet," *The Wall Street Journal*, September 1, 2004, at *online.wsj.com/article/0,,SB109399116510306244,00.html* (September 24, 2004, subscription required).
22. Richard McGregor, "China Steps Up Curbs on Internet," *Financial Times,* Sept. 11, 2002. See also Editorial,"Yahoo's China Concession," *The Washington Post*, August 19, 2002, p. A12, at *www.washingtonpost.com/wp-dyn/articles/A34015-2002Aug18.html* (September 24, 2004). Details on Yahoo's involvement with China's Internet censors is also found in Gutman, *Losing the New China*, p. 132.

consequently been censored. Google is especially feared by China's cybercensors because of its cache feature that makes available saved copies of Web pages that have been deleted and Web sites that have been taken down. Since 2002, Chinese visitors to Google.com have been re-routed to a local search engine.[23]

Surveillance of the Chinese Internet is greatly enhanced by the custom design of China's Internet portals. All Chinese Internet traffic is routed through five major channels using devices sold by a U.S.-based corporation. American engineers developed special routers, integrators, and a "special firewall box" programmed to monitor Internet traffic and detect selected keywords.[24] China Telecom bought "many thousands" of these special firewall boxes from a U.S. firm for $20,000 each.[25] These boxes allow the Chinese government to search for, identify, and intercept potentially subversive transmissions, which had theretofore been considered difficult to track.[26] By exporting sophisticated communications technology to China, North American telecoms and software companies facilitated the construction of the "Great Firewall of China" against the world and provided the Chinese government with a means to conduct surveillance against its citizens.[27]

Big Brother's Eyes at Internet Cafes

The Chinese government has also installed elaborate monitoring systems at all Chinese Internet cafes. For example, the Shanghai Cultural Broadcast and Film Management Bureau is installing software in 110,000 computers in the city's 1,329 Internet cafes for comprehensive long-term surveillance. This software allows the government to monitor, in real time, the identities of Internet users and the sites that they access or attempt to access. New regulations require all Internet users at cafes to register in their real names and provide identification cards before log-on. Press announcements of Shanghai's new Internet regulations indicate that the local security services expect all Internet cafe proprietors to cooperate—and pay for the new software upgrades. China's large eastern province of Shandong has also reported adoption of an "internet real names" project to track cybercafe Web surfers.[28]

Online conversations are subject to constant eavesdropping, and Web surfing is scrutinized. Yahoo-China, for example, reportedly hires supervisory "big mamas" for the teams of censors assigned to every Yahoo-hosted Internet chat room in China. One American expert in the Chinese Internet describes the big mamas' mission as deleting politically undesirable chat room comments in real time and sending warnings to violators in cyberspace. All Chinese chat rooms, according to this expert, are watched by surveillance teams who can also monitor e-mails, including Web-based accounts, and may use unblocked Web sites as "tripwire" stings to locate and trap possible agitators.[29]

Chinese censors periodically and inexplicably block and unblock foreign news sites that inquisitive surfers may try to access.[30] There is a special task force of some 30,000 "cybercops" who patrol the World Wide Web, block select foreign news sites, and terminate domestic sites with politically

23. Gutman, *Losing the New China*, p. 165.
24. Reporters Without Borders, "Internet Under Surveillance, 2004: China," June 22, 2004, at *www.rsf.fr/article.php3?id_article=10749&Valider=OK* (September 24, 2004).
25. Gutman, *Losing the New China*, p. 130.
26. Ethan Gutmann, "Who Lost China's Internet?" *The Weekly Standard*, February 15, 2002, at *www.weeklystandard.com/Utilities/printer_preview.asp?idArticle=922* (September 24, 2004).
27. Amnesty International, "State Control of the Internet in China," November 26, 2002, p. 13, at *web.amnesty.org/library/Index/engasa170072002?OpenDocument&of=COUNTRIES%5CCHINA* (October 6, 2004).
28. Adina Matisoff, "News Update—Mid-February–Early May 2004," China Rights Forum, No. 2, 2004, p. 9, at *iso.hrichina.org/download_repository/2/NewsUpdate6.2004.pdf* (September 24, 2004).
29. Gutmann, "Who Lost China's Internet?"

sensitive information. Coupled with the ability to log viewers of sensitive sites, security agents may record names of surfers who attempt to access forbidden sites or selectively unblocked sites for further monitoring. In this way China's Internet has increasingly become a tool for security agencies to identify, monitor, arrest, and imprison potential dissidents.[31]

Censorship Under the Guise of Moral Propriety?

The Beijing government emphasizes the dangers of corrupt influences on children and says that in one survey 60 of 100 juvenile delinquents in a Beijing courthouse were frequent visitors to pornography sites. In what appeared to be a commendable effort to bolster youth morals, Chinese authorities shut down over 30 pornography sites between June and July of 2004.[32]

Although President Hu's anti-porn crusade has superficially lofty goals, the nationwide crackdown conveniently tightens state control over the spread of digital information. In fact, more than 90 percent of the articles in China's legal regime governing Internet sites is "news and information," and less than 5 percent is "other inappropriate content."[33] Recent reports indicate that authorities in Shanghai intend to restrict Internet communications for religious groups. China maintains restrictions on religious expression and does not permit religious activities coordinated between Chinese and religious groups from abroad.[34] As digital communications present a potential gap in Beijing's scope of supervision, the crackdown against pornography appears to be a smokescreen for increased surveillance of political dissent.

Mobile Phone Text Messaging Tracked

For several days in late September 2004, a Chinese-citizen researcher for the Beijing bureau of *The New York Times* was—unbeknown to him—hunted by Chinese police for providing his employer with news that China's leader Jiang Zemin was planning to retire. The researcher had been visiting friends in Shanghai and had turned off his mobile phone. When he switched on his phone again a few days later, it took secret police less than an hour to track him down at a restaurant and arrest him.[35] It was just the latest evidence that China's mobile phone network has become a means of police surveillance. Yet for several years, Chinese citizens had used mobile phone text messages to disseminate information.

In February 2003, a mysterious virus swept through the southern Chinese province of Guangdong, decimating the staffs of hospitals and clinics. According to *The Washington Post*, "there were 900 people sick with SARS [sudden acute respiratory syndrome] in Guangzhou and 45 percent of them were health care professionals." The Chinese media suppressed news of the disease, apparently in the belief that the public would panic, but:

> [News] reached the Chinese public in Guangdong through a short-text message, sent to mobile phones in Guangzhou around noon on Feb. 8. "There is a fatal flu

30. Reuters, "Beijing Replaces Internet Blocks After Bush Departs," *The Taipei Times*, October 23, 2001, at *www.taipeitimes.com/News/front/archives/2001/10/23/108312* (October 6, 2004).
31. Reuters, "China Tightens Its Rules on Internet Address Managers," *The Taipei Times,* November 22, 2003, p. 5, at *www.taipeitimes.com/News/world/archives/2003/11/22/2003076827* (September 24, 2004).
32. "Wanglu Saohuang, Jiuyue Yao Rang Seqing Juechi" (sweep pornography from Internet, sex to be totally eradicated by September), *China Times*, July 20, 2004.
33. For example, see "Hulian Wangzhan Congshi Dengzai Xinwen Yewu Guanli Zhanxing Guiding" (provisional regulations on the management of registration of Internet sites involved in news activities), Xinhua News Online February 8, 2003, at *news.xinhuanet.com/newmedia/2003-02/08/content_897716.htm* (July 19, 2004).
34. Associated Press, "Officials in Shanghai to 'Update' Rules on Religion," *The Taipei Times*, p. 5, at *www.taipeitimes.com/News/world/archives/2004/07/21/2003179804* (October 6, 2004).
35. Josephine Ma, "Arrest of New York Times Researcher Came After It Broke News of Jiang's Departure," *South China Morning Post* (Hong Kong), September 24, 2004, p. A01.

in Guangzhou," it read. This same message was resent 40 million times that day, 41 million times the next day and 45 million times on Feb. 10.[36]

The SARS epidemic taught the Chinese security services that mobile phone text messages are a powerful weapon against censorship and state control of the media. The Chinese government announced in 2003 new plans to censor text messages distributed by mobile telephone. China Mobile, the country's largest service provider, alone tallied 40 billion text messages in 2002.[37] With over 220 billion text messages sent each year via all China's telecom providers, the Chinese government has had to establish 2,800 centers across the country to conduct routine text monitoring. However, interception of personal messages may not be peculiar to China for long. The Ministry of Public Security recently permitted the manufacturer of these low-cost surveillance systems to sell them on the open market, leading to their possible proliferation worldwide.[38]

A Faustian Deal for an Orwellian Future

Without innovations in technology provided to China by Western telecoms, networking, Internet portal, and software firms, the Chinese government could not have gained its current stranglehold over Internet information. The "Great Firewall of China," designed in large part by North American firms, is increasingly effective at monitoring and censoring online speech in a medium that had for a few short years carried a lively debate about democratic ideals. Chinese filtering systems have removed politically provocative Web sites and postings and have redirected Web surfers to search engines that show only content favorable to the regime.[39] China's Internet now serves to disseminate propaganda and block the flow of information and the proliferation of democratic ideas. Contrary to conventional wisdom, which holds the Internet as a great propagator of information and ideas, China's electronic communications are heavily censored and are increasingly used as an instrument for surveillance, repression, and propaganda.

Recommendations for U.S. Policy

A democratic China is indeed "in the most vital interest of the United States," and fostering an environment in China conducive to the free expression of ideas should be a primary objective. The Bush Administration and Congress must consider strategies to break through the Great Firewall. Specifically, the Administration and Congress should:

- **Designate Internet censorship and monitoring systems as "police equipment."** Since the Chinese telecoms and police agencies are using custom-designed Internet hardware and software primarily for police purposes—and because this equipment has been used broadly

36. John Pomfret, "Outbreak Gave China's Hu an Opening, President Responded to Pressure Inside and Outside Country on SARS," *The Washington Post*, May 13, 2003, p. A1, at *www.washingtonpost.com/wp-dyn/articles/A47408-2003May12.html* (September 24, 2004). See also Tian Jing and Feng Liang, "Hu-Jiang Power Struggles Enter Cyberspace," *Asia Times*, July 20, 2004, at *www.atimes.com/atimes/China/FG20Ad04.html* (September 24, 2004).

37. See U.S. Department of State, Bureau of Democracy, Human Rights, and Labor, "Country Reports on Human Rights Practices, 2003: China (Includes Tibet, Hong Kong, and Macau)," February 25, 2004, at *www.state.gov/g/drl/rls/hrrpt/2003/27768.htm* (October 4, 2004).

38. Reporters Without Borders, "China Under Surveillance," June 1, 2004; "China to Censor Text Messages," *BBC News*, July 2, 2004. See also "Statement of Jay Henderson, Director, East Asia & Pacific Division, Voice of America," in *SARS in China*, and Associated Press, "China Ups Surveillance on Mobile Phone Messaging—Reports," July 2, 2004, at *online.wsj.com/article/0,,BT_CO_20040702_001421,00.html* (September 24, 2004, subscription required).

39. Martin Fackler, "China Ends Google Search Block," *Associated Press*, September 12, 2002, at *www.blue-tech.com/topic.asp?TOPIC_ID=24&FORUM_ID=12&CAT_ID=4&Forum_Title=Others&Topic_Title=China+Ends+Google+Search+Block* (October 6, 2004). As of September 2004, according to a report in the *South China Morning Post*, Google searches omitted results from government-banned sites if search requests were made through computers connecting to the Internet in China. See Associated Press, "Google Conforms to Chinese Censorship," in *South China Morning Post*, September 27, 2004, p. 2, at *story.news.yahoo.com/news?tmpl=story2&u=/ap/20040925/ap_on_hi_te/google_china* (October 6, 2004).

to apprehend and arrest political dissidents—these types of software should be designated "police equipment" for the purposes of the Export Administration Regulations (which regulate the export of dual-use items for foreign policy and national security purposes).[40] U.S. exporters should be required to file adequate descriptions of their custom-designed systems with the U.S. government. License applications for exports of these systems to China should be treated in the same way as other police equipment exports to China.

- **Renew research into anti-censorship technologies.** A few years ago the Voice of America briefly sponsored a network of servers, codenamed "Triangle Boy," which was beyond the reach of Chinese censors.[41] Although reportedly successful, the system failed due to inadequate funding and over-cautious handling of the contracts. Rather than funding its expansion, VOA decided to pursue "safe-haven Web sites," but these are now blocked on a real-time basis by Chinese censors. There should be renewed efforts to create an information network that would permit Web surfers in China to access accurate news beyond China's Great Firewall.
- **Establish an Office of Global Internet Freedom.** Legislation—like the Global Internet Freedom Act of 2003 (H.R. 1950)—is already drafted that would create an Office of Global Internet Freedom under the International Broadcasting Bureau (the parent agency for the Voice of America) to coordinate U.S. efforts to develop counter-censorship technologies. The need for a concerted, U.S.-backed campaign to promote democracy in China is urgent, and authorizing legislation should be included in the next State Department authorization bill.

Conclusion

Chinese police surveillance of Internet communications has increased as Chinese citizens have gained more access to the medium. The censors' reach extends to each computer terminal, and even personal mobile phones and personal digital assistants. As Chinese citizens found during the SARS outbreak, mobile phone text messaging and access to the Internet were their only conduits for the truth.

Support for a democratizing China must be a primary objective of American policy. This should be done by challenging the Chinese Communist Party's monopoly on information in that country. U.S. firms that have provided the tools of censorship and surveillance to a police state should also help in defeating those tools. The United States established Radio Free Asia to provide Chinese short-wave radio listeners with uncensored sources of information about what was really happening in China and the world, but short-wave broadcasting is now obsolete. A similar effort on the World Wide Web would have a far greater impact.

—John J. Tkacik, Jr., is Research Fellow in China Policy in the Asian Studies Center at The Heritage Foundation. Augustine T. H. Lo and Emily Ho, interns at The Heritage Foundation, contributed to this paper.

40. The Export Administration Act, which governs shipments of "dual-use" military and civilian applications, lapsed in 1994, but continues to be implemented by emergency powers of the President. See George W. Bush, "Continuation of Export Control Regulations," Executive Order, August 17, 2001, at *www.whitehouse.gov/news/releases/2001/08/20010817.html* (October 4, 2004).

41. "Triangle Boy" was a proxy server system with a triangular architecture for the Chinese Internet user, a fleet of Web servers somewhere outside the Chinese firewall and a "mothership" that the servers report to, but which the Chinese government hackers cannot find. Chinese users who had managed to make contact would be e-mailed new Triangle Boy server addresses each day. When it was finally de-funded, Triangle Boy reportedly had a cache of 600 million Web pages and had tens of thousands of Chinese users. See Gutmann, *Losing the New China*, pp. 155–156.