FREEDOM HOUSE

THROTTLING DISSENT:

CHINA'S NEW LEADERS REFINE INTERNET CONTROL

Throttling Dissent: China's New Leaders Refine Internet Control

Madeline Earp, Research Analyst, Freedom on the Net

July 2013

ACKNOWLEDGEMENTS

Xiao Qiang, founder and chief editor of China Digital Times and an adjunct professor of the School of Information, UC Berkeley, served as an advisor for this report.

A second advisor based in Hong Kong requested anonymity.

At Freedom House, Sanja Tatic Kelly, project director for Freedom on the Net, guided this report and Sarah Cook, senior research analyst for East Asia provided insightful feedback and suggestions. June Kim prepared graphs and additional research. Tyler Roylance, Ilana Ullman and Mai Truong also contributed.

This report was made possible by the generous support of the Netherlands Ministry of Foreign Affairs.

Cover Image: Chinese soldiers march in formation, blocking the view of Tiananmen Square, where communist government forces gunned down hundreds of peaceful protesters in 1989. Photo by Malika Khurana.

ABOUT THIS REPORT

This special report is based on the 2013 China chapter of Freedom House's annual *Freedom on the Net* survey. *Freedom on the Net* is a comparative analysis of internet freedom with a unique methodology, and includes a detailed narrative report and a numerical score for each country assessed. The 2013 edition, which will be published in September, covers 60 countries. Past editions are available at www.freedomhouse.org.

China's numerical score will be published as part of the full report. However, as the home of one of the most systematically controlled and monitored online environments in the world, it will no doubt retain its place among countries where Freedom House categorizes the internet as Not Free. As the *Freedom on the Net 2012* survey noted, China increasingly serves as an incubator for sophisticated new types of internet restrictions, providing a model for other authoritarian countries.

For this reason, Freedom House is publishing the 2013 China narrative as a special report, examining key developments during the *Freedom on the Net* coverage period (May 1, 2012, through April 30, 2013) in the context of the recent leadership change in the Chinese Communist Party. Like all *Freedom on the Net* narratives, the report offers a comprehensive examination of three aspects of internet freedom:

Obstacles to Access: **What prevents users from getting online?**
This section examines infrastructure and the costs associated with internet access, as well as the legal, regulatory, and economic environment for service providers.

Limits on Content: **What can internet users say and do?**
This section looks at content that is banned by law, filtered, blocked, or voluntarily censored. It also examines the diversity of digital media and the impact of civic mobilization online.

Violations of User Rights: **What are the repercussions for online activity?**
Do internet users risk imprisonment, harassment, or attacks—whether physical or digital? This section also assesses online surveillance and privacy violations.

A full checklist of the methodological questions that served as a foundation for the narrative is available at http://www.freedomhouse.org/report-types/freedom-net.

KEY DEVELOPMENTS: MAY 1, 2012-APRIL 30, 2013

- Mobile replaced broadband as the number one means of accessing the internet in 2012 (see **OBSTACLES TO ACCESS**).
- China's cybercafés are now 40% owned by chains, which are easier for authorities to regulate than independent businesses (see **OBSTACLES TO ACCESS** and **VIOLATIONS OF USER RIGHTS**).
- Traffic on Virtual Private Networks (VPNs)—used to bypass censorship—was disrupted, sometimes obstructing commercial use (see **LIMITS ON CONTENT).**
- Regulators ordered online video services to censor short films in July 2012, when users adopted them to bypass film and broadcast restrictions (see **LIMITS ON CONTENT)**
- Security agents in Tibet and Xinjiang searched cellphones to pre-empt allegedly anti-state activity (see **VIOLATIONS OF USER RIGHTS)**.
- A Criminal Procedure Law amendment took effect in January 2013, strengthening legal grounds for detaining anti-state suspects incommunicado (see **VIOLATIONS OF USER RIGHTS)**.

KEY FIGURES

564 million: Internet users the government reported as of January 2013;

986 million: Mobile phone owners reported;

800 million: People still citing television as their main source of news (see **OBSTACLES TO ACCESS**).

94: China's position in one worldwide survey of broadband speeds;

3: Hong Kong's position in the same survey (see **OBSTACLES TO ACCESS**).

400 million: Microblog accounts registered on Sina Weibo;

46 million: Sina Weibo accounts that are actively used;

50,000: Sina Weibo accounts openly operated by ministries or officials (see **LIMITS ON CONTENT).**

24 hours: Time it takes for Sina Weibo to delete most banned posts (see **LIMITS ON CONTENT).**

12: Tibetans detained for allegedly inciting separatism, some via mobile phone (see **VIOLATIONS OF USER RIGHTS).**

20: Uighurs sentenced in March 2013 for alleged militant activity involving internet, phone and digital storage devices (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

The Chinese Communist Party's commitment to curtailing internet freedom was unwavering over the course of the leadership change that took place during the coverage period for this report, May 1, 2012, to April 30, 2013. If anything, the high-level meetings at which the handover was announced served as catalysts for tighter controls on content, measures to deliberately slow internet traffic, and intensified harassment of dissidents, as the party's propaganda and security agencies worked to eliminate any nascent political challenge. The internet restrictions Freedom House documented this year were faster and more nuanced than ever before.

The selection of Xi Jinping as the new party chief and head of state emphasized continuity, a message that was reinforced by the simultaneous promotion of party hard-liners like propaganda czar Liu Yunshan. The rhetoric of the new leadership also harkened back to the past. Party officials circulated seven "speak-nots," or taboo topics—which included "citizens' rights" and "press freedom"—to universities and media groups in May 2013. Meanwhile, Xi adopted the Maoist term "mass line" to encourage fellow cadres to remain close to the people.

This conservative discourse cannot conceal the unprecedented transformation taking place in China: More than 500 million people in the country are now online. Internet penetration is at 42 percent, compared with just 6 percent when Xi's predecessor, Hu Jintao, took office in 2003. Residents of cities like Shanghai and Beijing are the primary beneficiaries of this expanded access, while rural areas lag behind. An estimated 800 million people still rely on television outlets, like state broadcaster China Central Television (CCTV), as their main source of information.[1] But for the first time on record, more Chinese people connected to the internet via mobile phone than through any other method in the past year, meaning penetration will only continue to climb.

Internet access has provided Chinese citizens with new tools to challenge policy. This year, millions of online comments about air pollution spurred a nationwide upgrade of oil refineries. Online forums also host a surprising range of opinions on political topics. When Edward Snowden fled to Hong Kong after leaking U.S. National Security Agency secrets, users of microblog platforms in China both supported and derided him; some joked cynically that he should see how China handles its citizens' internet records.[2]

[1] Hu Yong et al., *Mapping Digital Media: China* (New York: Open Society Foundations, 2012), http://www.opensocietyfoundations.org/sites/default/files/mapping-digital-media-china-20121009.pdf.
[2] Wendy Qian, "Chinese Web Users React to PRISM: The End of the Affair with Google and Apple?" *Tea Leaf Nation*, June 11, 2013, http://www.tealeafnation.com/2013/06/chinese-web-users-react-to-prism-the-end-of-the-affair-with-google-and-apple/.

Many believe that such incremental civic gains will inevitably spark political reform. A 2013 meme imagined a future shift in the perspective of the Chinese authorities: "When there are a hundred of you, we will detain you," it read, but "when there are a hundred thousand of you—we will join you."[3] Yet the internet has also provided those authorities with an extraordinary range of tools to contain critical conversations. A 2012 academic review of censorship across nearly 1,400 online platforms in China estimated that 13 percent of posts containing sensitive keywords were deleted, many within 24 hours of publication, some within minutes.[4]

Even with vast technological and human resources at their disposal, censors struggled to limit some online debates in the past year. Actress Yao Chen posted a quotation from Soviet-era dissident Aleksandr Solzhenitsyn, "One word of truth outweighs the whole world," to her network of 32 million microblog followers in support of *Southern Weekly* journalists in Guangzhou who were on strike against censorship in January 2013.[5] Anti-Japanese protesters also overwhelmed content controls during a flare-up in the territorial dispute between China and Japan in September 2012. Online vitriol escalated into violent rioting, which Chinese Communist Party (CCP) officials consider a threat even when it supports their position.

But Chinese information authorities are also adept at manipulation, and increasingly adaptable as complex situations unfold. In Guangzhou, propaganda officials negotiated with journalists to end the January strike without conceding to all their demands, and the story fell out of the public eye. It was a memorable achievement, but no other newsrooms were emboldened to follow suit. A state-led wave of editorials condemning anti-Japanese activity helped rein in protests the previous September. Experts even speculate that censorship can be temporarily lifted, and criticism of select officials tacitly encouraged, as a weapon in the party's internal politics. Anticorruption campaigns spread like wildfire online in China, helping the central government hold local officials in check. Yet when the *New York Times* and Bloomberg accused the families of top leaders of amassing disproportionate wealth, their websites were subjected to punitive blocking and their staff computers were hacked.

Even when content is filtered, the process is being constantly refined, often by private companies that serve as intermediaries between the state and users. The 1989 Tiananmen Square massacre is so thoroughly censored that users of the popular Sina Weibo

[3] Xiao Shu, "The Southern Weekly Incident, An Exercise in Citizen Action," China Media Project, January 31, 2013, http://cmp.hku.hk/2013/01/31/31034/.
[4] Gary King, Jennifer Pan, and Margaret Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression," Working Paper, June 18, 2012, http://gking.harvard.edu/files/censored.pdf.
[5] Scott Greene, "Southern Weekly Editorial Staff Goes on Strike," China Digital Times, January 6, 2013, http://chinadigitaltimes.net/2013/01/southern-weekend-editorial-staff-goes-on-strike/.

microblogging platform are not even able to use the search term "today" on the anniversary, June 4.[6] Yet this year, Sina unblocked a handful of Tiananmen-related search terms, allowing users to access dozens of discussions—though unrelated to the 1989 protests in Beijing or the subsequent military crackdown.[7] By offering sanitized results rather than the standard message that blocked keywords usually produce, the company appeared determined to make its censorship invisible.

Far from stifling private innovation, the state has effectively harnessed it to further its own goals. Sina publicly acknowledges that it cannot yet fulfill all of the Chinese government's requirements, like registering its Weibo users' real names. But to avoid getting shut down, it will continue to try. Indeed, many of the more subtle developments documented in this report did not originate with the central propaganda department, a bastion of conservative ideology not known for nuance. Instead, they were developed by service providers looking to satisfy the government's demands while maintaining the illusion of freedom for their users. Google, since it challenged the Chinese government's censorship practices in 2010, has attempted to innovate on the side of transparency, briefly informing Chinese users of blacklisted search terms in 2012.[8] But its experiments have cost it considerable market share as the authorities seek to marginalize the company.

Much is at stake for these firms, but the penalties of defying the state are far greater for individual dissidents. Security agencies make use of widespread surveillance capabilities and a politicized legal system to pursue selective prosecutions of dozens of people like Cao Haibo, whose eight-year prison sentence for publishing antistate content online was reported in November 2012. What constitutes antistate content is alarmingly broad—in Cao's case it was articles he had written about democracy—and can include material published years before a case comes to trial, whether or not it was censored at the time. Ethnic minorities in regions where CCP rule is disputed or resented, such as Tibet and Xinjiang, are particularly vulnerable. At least a dozen Tibetans and 20 Uighurs were jailed during the coverage period in relation to their sharing of information online or via mobile phone. Prosecutors' claims that they were inciting separatism or violence are impossible to verify, as their trials lack due process and are closed to observers. The state continues to pour resources into separating these perceived enemies from families, lawyers, and journalists. In 2012, China spent more on "social stability maintenance"—which includes many of the practices of information control outlined in this report—than it did on defense.

[6] "Censoring a Commemoration: What June 4-Related Search Terms Are Blocked on Weibo Today," Citizenlab, June 3, 2013, https://citizenlab.org/2013/06/censoring-a-commemoration-what-june-4-related-search-terms-are-blocked-on-weibo-today/.
[7] "Sina Testing Subtle Censorship ahead of Tiananmen Anniversary," Greatfire.org, May 31, 2013, https://en.greatfire.org/blog/2013/may/sina-testing-subtle-censorship-ahead-tiananmen-anniversary-0.
[8] Censors quickly disabled the feature, and the company apparently discontinued it. Bill Bishop, "Today's China Readings," *Sinocism China Newsletter*, July 11, 2012, https://sinocism.com/?p=5722; "All Blocked Keywords According to Google," Greatfire.org, June 2, 2012, https://en.greatfire.org/blog/2012/jun/all-blocked-keywords-according-google.

The CCP's influence online reaches far beyond China's borders. Nearly a third of cyberattack traffic worldwide in 2012 was traced to Chinese soil, and cybersecurity experts tracked one notorious hacking group to a military facility in Shanghai. Such international activity generally falls outside the scope of this report, but it is rooted in the online environment outlined here. It also serves as an added reminder that Chinese internet freedom, or the lack thereof, has ramifications for the entire world.

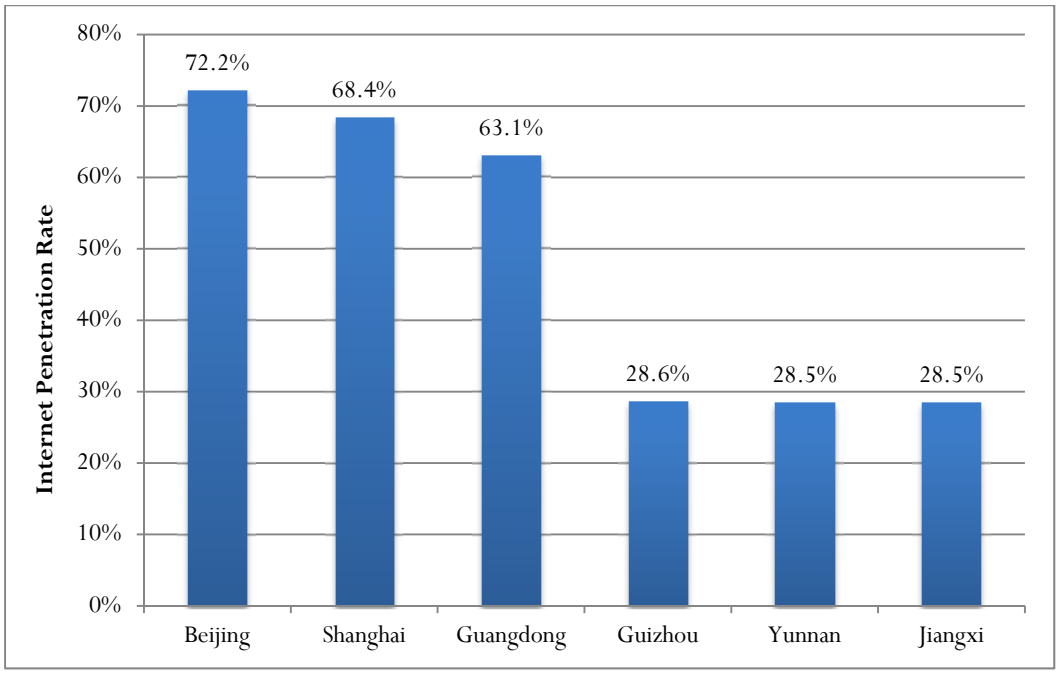
OBSTACLES TO ACCESS

China had the largest number of internet and mobile phone users in the world in January 2013, with an estimated 564 million and 986 million, respectively.[9] These figures, though staggering, paint an incomplete picture of China's uneven economic development and manipulated connectivity. Average broadband connection speeds are comparatively slow, leaving China in 94th place in global rankings.[10] It is stymied by poor infrastructure—particularly in the country's vast rural areas—and a telecommunications industry dominated by state-owned enterprises. Centralized control over international gateways and sporadic, localized shutdowns of internet access around sites of social unrest are significant obstructions to full and free access. Nationwide blocking, filtering, and monitoring systems further slow access to international websites.[11] The Hong Kong administrative region, free of these obstacles, enjoys the third-fastest average connection speeds worldwide, after South Korea and Japan,[12] and at a fraction of mainland prices.

The China Internet Network Information Center (CNNIC), an administrative agency under the Ministry of Industry and Information Technology (MIIT), reports that rates of internet adoption have actually slowed since 2011 as the urban market approaches saturation.[13] Moreover, the gap between penetration rates in urban and rural areas has widened since 2007.[14] The 72.2 percent of residents online in the capital, Beijing, vastly outnumber the 28.5 percent with internet access in the least-connected province of Jiangxi in the southeast.[15] This divide kept overall internet penetration at just 42.1 percent,[16] slightly higher than the global average, which was 35 percent in 2011.[17]

[9] CNNIC, "The CNNIC Released the 31st Statistical Report on Internet Development in China," News Release, January 15, 2013, http://www1.cnnic.cn/IDR/ReportDownloads/201302/P020130221391269963814.pdf.
[10] Lin Jingdong, "Global Speed Heavy: Mainland China Ranked 94th in the Second Half of 2012," *VentureData.org*, January 26, 2013, http://www.venturedata.org/?i480706_Global-speed-Heavy-Mainland-China-ranked-94th-in-the-second-half-of-2012.
[11] James Fallows, "The Connection has been Reset," The Atlantic, March 2008, http://www.theatlantic.com/magazine/archive/2008/03/-ldquo-the-connection-has-been-reset-rdquo/6650/.
[12] Christy Choi, "Hong Kong Has Fastest Peak Internet Speed in World," *South China Morning Post*, January 25, 2013, http://www.scmp.com/news/hong-kong/article/1135480/hong-kong-has-fastest-peak-internet-speed-world?page=all.
[13] CNNIC, *Zhong Guo Hu Lian Wang Fa Zhan Zhuang Kuang Tong* [The 28th Report on the Development of the Internet in China] (Beijing: CNNIC, 2011), http://www.cnnic.cn/research/bgxz/tjbg/201107/P020110721502208383670.pdf.
[14] CNNIC, *Zhong Guo Hu Lian Wang Fa Zhan Zhuang Kuang Tong* [The 29th Report on the Development of the Internet in China] (Beijing: CNNIC, 2012), 21, http://www.cnnic.cn/research/bgxz/tjbgdtygg/dtgg/201201/P020120116330880247967W020120116337628870651.pdf; Benat Bilbao-Osorio, Soumitra Dutta, and Bruno Lanvin, "The Global Information Technology Report 2013," World Economic Forum, 2013, http://www3.weforum.org/docs/WEF_GITR_Report_2013.pdf.
[15] CNNIC, "*Zhong Guo Hu Lian Wang Fa Zhan Zhuang Kuang Tong*," [The 31st Report on the Development of the Internet in China], January 2013, 15 http://www.cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/201301/P020130122600399530412.pdf.
[16] CNNIC, [The 31st Report on the Development of the Internet in China].
[17] ITU, *The World in 2011: ICT Facts and Figures* (Geneva: ITU, 2011), http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf.

Graph A. Internet Penetration Rate in Provinces of Mainland China between 2011 and 2012 (Source: CNNIC)



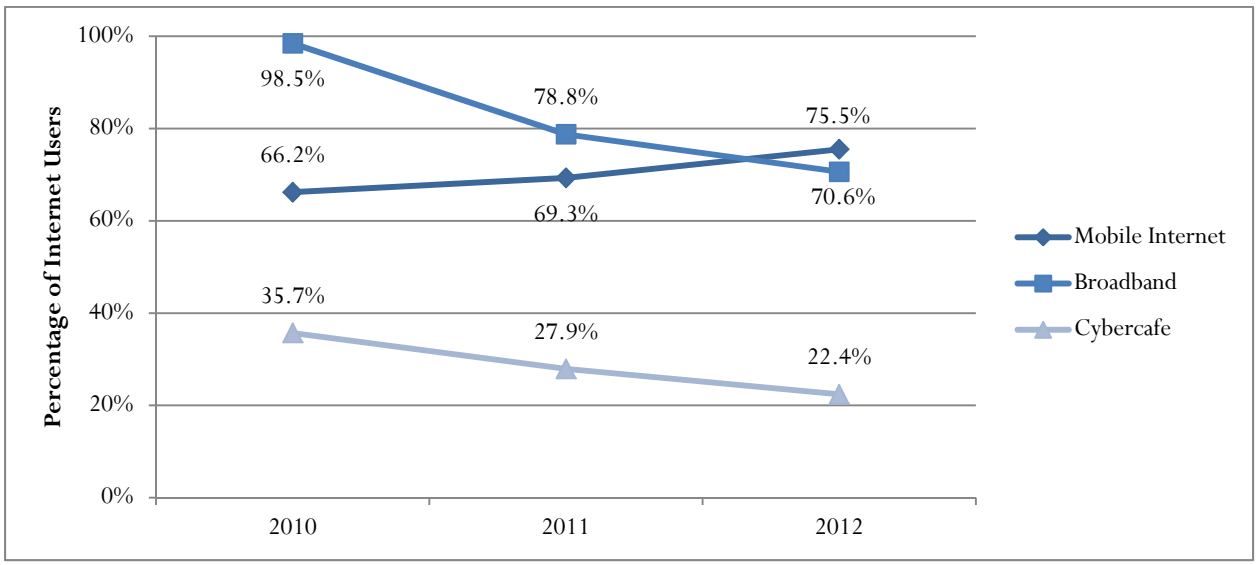
The CNNIC reported 422 million mobile internet users in December 2012. By contrast, broadband subscriptions declined from 450 million in 2010 to 380 million in 2012.[18] (Broadband subscriptions have dwarfed dial-up since 2005.[19])

Mobile replaced fixed-line broadband as China's preferred means of accessing the internet for the first time in 2012. Internet access via cybercafé declined, accounting for 22.4 percent of users, down from 27.9 percent in 2011.[20] While internet-enabled 3G (third-generation) phones are priced beyond the reach of many, platforms like the Tencent QQ instant-messaging service and Sina Weibo allow users to send and receive messages at low cost via 2G handsets.

Mobile replaced fixed-line broadband as China's preferred means of accessing the internet for the first time in 2012.

[18] 163.com web portal visualization of CNNIC, [The 31st Report on the Development of the Internet in China], http://tech.163.com/special/cnnic30/#full.
[19] "CNNIC Releases Internet Report: China's Internet Users Exceed 100 Million," *Xinhua News*, July 22, 2005, http://news.xinhuanet.com/newmedia/2005-07/22/content_3251081.htm.
[20] CNNIC, [The 31st Report on the Development of the Internet in China], 21.

Graph B. Percentage of Internet Users Getting Internet Access Through Mobile Phones, Broadband, and Cybercafés (Source: CNNIC)



The historically high cost of broadband internet access helps to account for the shift toward mobile. The government took steps to address this when a 2011 antimonopoly investigation accused the state-owned China Telecom and China Unicom of abusing their market dominance to manipulate broadband pricing and overcharge competitors. The investigation was the first instance in which a 2008 antimonopoly law was used against state-owned enterprises, and it was announced in an unusually public way on CCTV.[21] The telecom giants swiftly revised their internetwork pricing structures to allow rivals fair access to their infrastructural resources.[22] Interestingly, one of the beneficiaries of this measure may be a government regulator, the State Administration of Radio, Film, and Television (SARFT), which said in 2012 that it would launch a national cable network, funded by the Ministry of Finance and offering telephone, broadcasting, and internet services. The plan would advance the overall integration of these three services, a goal the State Council had previously pledged to achieve throughout China by 2015, though the timetable for its implementation is not clear.[23]

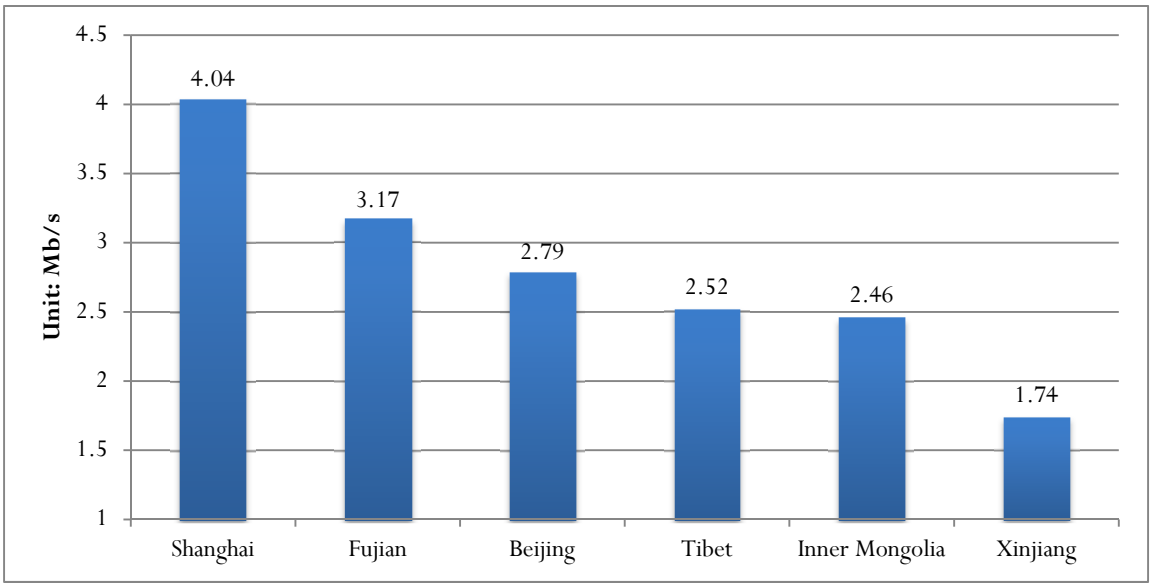
[21] Jan Holthuis, "War of the Giants – Observations on the Anti-Monopoly Investigation in China Telecom and China Unicom, HIL International Lawyers & Advisers, March 2, 2012, http://legalknowledgeportal.com/2012/03/02/war-of-the-giants-observations-on-the-anti-monopoly-investigation-into-china-telecom-and-china-unicom/..

[22] Lu Hui, "China Telecom, China Unicom Pledge to Mend Errors after Anti-monopoly Probe," *Xinhua News*, December 2, 2011, http://news.xinhuanet.com/english2010/china/2011-12/02/c_131285141.htm; "*Guo Jia Guang Dian Wang Luo Gong Si Jiang Qiang Cheng Li Zhong Yi Dong Wei Can Yu Chu Zi*" [State Radio and Television Networks Will be Set Up], *Sina*, November 15, 2012, http://tech.sina.com.cn/t/2012-11-15/03037799520.shtml..

[23] Tan Min, "SARFT Finishes Plan for National Cable Operator," *Caixin*, August 6, 2012, http://english.caixin.com/2012-08-06/100420145.html.

While customers can now choose from among scores of private internet service providers (ISPs), the large state enterprises are widely perceived as responsible for the costly, inefficient connections that continue to prevail.[24] The Beijing-based research company Data Centre of China Internet reported that the average cost of 1 Mbps of bandwidth was 469 times more on the mainland than in Hong Kong in 2011,[25] while consumers complained that broadband speeds remained slower than advertised in 2012.[26] The MIIT has sought other methods to improve internet service, such as mandating that homes constructed within reach of public fiber-optic networks be connected via a selection of service providers from April 2013 onward.[27] Whether China's infrastructure will be able to keep pace with such ambitious government projects, however, is still uncertain. Although the MIIT said all broadband users would have internet access at 100 Mbps by 2015, the average speed in the fastest city, Shanghai, was just 4.04 Mbps in 2012, compared with 2.52 Mbps in the less-developed—and more heavily censored—Tibetan Autonomous Region.[28]

Graph C. Average Broadband Connection Speed in 2012 Q4 (Source: ChinaCache)



[24] "Tighter Rules for Telecom Costs," *Shanghai Daily*, April 26, 2012, http://www.china.org.cn/business/2012-04/26/content_25241615.htm.

[25] "*Zhong Guo Kuandai Yong hu Diaocha*" [Survey of China's Broadband Users], Data Center of China Internet, 2011-2012, http://www.dcci.com.cn/media/download/905430773daab3f27453929ee140539fdc12.pdf. The center has not released data for 2012.

[26] "Chinese Internet Choked by "'Fake Broadband"' Providers," *Global Times*, October 8, 2012, http://www.globaltimes.cn/content/736926.shtml.

[27] Shen Jingting, "New Residences Required to Provide Fiber Network Connections," *China Daily*, January 9, 2013, http://usa.chinadaily.com.cn/business/2013-01/09/content_16099801.htm.

[28] "China's Broadband Speeds Show Shanghai Zooming Ahead [INFOGRAPHIC]," *Tech in Asia*, September 20, 2012, http://www.techinasia.com/china-broadband-speeds-2012-infographic/; "China Internet Report: The First Quarter of 2013," ChinaCache, May 2013, http://files.shareholder.com/downloads/ABEA-528MQE/2583814687x0x664689/2c293e5c-de24-4102-b7bd-828c0501bd94/ChinaCache_First_Quarter_2013_China_Internet_Report.pdf.

Mobile phone communication is also dominated by state-owned enterprises, including China Mobile, China Telecom, and China Unicom. This situation, too, is under review: The MIIT issued draft proposals to open the market in January 2013, allowing private companies to buy mobile network resources and repackage them for the user over a two-year trial period.[29] China Mobile began testing faster 4G service in some eastern Chinese cities in 2013, and the MIIT said in late 2012 that it would be issuing licenses to providers to upgrade to 4G service within a year.[30]

The government has been willing to liberalize the telecommunications market in part because of the country's centralized connection to the international internet. Six state-run operators maintain the country's international gateways.[31] This arrangement remains the primary infrastructural limitation on open internet access, as it gives the authorities the ability to cut off cross-border information requests. All ISPs must subscribe via the gateway operators and obtain a license from the MIIT. Internet access via mobile phones is also monitored by the international gateway operators under MIIT oversight.

The government has shut down access to entire communications systems in response to specific events, notably imposing an astounding 10-month internet blackout in the Xinjiang Uighur Autonomous Region after an outburst of ethnic violence in the regional capital Urumqi in July 2009.[32] Since then, authorities have enforced smaller-scale shutdowns lasting several days or weeks. Officials in predominantly Tibetan areas of western China twice cut off local internet access during 2012: once in February following clashes surrounding a series of self-immolations and reports that soldiers had opened fire on civilians,[33] and again for two days around the July 7 birthday of the Dalai Lama, Tibet's exiled spiritual leader.[34] More than 100 self-immolations—suicides committed in protest against Chinese rule—have been documented since 2009.[35]

[29] Seng Jingting, "Telecom Plans 'Will Help Break' Industry Monopoly," China Daily, January 1, 2013, http://www.chinadaily.com.cn/bizchina/2013-01/09/content_16098031.htm.
[30] "China Mobile Launches TD-LTE Commercial Trials in Hangzhou, Wenzhou," Marbridge Daily, February 4, 2013, http://www.marbridgeconsulting.com/marbridgedaily/archive/article/63196/china_mobile_launches_td_lte_commercial_trials_in_hangzhou_wenzhou#When:12:00:00Z; Want China Times, "China Paves Way for 4G Telecom Network Expansion," November 28, 2012, http://www.wantchinatimes.com/news-subclass-cnt.aspx?id=20121128000040&cid=1502.
[31] CNNIC, [The 31st Report on the Development of the Internet in China], 21.
[32] Chris Hogg, "China Restores Xinjiang Internet," *British Broadcasting Corporation (BBC)*, May 14, 2010, http://news.bbc.co.uk/2/hi/asia-pacific/8682145.stm.
[33] Tania Branigan, "China Cut Off Internet in Area of Tibetan Unrest," *Guardian*, February 3, 2012, http://www.guardian.co.uk/world/2012/feb/03/china-internet-links-tibetan-unrest.
[34] "China Celebrates Dalai Lama's Birthday by Cutting Communications in Tibetan Region," Index on Censorship, July 10, 2012, http://www.ifex.org/china/tibet/2012/07/10/communications_cut/.
[35] "Self-Immolations by Tibetans," International Campaign for Tibet, June 19, 2013, http://www.savetibet.org/resources/fact-sheets/self-immolations-by-tibetans/.

In other cases, the level of official interference with connectivity was hard to gauge. China was briefly isolated for two hours in April 2012 when users reported that all international websites were inaccessible. Hong Kong and U.S. users were unable to visit sites hosted in China during the same period. Cloud Flare Inc., a U.S.-based company that studies web performance, told the *Wall Street Journal* that the interruption appeared to have been triggered by overactive filtering, rather than a technical glitch, and that only traffic from China Telecom and China Unicom plummeted; smaller providers were unaffected.[36] In August 2012, the same company reported "increased difficulty with traffic out of China," but without a consistent pattern to indicate the cause.[37] An MIIT spokesperson denied rumors that China was "closing down the internet" in advance of the politically sensitive 18th Party Congress in the fall, but acknowledged conducting maintenance.[38]

Authorities exercise tight control over cybercafés and other public access points, which are licensed by the Ministry of Culture in cooperation with other state entities.[39] Consolidating these helps increase the efficiency of surveillance and censorship.[40]

By 2012, chains had absorbed around 40 percent of cybercafés following a ministry-led push to eliminate sole-proprietor locations by 2015.

By 2012, chains had absorbed around 40 percent of cybercafés following a ministry-led push to eliminate sole-proprietor locations by 2015. Over 10 different government and CCP entities, at both the national and local levels, are involved in internet censorship, with some instructions coming straight from the top. The State Internet Information Office was created in 2011 to streamline propaganda directives for online content, punish violators, and oversee telecommunications companies.[41] It has since increased controls on online video—

[36] Paul Mozur, "New Clarity on China Internet Outage," *China Real Time Report* (blog), *Wall Street Journal*, April 13, 2012, http://blogs.wsj.com/chinarealtime/2012/04/13/new-clarity-on-china-internet-outage/.
[37] Tania Branigan, "China's Internet Users Temporarily Blocked from Foreign Websites," *Guardian*, April 12, 2012, http://www.guardian.co.uk/world/2012/apr/12/china-internet-users-foreign-websites.
[38] Brian Spegele and Paul Mozur, "China Hardens Grip before Meeting," *Wall Street Journal*, November 10, 2012, http://online.wsj.com/article/SB10001424052970204707104578092461228569642.html.
[39] These include the Public Security Bureau and the State Administration for Industry and Commerce. "Yi Kan Jiu Mingbai Quan Cheng Tu Jie Wang Ba Pai Zhao Shen Qing Liu Cheng" [A look at an illustration of the whole course of the cybercafé license application process], Zol.com, http://detail.zol.com.cn/picture_index_100/index997401.shtml.
[40] "China's 2013 Internet Café Market Down 13% YoY," 17173.com, April 28, 2013, http://www.marbridgeconsulting.com/marbridgedaily/2013-04-28/article/65634/chinas_2013_internet_caf_market_down_13_yoy.
[41] The State Internet Information Office operates under the jurisdiction of the State Council Information Office. "China Sets Up State Internet Information Office," *China Daily*, May 4, 2011, http://www.chinadaily.com.cn/china/2011-05/04/content_12440782.htm. See also "New Agency Created to Coordinate Internet Regulation," *China Media Bulletin*, May 5, 2011, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-21#3.

particularly short-form "microfilms" that are commonly used to evade controls on content screened by mainstream movie theaters or news media[42]—and real-name registration for online platforms.[43] Two official regulatory entities, SARFT and the General Administration for Press and Publications (GAPP), are slated to merge, according to a plan announced in March 2013.[44]

[42] Mathew Scott, "Censors Catch Up With China's 'Micro Film' Movement," *Agence France-Presse*, July 16, 2012, http://www.google.com/hostednews/afp/article/ALeqM5itjrPwXQFfB7ueKsg1TdiOtItR8w?docId=CNG.09667aa7e67669f6f7d1a284e78d6e1d.c1.

[43] See Congressional-Executive Commission on China (CECC), *Annual Report 2012* (Washington: CECC, 2012), 50–53, http://www.gpo.gov/fdsys/pkg/CHRG-112shrg76190/pdf/CHRG-112shrg76190.pdf.

[44] Alice Xin Liu, "China's Two Main Censorship Bodies to Merge," *Uncut* (blog), Index on Censorship, April 19, 2013, http://uncut.indexoncensorship.org/2013/04/sarft-gapp-china-censorship/.

LIMITS ON CONTENT

LIMITS ON CONTENT: AN OVERVIEW
MAY 2012–APRIL 2013

Censorship predictably intensified in advance of the leadership transitions at the November 2012 party congress and the March 2013 National People's Congress session. Reports of unrest, such as Tibetans self-immolating, were especially curtailed. The methods used were generally more precise and less visible than in the past, with the exception of a campaign against Bloomberg and the *New York Times* for their probing reports on wealth accumulation by China's first families. Instead of filtering out the individual articles, censors blocked the entire websites, depriving them of readership and advertising revenue.

Users in China can still access content hosted outside China using circumvention tools, at least until more companies follow China Unicom, which started severing connections on which circumvention was detected in December. Meanwhile, microblog users sometimes find that their posts have become invisible to others, requiring them to repost to keep their content in the public domain. These customized controls and manipulative practices are better understood thanks to some meticulous research and reporting published in 2012 and 2013.

In the past year, digital media also fueled popular participation in key debates over issues of public interest, such as smog levels in Beijing. But it is becoming harder to assess whether these movements represent a challenge to the censorship apparatus. They may be a sign that information authorities are more adept than ever at channeling outbreaks of discontent away from political issues and into local, finite, social matters.

In keeping with the unmatched size of their online population, Chinese authorities employ the most elaborate system for internet content control in the world. Government agencies and private companies employ thousands of people to monitor, censor, and manipulate content, from news reports to social-network pages. Routine censorship can be reinforced surrounding politically sensitive events, or just in response to the latest hot topic. Even this heavily censored and manipulated online environment, however, provides more space for

average citizens to express themselves and air their grievances against the state than any other medium in China.

Content with the potential to delegitimize CCP rule is systematically censored. Criticism of top leaders or policies, both present and past, is almost always controlled—a category that encompasses the legacy of Mao Zedong, the 1989 military crackdown on student-led protests in Beijing, and the Korean War. Independent evaluations of China's human rights record or CCP policies toward ethnic minorities and the banned Falun Gong spiritual group are also off-limits,[45] as are dissident initiatives that challenge the one-party regime. Names of established dissidents are frequently blocked, to prevent them gaining a wider following.

Content with the potential to delegitimize CCP rule is systematically censored.

These standing taboos are supplemented by evolving, almost daily directives on negative developments or budding civic movements over issues like environmental pollution, food safety, or police brutality. Analysts increasingly agree that content control is aimed at suppressing nascent collective action, rather than comprehensively banning critical speech.[46] Individuals with significant social capital or a high international profile, which would allow them to mobilize mass support, are more likely to be censored.[47] As a result, censors can be remarkably tolerant of frustration vented at local governments or discussion of politically oriented terms like "democracy."[48] The prevalence of this term and others, like "freedom of speech," has risen in the Chinese blogosphere.[49] While that marks some progress toward openness, it also corresponds to a shift in CCP discourse. Censors first relaxed filters on the word "democracy" in 2005 after leaders redefined democratic governance as "the Chinese Communist Party governing on behalf of the people."[50]

[45] A study conducted in 2011 by scholars at Carnegie Mellon found that up to 53 percent of microblog posts generated from Tibet were deleted. Byron Spice, "Carnegie Mellon Performs First Large-Scale Analysis of 'Soft' Censorship Media in China," Carnegie Mellon University, March 7, 2012, http://www.cmu.edu/news/stories/archives/2012/march/march7_censorshipinchina.html.

[46] "Preventing the organization of protests is as important, if not more important, than preventing users from reading unapproved content." Jedidiah R. Crandall et al., "ConceptDoppler: A Weather Tracker for Internet Censorship," Conference Paper for the 14th ACM Conference on Computer and Communications Security, October 29-November 2, 2007, http://www.csd.uoc.gr/~hy558/papers/conceptdoppler.pdf; King, Pan, and Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression."

[47] "Cyberdisappearance in Action," *China Media Bulletin*, July 14, 2011, http://www.freedomhouse.org/sites/default/files/inline_images/Cyberdisappearance%20in%20Action_special_feature-FINAL_0.pdf.

[48] King, Pan, and Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression."

[49] Ashley Esarey and Xiao Qiang, "Digital Communication and Political Change in China," *International Journal of Communication* 5 (2011), 298–319, http://ijoc.org/index.php/ijoc/article/view/688/525. Xiao Qiang was an advisor for this report.

[50] Richard McGregor, *The Party: The Secret World of China's Communist Rulers* (New York: Harper Collins, 2010), 20.

Chinese authorities are not transparent about censorship. International critics who question limits on content receive responses ranging from denial ("the Chinese internet is open"[51]) to defiance, manifest in the phrase "internet sovereignty," meaning the right to practice censorship within Chinese borders. Domestically, leaders cite the need to curb pornography, gambling, rumors, and other harmful practices to justify content restrictions, though political topics are targeted at least as forcefully. Ironically, while burgeoning internet access has not overcome information controls, it has shone a light on the processes involved. Chinese freelance journalist Shi Tao was sentenced to ten years in prison in 2005 for e-mailing propaganda department directives to an overseas news website;[52] today, similar directives are routinely leaked online. Internal copies of a 2010 speech outlining internet management were circulated in online forums, allowing users to compare them with the bowdlerized version circulated released to the public.[53] Criticism of the censorship system itself, however, is itself heavily censored. [54]

The CCP's content-control system consists of three primary techniques: **automated technical filtering**, **forced self-censorship** by service providers, and **proactive manipulation:**

> **Automated technical filtering** includes the best-known layer of the censorship apparatus: the blocking of foreign websites commonly referred to as China's "Great Firewall." The term implies a solid boundary, and in some cases, whole domain names or internet protocol (IP) addresses are blocked. "Web throttling," which slows the loading of pages to render services nearly useless, is employed as well. Internet users reported slowed broadband speeds and narrow bandwidth characteristic of web throttling during the month of the 2012 party congress.[55]
>
> More common, however, is the authorities' use of deep-packet inspection technologies to scrutinize traffic, both the user's request for content and the results returned, for an ever-evolving blacklist of keywords. If one is detected, the technology signals both sides of the exchange to temporarily sever the connection. This granular control renders censorship less noticeable to users, firstly because specific pages can be blocked within otherwise approved sites, and secondly because

[51] "Saying of the Week: China's Internet Is Open," *China Digital Times*, February 6, 2013, http://chinadigitaltimes.net/2013/02/saying-of-the-week-chinas-internet-is-open/.
[52] Bob Dietz, "As Wang Is Freed, Chinese Journalist Shi Tao Still Held," Committee to Protect Journalists, August 31, 2012, http://cpj.org/blog/2012/08/as-wang-is-freed-chinese-journalist-shi-tao-still.php.
[53] Human Rights in China, "How the Chinese Authorities View the Internet: Three Narratives," China Rights Reform Issue No. 2 (2010), http://www.hrichina.org/crf/article/3240.
[54] King, Pan, Roberts "How Censorship in China Allows Government Criticism but Silences Collective Expression."
[55] "In Tandem with Slower Economy, Chinese Internet Users Face Slower Internet This Week," *China Tech News*, November 6, 2012, http://www.chinatechnews.com/2012/11/06/18835-in-tandem-with-slower-economy-chinese-internet-users-face-slower-internet-this-week.

the interruption appears to come from the source of the information, not a third-party intrusion.[56]

Of course, some censorship is designed to remind users that certain content is out of bounds.[57] One study redefines the Great Firewall as a panopticon, arguing that it need not block everything if the knowledge of monitoring suffices to promote the self-censorship that is pervasive among Chinese internet users. Other research suggests that security forces are most secretive when they are also conducting surveillance to uncover who is accessing banned content—particularly if that data can subsequently be used to justify detention or some other violation of the user's rights.[58]

Filtering is heterogeneous and often inconsistent, depending on timing, technology, and geographical region. ISPs reportedly take different approaches to the placement of filtering devices, which are not only in border routers, but also in the backbone and even in provincial-level internal networks, a development that would potentially allow interprovincial filtering.[59]

Filtering is heterogeneous and often inconsistent, depending on timing, technology, and geographical region.

China Mobile, China Telecom, and China Unicom extend automated technical keyword filtering to the mobile realm, monitoring text messages and deleting pornographic or other "illegal" content.[60] Users report that their correspondents receive blank messages in place of subject matter that contained apparently banned keywords. It is not clear exactly what content triggers deletion.[61]

[56] Ben Wagner, "Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control,'" Global Voices Advocacy, June 25, 2009, http://advocacy.globalvoicesonline.org/2009/06/25/study-deep-packet-inspection-and-internet-censorship/.
[57] The animated cartoon police officers Jingjing and Chacha, who appeared on Chinese computer screens to wag fingers at wayward users around the country in 2008, served as visible reminders of official oversight.
[58] Villeneuve, *Breaching Trust*.
[59] X. Xu, Z. Mao, and J. Halderman, "Internet Censorship in China: Where Does the Filtering Occur?" *Passive and Active Measurement*, Springer, 2011, 133–142, http://pam2011.gatech.edu/papers/pam2011--Xu.pdf.
[60] "China Mobile Users Risk SMS Ban in Porn Crackdown," *Agence France-Presse*, January 13, 2010, http://www.google.com/hostednews/afp/article/ALeqM5jF6dl0QS_1q8Eub7W73BSRNwdJWQ; Elaine Chow, "So About that Sexting Ban in China," *Shanghaiist*, January 20, 2012, http://shanghaiist.com/2010/01/20/okay_so_that_sexting_ban_in_china.php.
[61] Elaine Chow, "An Alleged List of Banned SMS Terms from China Mobile and Co.," *Shanghaiist*, January 4, 2011, http://shanghaiist.com/2011/01/04/an_alleged_list_of_banned_sms_terms.php#photo-1.

The blanket blockage of select web applications isolates the Chinese public from an international network of user-generated content—and domestic internet firms from competition. The video-sharing platform YouTube and the social-media sites Facebook, Twitter, Google+, and Foursquare are consistently blocked. Like a number of other services, Twitter was initially available and widely used, then blocked in 2009 in advance of the 20th anniversary of the Tiananmen Square massacre, once its potential for galvanizing collective action became apparent. It remains popular among Chinese users who are familiar with circumvention tools.[62] More recent blocks on applications like Google's cloud storage service, Drive, were effected immediately.[63] Users of other international applications that remain unblocked complain of sporadic disruptions. Users of the online document-sharing service SlideShare, which is owned by the U.S.-based professional networking site LinkedIn, reported it was temporarily inaccessible in July 2012.[64] LinkedIn itself had been blocked for two days in February 2011.[65]

The blanket blockage of select web applications isolates the Chinese public from an international network of user-generated content—and domestic internet firms from competition.

Forced self-censorship by service providers, makes commercial success contingent on compliance with content regulations. International web applications, once blocked, are quickly replaced by homegrown equivalents. Hundreds of millions of users are attracted to these domestic video-sharing websites, social-networking tools, and e-mail services.[66] As part of their licensing requirements, the companies must ensure that banned content is not posted or circulated; those that fail risk temporary or permanent closure.[67] Software for both censorship and surveillance is

[62] Rebecca MacKinnon, "China Blocks Twitter, Flickr, Bing, Hotmail, Windows Live, etc. Ahead of Tiananmen 20th Anniversary," CircleID, June 2, 2009, http://www.circleid.com/posts/20090602_china_blocks_twitter_flickr_bing_hotmail_windows_live/

[63] Steven Musil, "Google Drive Crashes into China's Great Firewall," *Cnet*, April 25, 2012, http://news.cnet.com/8301-1023_3-57421540-93/google-drive-crashes-into-chinas-great-firewall/.

[64] "LinkedIn's SlideShare Blocked in China," *China Media Bulletin*, July 19, 2012, http://www.freedomhouse.org/cmb/65_071912#3.

[65] Keith B. Richburg, "Nervous Unrest, Chinese Authorities Block Web Site, Search Terms," *Washington Post,* February 25, 2011, http://www.washingtonpost.com/world/nervous-about-unrest-chinese-authorities-block-web-site-search-terms/2011/02/25/ABPdw5I_story.html.

[66] Rick Martin, "Ogilvy's 'Social Media Equivalents' in China 2011," *Tech in Asia*, October 17, 2011, http://www.penn-olson.com/2011/10/17/china-social-media/.

[67] One, Fanfou, lost market share after a 2009 shutdown lasted several months. Melanie Lee, "Clampdown Rumored as Chinese 'Twitter' Sites Blocked," *Globe and Mail*, August 23, 2012, http://m.theglobeandmail.com/technology/clampdown-rumored-as-chinese-twitter-sites-blocked/article1368400/?service=mobile.

often built into their applications. For example, instant-messaging services such as Tom-Skype and QQ include programming that downloads updated keyword blacklists regularly.[68]

In addition to automated keyword filters, human censors delete postings on blogs, microblogs, comment sections of news items, and bulletin-board system (BBS) discussions before they appear to the public or shortly thereafter.[69] Experts say staff receive as many as three censorship directives per day by text message, instant message, phone call, or e-mail.[70] Local propaganda offices recruit volunteers to identify and report potentially undesirable content on social networks.[71]

Online news portals that operate without a press license are limited to reposting content that has already been approved by censors, rather than producing their own.[72] Propaganda directives to internet-based outlets often include specific instructions to amplify content from state media.[73] The search engine Baidu, which accounts for nearly 80 percent of China's search market,[74] similarly manipulates the results it offers based on government instructions, not only removing proscribed material, but also favoring state-approved information over content from nongovernmental or foreign sources. In July 2012, after internet users began circulating short documentary-style videos on social networks to avoid restrictions on news broadcasts and movies, regulators ordered online video service providers to

[68] TOM-Skype is a joint venture between Skype and Chinese wireless service TOM Online. Vernon Silver, "Cracking China's Skype Surveillance Software," Bloomberg, March 8, 2013, http://www.businessweek.com/articles/2013-03-08/skypes-been-hijacked-in-china-and-microsoft-is-o-dot-k-dot-with-it; Jedidah R. Crandall et al., "Chat Program Censorship and Surveillance in China: Tracking TOM-Skype and Sina UC," *First Monday* 18, no. 7 (2013), http://firstmonday.org/ojs/index.php/fm/article/view/4628/3727; Jeffrey Knockel, "TOM-Skype Research," http://cs.unm.edu/~jeffk/tom-skype/.

[69] King, Pan, and Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression."

[70] Xiao Qiang, "From 'Grass-Mud Horse' to 'Citizen': A New Generation Emerges through China's Social Media Space," Congressional-Executive Commission on China, November 17, 2011, http://www.cecc.gov/sites/chinacommission.house.gov/files/documents/hearings/2011/CECC%20Hearing%20Testimony%20-%20Xiao%20Qiang%20-%2011.17.11.pdf.

[71] "*Web 3.0 Yuan Nian De Zhong Guo Hu Lian Wang Hang Ye Zi Lv Shi Jian Yu Xi Kao*" [Self-Disciplined Practice and Thoughts of Chinesse Internet Industry in Web 3.0], *Wenming.cn*, April 2011, http://www.wenming.cn/xwcb_pd/yjpl/201104/t20110407_142975.shtml; "*Beijing Zhao Mu Wang Luo Jian Du Zhi Yuan Zhe*" [Beijing to Recruit Volunteers for Network Monitoring], *Beijing News*, May 26, 2012, .

[72] "Interim Provisions on the Administration of Internet Websites Engaged in News Posting Operations," November 1, 2000, excerpts available at http://www.cecc.gov/pages/virtualAcad/exp/explaws.php.

[73] Keith B. Richburg, "Chinese Editors, and a Web Site, Detail Censors' Hidden Hand," *Washington Post*, April 13, 2011, http://www.washingtonpost.com/world/chinese-editors-and-a-web-site-detail-censors-hidden-hand/2011/04/01/AFpMiRSD_story.html.

[74] Phil Berlowitz, "Baidu Revenue and Profit Growth Rate Slow in Fourth Quarter," *Reuters*, February 4, 2013, http://www.reuters.com/article/2013/02/04/us-baidu-results-idUSBRE91310020130204.

start deleting any items that failed adhere to "correct guidance," a euphemism for censorship orders.[75]

Microblogging services, offered by Sina, Tencent, Sohu, and other companies, saw an astonishing 300 percent growth during their peak development period from 2010 to 2011. With more than half of China's internet users registered for a microblog account by January 2013,[76] these fast-paced networks and their rambunctious user base pose a unique challenge to censors trying to rein in sensitive discussion. The CCP established party branches in the offices of four microblog providers in February 2012, according to news reports.[77] Company executives also benefit from political connections and patronage.[78]

Sina employs both automated and human monitors to manage Weibo content.

Sina Weibo, benefiting in part from the vacuum left by the 2009 ban on Twitter, had accumulated 400 million registered accounts by November 2012,[79] though only 46 million are active.[80] Unlike on Twitter, Weibo users can develop elaborate discussion threads in response to each post, all of which are lost if the original post is censored. The comment function can also be independently shut off to prevent isolated posts from gaining traction.[81]

Sina employs both automated and human monitors to manage Weibo content. Their methods include deleting individual posts or accounts, often with 24 hours of an

[75] "Regulators Announce New Restrictions on Online Video," *China Media Bulletin*, July 12, 2012, http://www.freedomhouse.org/cmb/64_071212#2.

[76] Not all accounts are active. "*Di 31 Ci Zhongguo Hulianwangluo Zhuangkuang Tongji Baogao*" [The 31st Statistical Report on China's Internet Development," China Internet Network Information Center, January 15, 2013, http://www.cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/201301/t20130115_38508.htm.

[77] Qiao Long, "CCP Proposes Cells for Microblogs," *Radio Free Asia*, February 7, 2012, http://www.rfa.org/english/news/china/microblogs-02072012175742.html.

[78] "Tech Company Leaders Join Legislative, Advisory Bodies," *China Media Bulletin*, March 7, 2013, http://www.freedomhouse.org/cmb/82_030713#3.

[79] Josh Ong, "China's Sina Weibo Passes 400m Users, Acknowledges Pressure from Rival Tencent's WeChat," *The Next Web*, November 16, 2012, http://thenextweb.com/asia/2012/11/16/sina-books-152-million-in-q3-revenue-as-it-faces-tough-competition-from-tencents-wechat/.

[80] Gady Epstein, "Small Beginnings: Microblogs are a Potentially Powerful Force for Changes, But They Have to Tread Carefully," Economist, April 6, 2010, http://www.economist.com/news/special-report/21574632-microblogs-are-potentially-powerful-force-change-they-have-tread.

[81] Gady Epstein, "The Great Firewall: The Art of Concealment," *The Economist*, April 6, 2013, http://www.economist.com/news/special-report/21574631-chinese-screening-online-material-abroad-becoming-ever-more-sophisticated/print.

offending post, but sometimes long after publication;[82] making published posts visible only to the account owner; and sending personal warnings.[83] In addition, researchers counted over 800 terms filtered from Weibo search results at various times, including "Cultural Revolution" and "propaganda department."[84] Activists and other users with large followings come under particular scrutiny.[85]

Despite these efforts, the company has frequently fallen afoul of propaganda authorities. When the CCP's purge of Chongqing party chief Bo Xilai in early 2012 prompted unconfirmed online reports of a failed coup, comment functions were temporarily disabled on both Sina and Tencent microblogs. State media reported that the companies were "punished for allowing rumors to spread."[86] Sina subsequently closed several accounts for alleged rumor-mongering.[87] It also launched new user guidelines and a points-based system that assigned demerits to users who published banned content, leading to warnings and eventual account closure, while rewarding those who engaged in unspecified "promotional activities."[88] The intervention may have taken a toll on the company's market share. Rival microblog service Tencent announced 540 million registered users—with 100 million active daily—at the end of 2012.[89]

Foreign service providers must agree to self-censor in return for access to the immense Chinese market, and most comply. In 2012, New Tang Dynasty

[82] Keith B. Richburg, "China's 'Weibo' Accounts Shuttered as Part of Internet Crackdown," *Washington Post*, January 3, 2013, http://www.washingtonpost.com/world/chinas-weibo-accounts-shuttered-as-part-of-internet-crackdown/2013/01/03/f9fd92c4-559a-11e2-89de-76c1c54b1418_story.html.

[83] Xiao, "From 'Grass-Mud Horse' to 'Citizen.'"

[84] Xiao, "From 'Grass-Mud Horse' to 'Citizen.'" See also Tao Zhu et al., "The Velocity of Censorship: High-Fidelity Detection of Microblog Post Deletions," Paper for 22nd USENIX Security Symposium in Washington D.C. in August 2013, http://arxiv.org/ftp/arxiv/papers/1303/1303.0597.pdf; King-wa Fu and Michael Chu, "Reality Check for the Chinese Microblog Space: A Random Approach," *PLoS ONE*, Volume 8(3), 2013, http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0058356#pone.0058356-China1.

[85] David Bandurski, "Brutality and Tragedy Unseen," China Media Project, February 1, 2012, http://cmp.hku.hk/2012/02/01/18380/;
David Bandurski, "Thank Goodness for Hong Kong," China Media Project, January 31, 2012, http://cmp.hku.hk/2012/01/31/18311/.

[86] "China's Major Microblogs Suspend Comment Function to 'Clean up Rumors,'" *Xinhua News*, March 31, 2012, http://english.peopledaily.com.cn/90882/7775525.html.

[87] "Boxun News Site Attacked Amid Bo Xilai Coverage," Committee to Protect Journalists, April 25, 2012, http://cpj.org/2012/04/boxun-news-site-attacked-amid-bo-xilai-coverage.php.

[88] Experts believe "promotional activities" involve reporting other users or promoting progovernment content. See, "China," OpenNet Initiative, August 9, 2012, https://opennet.net/blog/2012/05/sina-weibo-updates-user-contract-more-content-restrictions; "Sina Weibo Introduces 'User Contract,'" *Caijing*, May 9, 2012, http://english.caijing.com.cn/2012-05-09/111842544.html.

[89] "Tencent Microblog Registered User Base Hits 540 Mln," *Yangcheng Evening News*, January 21, 2013, available at http://www.marbridgeconsulting.com/marbridgedaily/archive/article/62820/tencent_microblog_registered_user_base_hits_540_mln#When:12:00:00Z.

Television—a Chinese-language, New York–based broadcaster established by Falun Gong practitioners—reported that U.S. technology giant Apple had removed applications created by the station from its online App Store in China in July, on the grounds that their content was "illegal in China."[90] In Chinese-language versions of Apple's voice-controlled artificial intelligence system Siri, the system reportedly declined to answer questions related to the Tiananmen Square massacre, such as a query about "June," and in one test it refused even to direct the user to Tiananmen Square.[91] China accounted for 20 percent of Apple's sales in the first quarter of 2012, and the country is its second-biggest market after the United States.[92]

International service providers that refuse to censor content face an uncertain future. In 2010, Google lost significant market share when it began redirecting mainland users to its uncensored Hong Kong–based search engine. The company explained that it had made the decision after suffering sustained attacks on its intellectual property by military-grade hackers traced to Chinese computers.[93] By doing so publicly, and drawing attention to the way the same hackers had targeted Gmail accounts used by journalists and human rights activists focused on China issues, it also increased transparency about censorship.[94] Google retained its Chinese license and continued its less politically sensitive operations, like the AdSense advertising service and the Android mobile operating system, largely unimpeded.[95] Yet its flagship search engine has foundered in comparison with domestic competitors. In 2012, it began notifying Chinese users on which keywords were likely to trigger connectivity problems.[96] By 2013, it had turned off this notification function, which some users reported was itself subject to censorship.[97] If private

International service providers that refuse to censor content face an uncertain future.

[90] "LinkedIn's SlideShare Blocked in China," *China Media Bulletin*, July 19, 2012, http://www.freedomhouse.org/cmb/65_071912#3.
[91] "Apple's Digital Assistant Flunks Test on Taboo Topics," *China Media Bulletin*, June 21, 2012, http://www.freedomhouse.org/cmb/61_062112.
[92] Bruce Einhorn, "Apple vs. Google: Starkly Different China Experiences," *Bloomberg Businessweek*, June 12, 2012, http://www.businessweek.com/articles/2012-06-12/apple-and-google-are-having-very-different-china-experiences.
[93] David Drummond, "A New Approach to China," Google blog, January 12, 2012, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.
[94] Alexandra Stevenson, "Google's China Market Share: Declining," *Beyondbrics* (blog), *Financial Times*, April 22, 2011, http://blogs.ft.com/beyond-brics/2011/04/22/googles-china-market-share-declining/#axzz2Kj0UxcN8.
[95] Loretta Chao, "Chinese Regulators Renew Key License for Google," *Wall Street Journal*, September 7, 2011, http://online.wsj.com/article/SB10001424053111904836104576556203077777200.html.
[96] Alan Eustace, "Better Search in Mainland China," *Inside Search* (blog), Google, May 31, 2012, http://insidesearch.blogspot.co.uk/2012/05/better-search-in-mainland-china.html.
[97] "Google Turns Off China Censorship Warning," *BBC*, January 7, 2013, http://www.bbc.co.uk/news/technology-20932072.

companies choose not to alert readers about blocked content, censorship decisions remain both arbitrary and opaque. There are no formal avenues for appeal.

Chinese companies expanding overseas may have difficulty serving users accustomed to fewer online controls. In 2012, users of Tencent's messaging program WeChat complained that the service was applying China's censorship rules in Singapore and Thailand.[98]

Chinese companies expanding overseas may have difficulty serving users accustomed to fewer online controls.

Proactive manipulation is the third primary method of content control in China, and Chinese authorities view cyberspace as a field for "ideological struggle."[99] Since 2005, propaganda units at all levels have trained and hired web commentators to post progovernment remarks and lead online discussions.[100] They also report users who have posted offending statements, target government critics with negative remarks, or deliberately muddy the facts of a particular incident, such as an account of police abuse.[101] Recent reports estimate the number of paid propaganda workers in the tens of hundreds of thousands.[102] These methods are not always effective. Many commenters are more concerned about filling their quota and impressing their bosses than mounting a convincing argument, and web users are wary of content manipulation. Companies also pay for positive comments to promote their products —known in public relations circles as astroturfing—which further erodes public trust in online content.[103]

Government employees also engage citizens in online discussions. In 2012, an official Sina report said 50,000 Weibo accounts were operated by government ministries and

[98] "China's Tencent Accused of Censoring App Users Abroad," *China Media Bulletin*, January 24, 2013, http://www.freedomhouse.org/cmb/78_012413#5.
[99] Oiwan Lam, "China: The Internet as an Ideology Battlefield," Global Voices Advocacy, January 6, 2010, http://advocacy.globalvoicesonline.org/2010/01/06/china-internet-as-an-ideology-battlefield/.
[100] David Bandurski, "Internet Spin for Stability Enforcers," China Media Project, May 25, 2010, http://cmp.hku.hk/2010/05/25/6112/.
[101] Propaganda workers are colloquially known as the 50 cent party, after the amount they are reportedly paid per post, though recent reports put the going rate as low as 10 cents, while some commentators may be salaried employees. See, Perry Link, "Censoring the News Before It Happens," *New York Review* (blog), *The New York Review of Books*, July 10, 2013, http://www.nybooks.com/blogs/nyrblog/2013/jul/10/censoring-news-before-happens-china/, and Rongbin Han, "Manufacturing Consent in Censored Cyberspace: State-Sponsored Online Commentators on Chinese Internet Forums," Paper for Annual Meeting of America Political Science Association, New Orleans, August 31-September 2, 2012, http://ssrn.com/abstract=2106461.
[102] Perry Link, "Censoring the News Before It Happens."
[103] Rongbin Han, , "Manufacturing Consent in Censored Cyberspace."

public officials.[104] Even Hu Jintao, who famously avoided unscripted encounters with the press during his presidency, engaged a cherry-picked audience of *People's Daily* readers in a live web chat in 2008.[105]

The past year also offered an intriguing glimpse of CCP officials apparently wielding censorship tools against their opponents within the party ahead of the leadership shuffle. In mid-2012, Baidu returned fleetingly open results related to the 1989 crackdown and other human rights abuses associated with former president Jiang Zemin and his supporters. Observers speculated that President Hu's rival CCP faction was relaxing controls to embarrass its adversaries.[106] Meanwhile, leftist websites that had been supportive of Bo and his neo-Maoist rhetoric were shut down after his ouster.[107]

Despite the technical filtering, enforced self-censorship, and manipulation, the internet is a primary source of news and forum for discussion, particularly among the younger generation. Chinese cyberspace is replete with online auctions, social networks, homemade music videos, a large virtual gaming population,[108] and spirited discussion of some social and political issues. Overtly political organizations, ethnic minorities, and persecuted religious groups remain underrepresented, though they have used the internet to disseminate banned content, and overseas media and human rights groups report sending e-mail to subscribers in China with news, instructions on circumvention technology, or copies of banned publications. Civil society organizations involved in charity, education, health care, and other social and cultural issues often have a vigorous online presence.

[104] "*Shou Fen Bu Wei Weibo Yun Ying Bao Gao Mian Shi Zhuan Jia Jian Yi Bu Yi Guo Du Mai Meng* ," [The First Microblog of Government Ministry is Published. Experts Advise That It Should Not Be Overused], *Xinhua News*, August 25, 2012, http://news.xinhuanet.com/politics/2012-08/25/c_112842885.htm.

[105] The chat was an example of top leaders' efforts to avoid unscripted interactions. While *People's Daily* readers already represent a self-selecting group likely to support the CCP, news reports said many of the chat's participants were paid. David Bandurski, "FEER: China's Guerrilla War for the Web," China Media Project, July 7, 2008, http://cmp.hku.hk/2008/07/07/1098/.

[106] "Users Report Fleeting Censorship Gaps on Taboo Topics," *China Media Bulletin* March 29, 2012, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-52#Users%20report.

[107] "Microblog Comments Suspended to Allow Rumor 'Cleansing,'" *China Media Bulletin*, April 12, 2012, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-53#2.

[108] China's online gaming culture is regulated by contradictory controls. Game consoles were banned in 2000, ostensibly for health reasons, but some 120 million Chinese players access online games via computers and mobile devices. Moreover, the CCP heavily subsidizes the production of games that promote ideological themes for propaganda purposes. Some 2013 reports said the Ministry of Culture was planning to lift the console ban. Malcom Moore, "China Embraces Online Gamers," *Telegraph*, January 20, 2013, http://www.telegraph.co.uk/news/worldnews/asia/china/9814114/China-embraces-online-gamers.html.

The word "netizen"—a direct translation of the Chinese wangmin, or citizen of the internet—conveys the legitimate sense of civic engagement associated with online exchanges. Microblogs have amplified these dynamics and generated a strong sense of empowerment among many Chinese users, censorship notwithstanding.[109] Whereas Chinese citizens traditionally trek to the seat of power to present their grievances, microblogs and other internet technologies offer a way to overcome the geographic, financial, and physical challenges of such petitioning. Moreover, despite the leadership's dread of collective action, officials frequently yield to public pressure. Weibo users forced the authorities to start addressing air pollution in 2013 by raising their concerns in multiple cities and provinces.[110] In January, the CCP dismissed leftist Central Compilation and Translation Bureau Director Yi Junqing after an ex-lover blogged about their affair, drawing widespread opprobrium, in what the *New York Times* characterized as the latest in a "spate of scandals appearing online."[111]

The word "netizen"—a direct translation of the Chinese wangmin, or citizen of the internet—conveys the legitimate sense of civic engagement associated with online exchanges.

Online protests against official wrongdoing have gained considerable momentum and media visibility in the microblog era. One county-level party chief allegedly removed his expensive watch before appearing in photographs with Premier Li Keqiang in April 2013, perhaps to avoid becoming the latest local cadre to be censured for luxury spending. Internet users caught the tan line on his wrist and quickly found earlier photos that showed him with what seemed to be a designer timepiece.[112] In 2012, the story of a journalist's suspension for exposing officials' luxury cigarette habit in the city of Wei'an, published on his personal microblog, drew more attention than his original report.[113] Also that year, Chinese netizens expressed outrage over a case of compulsory abortion after photographs were posted online.[114] Censors do intervene if these stories and campaigns gain too high a profile or implicate overall CCP governance. After a disastrous storm in Beijing in mid-2012, resident microblog users complained about official rescue efforts and expressed fury when the municipality solicited

[109] David Barboza, "Despite Restrictions, Microblogs Catch On in China," *New York Times*, May 15, 2011, http://www.nytimes.com/2011/05/16/business/global/16blogs.html.
[110] Epstein, "Small Beginnings."
[111] Madeline Earp, "Shallow Victory for China's Journalists, Protestors," Committee to Protect Journalists, July 5, 2012, http://cpj.org/blog/2012/07/shallow-victory-for-chinas-journalists-protesters.php.
[112] Laura Zhou, "Watch Imprint on Quake Official's Wrist Goes Viral on Internet," *South China Morning Post*, April 24, 2013, http://www.scmp.com/news/china/article/1221756/watch-imprint-quake-officials-wrist-goes-viral-internet.
[113] Earp, "Shallow Victory for China's Journalists, Protestors."
[114] "Forced Abortion Stirs Netizen Outcry, Husband Missing after Interview," *China Media Bulletin*, June 28, 2012, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-62#2.

donations for disaster relief. These comments were deleted in the tens of thousands, and flood-related search terms were blocked, despite an obvious threat to public safety.[115]

The transformative effect of online activism in China is undeniable, and yet the solutions that result from these high-pressure encounters typically fall short of systemic reform or democratic decision making. Consequently, they fail to ensure meaningful accountability.[116] After the Beijing floods, the city's mayor announced his resignation, but he was quickly promoted to Beijing party secretary.[117] One year earlier, a deadly high-speed train collision in Wenzhou was first reported by Weibo users who circulated real-time reports, calls for help, and photos.[118] But in 2012, censors obstructed news coverage of the anniversary, and a promised investigation into the cause of the disaster had yet to contact its victims.[119]

Mobilization can also have a negative impact. Online thugs terrorizing officials for alleged corruption may look like a positive development, until the same forces attack ordinary internet users over a perceived insult. Nationalism and xenophobia are prominent components of Chinese cyberspace, though censorship targeting rational dissent instead of inflammatory discourse arguably magnifies their impact. In September 2012, censorship directives were either withheld or ignored following anti-Japanese protests linked to China's territorial dispute with Japan over the uninhabited Diaoyu or Senkaku Islands in the East China Sea. Many commentators interpreted the lack of censorship as a tacit endorsement of the protests, which escalated and turned violent until censors reentered the fray with a modulated message that successfully curtailed news coverage and discussion.[120] But the rioters are as likely to have influenced policymakers as any of the other competing military

[115] "Beijing Flood Criticism Erupts Online amid Media Controls," *China Media Bulletin*, June 26, 2012, http://www.freedomhouse.org/cmb/66_072612#3.

[116] According to one study, censors stopped blocking names of villages whose residents were protesting as soon as traditional media reported on the provincial authorities' response, even though tensions had not yet fully died down and the effectiveness of the response had yet to be shown. In other words, reports on protests in the context of an ostensibly benevolent response from party officials are not perceived as a threat worthy of censorship. See, "Finish Study Analyzes Keyword Censorship during Mass Incidents," *China Media Bulletin* December 13, 2012, http://www.freedomhouse.org/cmb/77_121312#5.

[117] Gong Lei, "Beijing Gets New Party Chief," Xinhua, July 3, 2012, http://news.xinhuanet.com/english/china/2012-07/03/c_131692802.htm.

[118] Sharon LaFraniere, "China Finds More Bodies, and a Survivor, in Trains' Wreckage," *New York Times*, June 25, 2011, http://www.nytimes.com/2011/07/26/world/asia/26wreck.html; Michael Wines and Sharon LaFraniere, "Baring Facts of Train Crash, Blogs Erode China Censorship," *New York Times*, June 28, 2011, http://www.nytimes.com/2011/07/29/world/asia/29china.html; "Train Crash Cover-Up Fuels Public Outrage," *China Media Bulletin*, July 28, 2011, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-31#1.

[119] Madeline Earp, "Propaganda Officials Miss the Boat on 'China's Katrina,'" Committee to Protect Journalists, July 26, 2012, http://cpj.org/blog/2012/07/propaganda-officials-miss-the-boat-on-chinas-katri.php.

[120] William Wan, "Chinese Government Both Encourages and Reins in Anti-Japan Protests, Analysts Say," *Washington Post*, September 17, 2012, http://www.washingtonpost.com/world/chinese-government-both-encourages-and-reins-in-anti-japan-protests-analysts-say/2012/09/17/53144ff0-00d8-11e2-b260-32f4a8db9b7e_story.html.

and foreign affairs agendas during the crisis because of the domestic security implications if they were not contained, according to the Canberra-based scholar Geremie Barmé.[121]

As high-profile events like these draw more attention to China's pervasive information controls, censors find themselves pitted against not just political activists, but also ordinary citizens. It is common for users to counter censorship with humorous neologisms that substitute for banned keywords.[122] This forces censors to work overtime, temporarily filtering seemingly innocuous vocabulary like "river,"[123] "tomato,"[124] or "porridge."[125] These overactive controls impinge further on daily life—jasmine flower sales, for instance, were affected when the word "jasmine" was blocked due to its association with Tunisia's 2011 democratic revolution[126]—and inspire further acts of creative online rebellion. This version of the Chinese internet does not resemble a repressed information environment so much as "a quasi-public space where the CCP's dominance is being constantly exposed, ridiculed, and criticized, often in the form of political satire, jokes, videos, songs, popular poetry, jingles, fiction, Sci-Fi, code words, mockery, and euphemisms."[127]

The number of internet users who challenge information controls to access political content—rather than to download pornography or pirated movies—appears to be growing.

The number of internet users who challenge information controls to access political content—rather than to download pornography or pirated movies—appears to be growing. Exact numbers of people actively combatting censorship are difficult to calculate. Internet expert Xiao Qiang put the activist community at two or three million in a mid-2013 estimate.[128] Others look for indicators like the number of Chinese users who continue to access Twitter, which can

[121] "The Chinese government […] was pushed into certain directions […] and saying, "If we go in such a direction, the masses will attack the Public Security Bureau, and the foreign affairs ministry and the army—we'll just go with the masses. And that's an extraordinary development."" "A Discussion with Geremie R. Barme," *Sinica Podcast*, March 8, 2013, http://popupchinese.com/lessons/sinica/a-discussion-with-geremie-r-barme.

[122] Brook Larmer, "Where an Internet Joke Is Not Just a Joke," *New York Times*, October 26, 2011, http://www.nytimes.com/2011/10/30/magazine/the-dangerous-politics-of-internet-humor-in-china.html.

[123] The surname of former Chinese leader Jiang Zemin means "river."

[124] The Chinese word for "tomato" is a homonym for the phrase "western red city," a reference to Chongqing and its purged party boss, Bo Xilai. Madeline Earp, "Chinese Censors Target Tomatoes amid Bo Xilai Scandal," Committee to Protect Journalists, July 5, 2012, http://cpj.org/blog/2012/04/chinese-censors-target-tomatoes-amid-bo-xilai-scan.php.

[125] "Porridge" evoked the *Southern Weekly* anticensorship protest by referring to a common southern Chinese delicacy.

[126] Andrew Jacobs, "Catching Scent of Revolution, China Moves to Snip Jasmine," *New York Times*, May 10, 2011, http://www.nytimes.com/2011/05/11/world/asia/11jasmine.html.

[127] Xiao, "From 'Grass-Mud Horse' to 'Citizen.'"

[128] Rebecca MacKinnon, "The Shawshank Prevention," *Foreign Policy*, May 2, 2012, http://www.foreignpolicy.com/articles/2012/05/02shawshank_prevention?page=full&wp_login_redirect=0.

only be reached via circumvention software since its 2009 ban. However, those counts vary wildly, from thousands to 35 million; experts have dismissed the latter as vastly inflated.[129]

The ad hoc techniques these users commonly adopt to flout censors include opening multiple blogs on different hosting sites and circulating banned information directly through peer-to-peer networks, which bypass central servers. Text transformed into image, audio, or video files evades keyword sensors. Software developers, both domestic and overseas, also offer technologically sophisticated tools like virtual private networks (VPNs), which direct the user's traffic—usually using an encrypted connection—through a server outside the firewall to circumvent technical filtering.

International news reports noted spikes in usage of these tools at politically important moments in early 2012—such as Bo Xilai's ouster—when heavy censorship was in place.[130] Circumvention tool developers independently corroborated this for Freedom House. Significantly, developers said the baseline number of users increased as first-time users who adopted the tools during a crisis continued to use them, even after it dissipated.[131]

The growth in the use of such tools has spawned attempts to block them. In 2011, internet security experts noticed activity indicating that Chinese ISPs may have been testing a new system for identifying the type of encrypted services often used by circumvention tools.[132] By December 2012, China Unicom was reportedly cutting connections when it detected VPN usage.[133] Even when not actively disrupted, encryption may attract surveillance. While dozens of China-based companies, as well as overseas firms, promote an evolving roster of commercial circumvention tools, not all are transparent about user privacy. In the words of internet freedom expert Rebecca Mackinnon, "most people are focused simply on accessing banned websites and aren't thinking about surveillance."[134] This leaves a growing community vulnerable to invasive rights violations.

[129] Jason Q. Ng, "There Are NOT Millions of Twitter Users in China: Supporting @ooof's Result and Refuting GWI's Conclusion," *Blocked on Weibo* (blog), January 6, 2013, http://blockedonweibo.tumblr.com/post/39828699303/there-are-not-millions-of-twitter-users-in-china; Jon Russell, "No, Facebook Does Not Have 63.5 Million Active Users in China," The Next Web, September 28, 2012, http://thenextweb.com/asia/2012/09/28/no-way-jose/.
[130] MacKinnon, "The Shawshank Prevention."
[131] E-mail communication with circumention tool developer who requested anonymity, June 2012.
[132] Sharon LaFraniere and David Barboza, "China Tightens Censorship of Electronic Communications," *New York Times*, March 21, 2011, http://www.nytimes.com/2011/03/22/world/asia/22china.html; Andy Greenberg, "China's Great Firewall Tests Mysterious Scans on Encrypted Connections," *Forbes*, November 17, 2011, http://www.forbes.com/sites/andygreenberg/2011/11/17/chinas-great-firewall-tests-mysterious-scans-on-encrypted-connections/.
[133] Charles Arthur, "China Tightens 'Great Firewall' Internet Control with New Technology," *Guardian*, December 14, 2012, http://www.guardian.co.uk/technology/2012/dec/14/china-tightens-great-firewall-internet-control.
[134] MacKinnon, "The Shawshank Prevention."

VIOLATIONS OF USER RIGHTS

VIOLATIONS OF USER RIGHTS: KEY FINDINGS
MAY 2012-APRIL 2013

A 2012 amendment to the Criminal Procedure Law took effect in January 2013. While not all its provisions were negative, the amendment did appear to strengthen the legal grounds for detaining suspects incommunicado if they were suspected of anti-state activity—a category that includes individuals like Cao Haibo, a cybercafé employee sentenced in a closed trial in November 2012 to eight years in jail for discussing democracy online. Other online activists faced physical attacks, interrogation and house arrest.

Many were deprived of due process: After 2013 unrest in Xinjiang, at least twenty individuals were sentenced because they "used the Internet, mobile phones and digital storage devices" to incite terrorism, local reports alleged, without elaborating. Also in 2013, as international concern at the rising number of self-immolations in Tibet mounted, the *Times* reported at least a dozen Tibetans detained for inciting and publicizing suicides, including sending photographs of burning bodies overseas via mobile phone. International monitoring groups documented unprecedented levels of surveillance targeting Tibetans, including searches of mobile devices. Police surveillance powers were bolstered by new rules encouraging users to register their real names online in December 2012. Some Beijing businesses offering internet were told to install government spyware or disconnect.

Several U.S-based media outlets revealed in January 2013 that Chinese hackers had infiltrated their computers and staff email accounts, while analysts traced several hackers operating globally to physical locations in China—in one case, to a specific military location in Shanghai—and revealed an escalation in their technical sophistication. Less well-documented is the exposure faced by Chinese web users. A Chinese military report in May 2012 said nearly 9 million Chinese computers were infected with malicious viruses, while international hackers claimed responsibility for illegally accessing China Telecom's vast stores of personal data.

Article 35 of the Chinese constitution guarantees freedoms of speech, assembly, association, and publication, but such rights are subordinated to the CCP's status as the ruling power. In addition, the constitution cannot, in most cases, be invoked in courts as a legal basis for asserting rights. The judiciary is not independent and closely follows party directives, particularly in politically sensitive freedom of expression cases. China lacks specific press or internet laws, but government agencies issue a variety of regulations to establish censorship guidelines. Regulations—which can be highly secretive—are subject to constant change and cannot be challenged by the courts.

Prosecutors exploit vague provisions in China's criminal code, laws governing printing and publications, and state secrets legislation to imprison citizens for online activity such as blogging, downloading censored material from overseas, or sharing information by text message, e-mail or social media platforms. Recent legislative amendments fall short of international standards for protecting defendants, and in some cases strengthen police power. In 2010, the National People's Congress amended the State Secrets Law,[135] obliging telecommunications operators and ISPs to cooperate with authorities investigating leaked state secrets or risk losing their licenses.[136] Since authorities can retroactively classify content to justify a prosecution under this law, its formalized extension to the digital realm is deeply problematic. An amendment to the Criminal Procedure Law that took effect in 2013 bolstered the legal grounds for detaining suspects in undisclosed locations in cases pertaining to national security—a category that includes online offenses against the state. It did introduce a review process for allowing police surveillance of suspects' electronic communications, which the Public Security Ministry allows in a range of criminal cases, but the wording of the amendment was vague about the procedure for that review.[137] In addition, local officials periodically use criminal defamation charges to detain and in some cases imprison whistle-blowers who post corruption allegations online.[138]

Trials and hearings lack due process, often amounting to little more than sentencing announcements, and detainees frequently report abuse in custody, including torture and lack of medical attention.[139]

[135] "*Zhong Hua Ren Min Gong He Guo Zhu Xi Ling, Di Er Shi Ba Hao*" [Presidential order of the People's Republic of China, No. 28," April 29, 2010, http://www.gov.cn/flfg/2010-04/30/content_1596420.htm.
[136] Jonathan Ansfield, "China Passes Tighter Information Law," *New York Times*, April 29, 2010, http://www.nytimes.com/2010/04/30/world/asia/30leaks.html.
[137] Luo Jieqi, "Cleaning Up China's Secret Police Sleuthing," *Caixin*, January 24, 2013, http://articles.marketwatch.com/2013-01-24/economy/36525447_1_police-abuse-police-investigations-police-officers.
[138] Justin Heifetz, "The 'Endless Narrative' of Criminal Defamation in China," Journalism and Media Studies Centre of the University of Hong Kong, May 10, 2011, http://coveringchina.org/2011/05/10/the-endless-narrative-of-criminal-defamation-in-china/.
[139] See for example, "Tortured, Dissident Christian Lawyer Talks about His Ordeal," *Asianews.it*, September 15, 2011, http://www.asianews.it/news-en/Tortured,-dissident-Christian-lawyer-talks-about-his-ordeal-22641.html;

Reporters Without Borders documented a total of 69 netizens in Chinese jails as of February 2013.[140] Individuals sentenced during the coverage period included Cao Haibo, a cybercafé employee who received eight years in jail 2012 for promoting democracy online.[141] Long-term detainees include 2010 Nobel Peace Prize winner Liu Xiaobo, who is serving an 11-year sentence on charges of "inciting subversion of state power" for publishing online articles, including the prodemocracy manifesto Charter 08.[142] Though these represent a tiny percentage of the overall user population, the harsh sentences have a chilling effect on the close-knit activist and blogging community and encourage self-censorship in the broader public.

Reporters Without Borders documented a total of 69 netizens in Chinese jails as of February 2013.

Members of religious and ethnic minorities face particularly harsh treatment for transmitting information abroad and accessing or disseminating banned content.[143] In the aftermath of ethnic violence in Tibet in 2008 and Xinjiang in 2009, local courts imposed prison sentences on at least 17 individuals involved in websites that reported on Tibetan or Uighur issues, often in closed trials.[144] Many details of the charges and sentences were not reported even to the defendants' families, but at least two Uighur website managers, Memetjan Abdulla and Gulmire Imin, were jailed for life. After more unrest in Xinjiang in 2013, at least 20 individuals were sentenced because they supposedly "used the Internet, mobile phones and digital storage devices to organize, lead and participate in terror organizations, provoke incidents, and incite separatism."[145] Also in 2013, as international concern at the rising number of self-immolations in Tibet mounted, the *New York Times* reported that at least a dozen Tibetans had been detained for allegedly inciting and publicizing the protests, including by sending photographs overseas via mobile phone.[146] A

Paul Mooney, "Silence of the Dissidents," *South China Morning Post*, July 4, 2011, http://pjmooney.com/en/Most_Recent_Articles/Entries/2011/7/4_Silence_of_The_Dissidents.html.

[140] "World Report: China," Reporters Without Borders, http://en.rsf.org/report-china,57.html. Unreported cases may put the total number of jailed internet users considerably higher.

[141] "China Internet Cafe Worker Cao Haibo Jailed," *BBC*, November 1, 2012 http://www.bbc.co.uk/news/world-asia-china-20172104 Cao's sentence was reported in November after a May trial.

[142] Sharon Hom, "Google and Internet Control in China: A Nexus between Human Rights and Trade?" (testimony, U.S. Congressional-Executive Commission on China, Washington, DC, March 24, 2010), http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg56161/pdf/CHRG-111hhrg56161.pdf .

[143] Falun Gong practitioners are often given harsh sentences for online communications, according to Patrick Poon, Executive Secretary and Director of Hong Kong Office of the Independent Chinese PEN Centre, who communicated with Freedom House by e-mail.

[144] "Attacks on the Press in 2011: China," Committee to Protect Journalists, http://www.cpj.org/2012/02/attacks-on-the-press-in-2011-china.php

[145] Chris Buckley, "China Convicts and Sentences 20 Accused of Militant Separatism in Restive Region," *New York Times*, March 27, 2013, http://www.nytimes.com/2013/03/28/world/asia/china-sentences-20-for-separatists-acts-in-restive-region.html.

[146] "Tibetans Held for Mobile-Phone Dalai Lama Images," *China Media Bulletin*, December 6, 2012, http://www.freedomhouse.org/cmb/76_120612#5.

Tibetan-language notice apparently posted by public security officials in Gansu Province warned that circulating banned content including "websites," "emails and audio files," and "SMS texts" would result in severe beating, according to Reporters Without Borders.[147]

Three other extrajudicial measures used to punish internet users are detention in "reeducation through labor" camps, house arrest, and covert detention.

- **Reeducation through labor**
  Public security officials can sentence suspects to up to four years in work camps without trial, an unpopular procedure that has drawn increasing calls for reform.[148] State media have become unusually vocal regarding the system's potential for abuse.[149] In November 2012, Chongqing village official Ren Jiayu, a 25-year-old who had been sentenced to two years' reeducation through labor for pseudonymous microblog comments about Bo Xilai, was released early after generating widespread online support; the event, and a CCTV interview with the former inmate, attracted over 1.5 million comments on Sina Weibo.[150] This minor success may reflect nothing more than the change in Bo Xilai's political fortunes. In early 2013, however, in a possible prelude to centralized reform, state media reported that provincial authorities in Yunnan and Guangdong were preparing to abolish reeducation through labor.[151] The official Xinhua news agency later backtracked, saying the media had "read too much" into these developments. The status of the reform effort remains unclear; some experts still view a major overhaul as unlikely.

- **House arrest**
  This features invasive surveillance at the detainee's home, where internet and mobile phone connections are often severed to prevent the individual from contacting supporters and journalists. This is apparently intended to reduce external interest in the detainee's welfare, though it can have the opposite effect. Liu Xia, who is married to Liu Xiaobo, has been isolated at home since his incarceration, but this has

[147] Reporters Without Borders, "Authorities Openly Threaten Those Who Circulate Information with 'Torture,'" news release, March 29, 2012, http://en.rsf.org/chine-authorities-openly-threaten-those-29-03-2012,42216.html.
[148] Dui Hua, "Reform of China's 'Re-Education Through Labor' System is Slow Work in Progress," *Dialogue* no. 36, August 29, 2009, http://duihua.org/wp/?p=2756.
[149] "Victims of Re-education Through Labor System Deserve Justice," *Xinhua News*, January 28, 2013, http://www.globaltimes.cn/content/758696.shtml.
[150] Oiwan Lam, "China: Campaign to End the Unconstitutional Re-Education Through Labour System," *Global Voices*, October 20, 2012, http://globalvoicesonline.org/2012/10/20/china-campaign-to-end-the-unconstitutional-re-education-through-labour-system/; Abby, "Spotlight on China's 'Re-Education Through Labor,'" *Global Voices*, November 28, 2012, http://globalvoicesonline.org/2012/11/28/spotlight-on-chinas-re-education-through-labour/.
[151] Cao Yin, "Yunnan Puts Laojiao Approvals on Hold," *China Daily*, February 7, 2013, http://usa.chinadaily.com.cn/china/2013-02/07/content_16210279.htm; Huang Jin and Chen Lidan, "Guangdong to Stop Re-education Through Labor System in China," *Xinhua News*, January 30, 2013, http://english.peopledaily.com.cn/90882/8113531.html.

generated repeated attempts to contact her, and Associated Press journalists evaded her surveillance detail to interview her in 2012.[152] While there are several cases of long-term house arrest, it can be adjusted arbitrarily over time. In September 2012, academic and blogger Jiao Guobiao was first banned from traveling to an overseas conference and placed under strict house arrest for several days, then arrested and detained for two weeks after publishing an online article about the disputed Diaoyu (Senkaku) Islands, and finally released, to continued surveillance.[153] Some groups compile tallies of dissidents known to be held under house arrest, but there are no statistics available to show which of them may have been targeted specifically for their online activity.[154]

- **Covert detention**
  State agents can abduct and hold individuals in secret locations without informing their families or legal counsel. This long-standing practice, which initially lacked a legal foundation, came into the spotlight in 2011 as authorities reacted to the threat of Arab Spring–style protests.[155] Among dozens of cases reported that year, prominent artist and blogger Ai Weiwei was abducted and held from April to June 2011 and subsequently fined for alleged tax evasion.[156] In 2012, as noted above, the National People's Congress enacted an amendment of the Criminal Procedure Law that strengthened the legal basis for detaining suspects considered a threat to national security in undisclosed locations, among other changes. In response to public feedback, a clause was added requiring police to inform a suspect's family of such a detention, though they need not disclose where and why the suspect is being held. Despite this improvement, the amendment maintained vague language that is open to abuse by police and security agents.[157]

[152] Isolda Morillo and Alexa Olesen, "China Nobel Wife Speaks on Detention," *Associated Press*, December 6, 2012, http://bigstory.ap.org/article/ap-exclusive-detained-china-nobel-wife-speaks-out. International news reports also follow well-known individuals like Tibetan blogger Tsering Woeser, who is periodically placed under house arrest, most recently in June 2013. See, "Tibetan Writer Woeser Again Placed under House Arrest," Radio Free Asia, June 20, 2013, http://www.rfa.org/english/news/tibet/arrest-06202013171541.html.

[153] PEN America, "Writer and ICPC Member Dr. Jiao Guobiao Released," news release, October 1, 2012, http://www.pen.org/rapid-action/2012/10/01/writer-and-icpc-member-dr-jiao-guobiao-released.

[154] "Deprivation of Liberty and Torture/Other Mistreatment of Human Rights Defenders in China," Chinese Human Rights Defenders (CHRD), June 30, 2013, http://chrdnet.com/wp-content/uploads/2013/03/FOR-WEB_Partial-data-6-30-2013-updt-7-5_VC-7-10-R-2.pdf.

[155] Edward Wong, "Human Rights Advocates Vanish as China Intensifies Crackdown," *New York Times*, March 11, 2011, http://www.nytimes.com/2011/03/12/world/asia/12china.html.

[156] Kate Taylor, "Arts Group Calls for Worldwide Sit-In for Ai Weiwei," *New York Times*, April 14, 2011, http://artsbeat.blogs.nytimes.com/2011/04/14/arts-group-calls-for-worldwide-sit-in-for-ai-weiwei/?scp=9&sq=&st=nyt; Wu Yu, "*Ai Wei Wei Bei Zhi 'Se Qing', Wang Min 'Ai Luo Luo*'" [Ai Weiwei was criticized for pornography, netizens fought back], *Deutsche Welle*, November 19, 2011, http://www.dw-world.de/dw/article/0,,15543929,00.html.

[157] The amendment took effect on January 1, 2013. Observers praised other aspects of the measure, including tentative steps toward increasing police accountability for surveillance "China's New Law Sanctions Covert Detentions," Committee to Protect Journalists, March 14, 2012, http://cpj.org/2012/03/chinas-new-law-sanctions-covert-detentions.php..

Internet users have occasionally fallen victim to forced psychiatric detention, a measure used to commit individuals to mental institutions and prevent them from seeking redress for injustice or engaging in other unwelcome behavior. The whereabouts of at least one detainee, Li Qidong, who officials hospitalized in Liaoning in 2009 after he criticized the government in online articles, are not known.[158]

Law enforcement officials frequently summon individuals for questioning in relation to online activity, an intimidation tactic referred to euphemistically online as "being invited for tea."[159] Activists have also been instructed to travel during times of political activity or heightened public awareness of their cause. Security agents sent photojournalist Li Yuanlong on a "forced vacation" from his native Guizhou Province in 2012, after he published shocking photographs of children who had died of exposure on a popular website, prompting calls for accountability from local schools and officials.[160]

Law enforcement officials frequently summon individuals for questioning in relation to online activity, an intimidation tactic referred to euphemistically online as "being invited for tea."

Internet users sporadically report encountering violence as a result of online activity. In August 2012, masked men raided the offices of a Hong Kong citizen-journalism platform and destroyed computers, apparently in retaliation for the site's coverage of local politics. Hu Jia, a dissident who is active online, reported that security agents beat him during an eight-hour detention in March 2013, on the day before Xi Jinping took office as president.[161]

[158] Chinese Human Rights Defenders (CHRD), *The Darkest Corners: Abuses of Involuntary Psychiatric Commitment in China* (CHRD, 2012), http://chrd.equalit.ie/wp-content/uploads/2012/08/CRPD_report_FINAL-edited2.pdf.
[159] Oiwan Lam, "China: Bloggers 'Forced to Drink Tea' with Police," Global Voices Advocacy, February 19, 2013, http://advocacy.globalvoicesonline.org/2013/02/19/china-bloggers-forced-to-drink-tea-with-police/; Michael Sheridan, "China Offers Its Dissidents Tea and Subtle Tyranny," *Sunday Times*, January 13, 2013, http://www.thesundaytimes.co.uk/sto/news/world_news/Asia/article1193304.ece.
[160] "Photojournalist 'Sent on Holiday' After Covering Death of Five Children," Reporters Without Borders, December 5, 2012, http://en.rsf.org/china-photojournalist-sent-on-holiday-05-12-2012,43764.html.
[161] Isaac Stone Fish, "Chinese Dissident Allegedly Beaten as Xi Jinping Becomes President," *Passport* (blog), *Foreign Policy*, March 14, 2013, http://blog.foreignpolicy.com/posts/2013/03/14/chinese_dissident_allegedly_beaten_as_xi_jinping_becomes_president.

Users hoping to avoid repercussions for their online activity face a rapidly dwindling space for anonymous communication as real-name registration requirements expand online, among mobile phone retailers, and at public internet facilities. The authorities justify real-name registration as a means to prevent cybercrime, though experts counter that uploaded identity documents are vulnerable to theft or misuse,[162] especially since some verification is done through a little-known government-linked contractor.[163]

Users hoping to avoid repercussions for their online activity face a rapidly dwindling space for anonymous communication as real-name registration requirements expand online, among mobile phone retailers, and at public internet facilities.

In December 2012, the CCP's governing Standing Committee approved new rules to strengthen the legal basis for real-name registration by websites and service providers.[164] The rules threatened violators with "confiscation of illegal gains, license revocations and website closures," largely echoing the informal arrangements already in place across the sector.[165] Comment sections of major news portals, bulletin boards, blog-hosting services, and e-mail providers already enforce some registration.[166] The MIIT also requires website owners and internet content providers to submit photo identification when they apply for a license, whether the website is personal or corporate.[167] Nevertheless, the new rules are significant in extending regulation to the e-commerce and business sectors, which typically benefit from more freedom than their counterparts in the news media, civil society, or academia. The rules oblige these providers

[162] Danny O'Brien, "China's Name Registration Will Only Aid Cybercriminals," Committee to Protect Journalists, December 28, 2012, http://www.cpj.org/internet/2012/12/chinas-name-registration-will-aid-not-hinder-cyber.php.

[163] "*Du Zi He Cha Wei Bo Shi Ming Guo Zheng Tong She Long Duan*" [Real-Name Verification of Weibo Suspected Monopolized by Guo Zheng Tong], *Hong Kong Commercial Daily*, December 30, 2011, http://www.hkcd.com.hk/content/2011-12/30/content_2875001.htm; "*Beijing Yao Qiu Wei Bo Yong Shi Ming Fa Yan*" [Beijing Users of Weibo Required for Real-Name Verification], BBC, December 16, 2011, http://www.bbc.co.uk/zhongwen/trad/chinese_news/2011/12/111216_beijing_weibo.shtml.

[164] "National People's Congress Standing Committee Decision Concerning Strengthening Network Information Protection," China Copyright and Media, December 28, 2012, http://chinacopyrightandmedia.wordpress.com/2012/12/28/national-peoples-congress-standing-committee-decision-concerning-strengthening-network-information-protection/.

[165] Joe McDonald, "China Real-Name Registration Is Now Law in Country," *Huffington Post*, December 28, 2012, http://www.huffingtonpost.com/2012/12/28/china-real-name-registration_n_2373808.html.

[166] "*Wen Hua Bu 2009 Jiang Da Li Zhen Zhi Hu Lian Wang Di Su Zhi Feng*" [Ministry of Culture Will Curb Trend of Internet Indecency in 2009], *Net Bar China*, January 6, 2009, http://www.netbarcn.net/Html/PolicyDynamic/010619543882 52.html; Chen Jung Wang, "*Shi Min Zhi Rang Gao Xiao BBS Bian Lian*" [Real Name System Intimidates High School BBS], CNHubei, November 29, 2009, http://www.cnhubei.com/200511/ca936578.htm; "*Zhong Guo Hu Lian Xie Hui: Bo Ke Tui Xing Shi Min Zhi Yi Chen Ding Ju*" [Internet Society of China: Real Name System for Bloggers is Set], *Xinhua News,* October 22, 2006, http://www.itlearner.com/article/3522.

[167] Elinor Mills, "China Seeks Identity of Web Site Operators," *CNET News*, February 23, 2010, http://news.cnet.com/8301-27080_3-10458420-245.html.

to gain consent for collecting personal electronic data, as well as outline the "use, method, and scope" of its collection; yet they offer no protection against law enforcement requests for these records.[168] Chinese providers are required to retain user information for 60 days, and provide it to the authorities upon request without judicial oversight or informing the user.[169]

Microblog providers have struggled to enforce identity checks. Online reports of Sina Weibo users trading defunct identification numbers to facilitate fake registration indicated that the requirements were easy to circumvent.[170] Sina's 2012 report to the U.S. Securities and Exchange Commission anxiously noted the company's exposure to potentially "severe punishment" by the Chinese government as a result of its failure to ensure user compliance.

When social-media sites offer online payment systems, many users voluntarily surrender personal details to enable financial transactions. Mobile phone purchases have required identification since 2010, so providing a phone number is a common way of registering with other services.[171] In fact, one analyst estimated that approximately 50 percent of microblog users had unwittingly exposed their identities to providers by 2012, simply by accessing the platform from their mobile phone.[172]

When social-media sites offer online payment systems, many users voluntarily surrender personal details to enable financial transactions.

Implementation of the real-name policy may continue to vary, not just because it is hard to enforce, but also because registration makes it harder for the state's hired commentators to operate undetected. One study reported that some officials openly encourage commentators to use pseudonyms and fake ID to hide their affiliation with the propaganda department.[173]

[168] Tim Stratford et al., "China Enacts New Data Privacy Legislation," Publication from Covington & Burling LLP, January 11, 2013, http://www.cov.com/files/Publication/83ff413a-af68-4675-850e-a0f54533d149/Presentation/PublicationAttachment/240e4b51-6450-4403-8cfe-b0cea77c8370/China_Enacts_New_Data_Privacy_Legislation.pdf.
[169] "China," OpenNet Initiative, August 9, 2012, http://opennet.net/research/profiles/china-including-hong-kong.
[170] C. Custer, "How to Post to Sina Weibo without Registering Your Real Name," *Tech in Asia*, March 30, 2012, http://www.techinasia.com/post-sina-weibo-registering-real/.
[171] "*Shou Ji Shi Ming Zhi Jin Qi Shi Shi, Gou Ka Xu Chi Shen Fen Zheng*" [Mobile phone real name system implemented today, SIM card purchasers have to present their ID documents], *News 163*, October 1, 2010, http://news.163.com/10/0901/00/6FF3HKF8000146BD.html.
[172] Song Yanwang, "*Jing Hua Wang Luo Huan Jing Xin Gui Yin Huan An Cang Weibo Shi Ming Zhi Ling Yung Ying Shang Mian Lin Da Kao*" [Internet Clean-Up Regulations Conceal Obscure Issues. Weibo's New Real-Name Registration Rule Poses Challenge for Telecom Operator], *Net.China.com.cn*, March 15, 2012, http://net.china.com.cn/txt/2012-03/15/content_4875947.htm.
[173] Rongbin Han, , "Manufacturing Consent in Censored Cyberspace."

Real-name registration is just one aspect of pervasive surveillance of internet and mobile phone communications in place in China.

Real-name registration is just one aspect of pervasive surveillance of internet and mobile phone communications in place in China. Rapidly developing phone technology offers new opportunities for the surveillance state. A 2011 Beijing city initiative to produce real-time traffic data by monitoring the location of the city's 17 million China Mobile subscribers sparked concern from privacy experts, who said it could be used to trace and punish activists.[174] The timeline for the program's implementation is not known.

The deep-packet inspection technology used to censor keywords can monitor users as they try to access or disseminate similar information. Private instant-messaging conversations and text messages have been cited in court documents. One academic study reported that queries for blacklisted keywords on Baidu automatically sent the user's IP address to a location in Shanghai affiliated with the Ministry of Public Security.[175] Given the secrecy surrounding such capabilities, however, they are difficult to verify.

Police periodically try to force mandatory surveillance software on organizations and individuals, with mixed success. Cybercafés check photo identification and record user activities, and in some regions, surveillance cameras in cybercafés have been reported transmitting images to the local police station.[176] However, users successfully resisted attempts at mandatory installation of antipornography software known as Green Dam Youth Escort in 2009, after experts voiced privacy and censorship concerns. Some Beijing companies were threatened with disconnection in 2012 if they failed to install government-designated software capable of logging web traffic, blocking sites, and communicating with local police servers.[177] A similar effort to force businesses offering wireless internet access in

[174] "*Beijing Ni Yong Shou Ji Xin Hao Zhui Zong Shi Min Chu Xing Qing Kuang*" [Beijing plans to track mobile phone users in real-time], *Yahoo News*, March 3, 2011, http://news.cn.yahoo.com/ypen/20110303/237829.html; Cecilia Kang, "China Plans to Track Cellphone Users, Sparking Human Rights Concerns," *Washington Post*, March 3, 2011, http://voices.washingtonpost.com/posttech/2011/03/china_said_it_may_begin.html.

[175] Becker Polverini and William M. Pottenger, "Using Clustering to Detect Chinese Censorware," Eleventh Annual Workshop on Cyber Security and Information Intelligence Research, Article No. 30, 2011. Extended Abstract available at: http://www.intuidex.com/whitepapers/CSIIRW_Chinese_Censorship_Paper.pdf.

[176] Naomi Klein, "China's All-Seeing Eye," NaomiKlein.org, May 14, 2008, http://www.naomiklein.org/articles/2008/05/chinas-all-seeing-eye.

[177] Kevin Voigt, "International Firms Caught in China's Security Web," *CNN*, August 24, 2012, http://edition.cnn.com/2012/08/24/business/china-foreign-companies-internet/index.html.

Beijing's Dongcheng district to purchase expensive surveillance equipment in 2011 caused some to disconnect rather than pay.[178] Others ignored the directive without repercussions.

As with censorship, surveillance disproportionately targets individuals and groups perceived as antigovernment. Reports citing anonymous government officials noted that a camera grid system known as "Skynet" may have "a camera on every road in Tibet" as part of the effort to contain self-immolations.[179] A Tibetan rights group reported police inspections of mobile phones for banned content in Lhasa in March 2013.[180] A June 2013 report by Human Rights Watch put these activities in the context of a three-year campaign by 5,000 teams of CCP personnel conducting surveillance throughout the Tibetan Autonomous Region.[181]

Beyond regional flashpoints, the national "Safe Cities" program offers security officials an advanced system for monitoring public spaces across China.[182] The "social stability maintenance" budget that supports these programs surpassed China's defense budget in 2012.[183]

Both international and local firms jockey for lucrative surveillance-related equipment contracts in China. During 2011, two lawsuits were filed in U.S. courts against the American technology company Cisco Systems, asserting that there was evidence the firm had customized its surveillance equipment to assist Chinese security agencies in apprehending Falun Gong practitioners and democracy activists. Cisco denied the allegations, and the cases were pending as of May 2013.[184] Uniview Technologies, a Chinese

[178] Zhao Zhuo, "*Beijing Bu Fen Ka Fei Ting Ting Zhi Ti Gong Wu Xian Wang Luo*" [Some cafés in Beijing suspend Wi-Fi service], *Beijing Youth Daily*, July 27, 2011, http://bjyouth.ynet.com/article.jsp?oid=79986791.

[179] Malcolm Moore, "China Using Massive Surveillance Grid to Stop Tibetan Self-Immolation," *Telegraph*, November 9, 2012, http://www.telegraph.co.uk/news/worldnews/asia/china/9667701/China-using-massive-surveillance-grid-to-stop-Tibetan-self-immolation.html.

[180] "China Launches Crackdown on Personal Cellphones in Lhasa," Tibetan Centre for Human Rights and Democracy, March 11, 2013, http://www.tchrd.org/2013/03/china-launches-crackdown-on-personal-cellphones-in-lhasa/#more-1288. Radio Free Asia also reported police requisitioning computers and cellphones belonging to Uighur students for inspection when they returned to the region for the school holidays. "Chinese Controls on Uyghur Students Ahead of Ramadan," Radio Free Asia, June 13, 2013, http://www.rfa.org/english/news/china/students-06132013105142.html.

[181] According to Human Rights Watch, the goals of the campaign included "categorizing Tibetans according to their religious and political thinking, and establishing institutions to monitor their behavior and opinions." Human Rights Watch, "China: 'Benefit the Masses' Campaign Surveilling Tibetans," news release, June 19, 2013, http://www.hrw.org/news/2013/06/18/china-benefit-masses-campaign-surveilling-tibetans.

[182] Andrew Jacobs and Penn Bullock, "Firm Romney Founded Is Tied to Chinese Surveillance," *New York Times*, March 15, 2012, http://www.nytimes.com/2012/03/16/world/asia/bain-capital-tied-to-surveillance-push-in-china.html.

[183] Edward Wong and Jonathan Ansfield, "China's Communist Elders Take Backroom Intrigue Beachside," *New York Times*, July 21, 2012, http://www.nytimes.com/2012/07/22/world/asia/chinas-communist-elders-take-backroom-intrigue-beachside.html.

[184] Somini Sengupta, "Group Says It Has New Evidence of Cisco's Misdeeds in China," *New York Times*, September 2, 2011, http://www.nytimes.com/2011/09/03/technology/group-says-it-has-new-evidence-of-ciscos-misdeeds-in-china.html; "Suit Claims Cisco Helped China Repress Religious Group," *Thomson Reuters News & Insight*, May 20, 2011, http://newsandinsight.thomsonreuters.com/Legal/News/2011/05_-

firm that offers software allowing police to share images between jurisdictions in real time, is owned by the U.S. private equity company Bain Capital.[185]

China is a key global source of cyberattacks, responsible for nearly a third of attack traffic observed by the content delivery network Akamai in a 2012 worldwide survey.[186] The survey traced the attacks to computers in China using IP addresses, meaning the machines themselves may have been controlled from somewhere else. In January 2013, following the precedent set by Google's revelation of hacking in 2010, the *New York Times* announced that Chinese hackers had infiltrated its computer systems and obtained staff passwords in the wake of the paper's censored exposé on wealth amassed by then premier Wen Jiabao's family.[187] The revelation prompted similar reports of hacking from Bloomberg, the *Wall Street Journal*, and the *Washington Post*.[188]

The scale and targets of illegal cyber activity lead many experts to believe that Chinese military and intelligence agencies either sponsor or condone it, though even attacks found to have originated in China can rarely be traced directly to the state. However, the geographically diverse array of political, economic, and military targets that suffer attacks reveal a pattern in which the hackers consistently align themselves with Chinese national goals. In one 2012 example, the *Indian Express* reported that hackers based in China had

The scale and targets of illegal cyber activity lead many experts to believe that Chinese military and intelligence agencies either sponsor or condone it, though even attacks found to have originated in China can rarely be traced directly to the state.

May/Suit_claims_Cisco_helped_China_repress_religious_group/; Don Tennant, "Second Lawsuit Accuses Cisco of Enabling China to Oppress Citizens," *IT Business Edge*, June 9, 2011, http://www.itbusinessedge.com/cm/blogs/tennant/second-lawsuit-accuses-cisco-of-enabling-china-to-oppress-citizens/?cs=47334; Mark Chandler, "Cisco Supports Freedom of Expression, an Open Internet and Human Rights," *The Platform* (blog), Cisco, June 6, 2011, http://blogs.cisco.com/news/cisco-supports-freedom-of-expression-an-open-internet-and-human-rights/.

[185] Jacobs and Bullock, "Firm Romney Founded Is Tied to Chinese Surveillance."

[186] Akamai, 3rd Quarter 2012 Executive Summary.

[187] Nicole Perlroth, "Hackers in China Attacked the Times for Last 4 Months," *New York Times*, January 30, 2013, http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html.

[188] Samuel Wade, "New York Times Hacking Highlights Other Cases," *China Digital Times*, February 1, 2013, http://chinadigitaltimes.net/2013/02/new-york-times-hacking-highlights-other-cases/; Nicole Perlroth, "Washington Post Joins List of News Media Hacked by the Chinese," *New York Times*, February 1, 2013, http://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html.

targeted computer systems of India's Eastern Naval Command headquarters in Visakhapatnam.[189] The most convincing documentation of a state connection was reported by U.S.-based cybersecurity firm Mandiant in February 2013, after the company traced sophisticated attacks on American intelligence targets to a military unit in Shanghai.[190]

Hackers, known in Chinese online circles as *heike* (dark guests), employ various methods to interrupt or intercept online content. Both domestic and overseas groups that report on China's human rights abuses have suffered from distributed denial-of-service (DDoS) attacks, which temporarily disable websites by bombarding host servers with an unmanageable volume of traffic. In a development that echoes the trajectory of China's overall information control, hackers increasingly intimidate service providers into cooperating with them. A massive DDoS attack on the exile-run Chinese-language news website Boxun in 2012 threatened the entire Colorado-based hosting company, name.com, and was accompanied by an e-mailed demand that the company disable Boxun for good.[191] Name.com resisted and helped Boxun switch servers, but hackers with the power to bring down whole businesses may well find other companies more compliant.

Another well-documented tactic is spear-phishing, in which targeted e-mail messages are used to trick recipients into downloading malicious software by clicking on a link or a seemingly legitimate attachment.[192] In a 2012 analysis, the U.S.-based computer security firm Symantec linked the group responsible for the 2010 Google breach—dubbed "the Elderwood gang" after a signature coding parameter—to a series of "watering hole" attacks, in which the hackers lay in wait for a self-selecting group of visitors to specific websites. The targeted sites included defense companies as well as human rights groups focused on China and Tibet; one of the sites was Amnesty International Hong Kong.[193] Most concerning, according to Symantec, were the gang's frequent "zero day" attacks, which exploit previously unknown vulnerabilities in the source code of programs that are widely distributed by software giants like Adobe and Microsoft. Groups that can pull off these attacks are scarce, since uncovering security loopholes requires huge manpower and

[189] Manu Pubby, "China Hackers Enter Navy Computers, Plant Bug to Extract Sensitive Data," *Indian Express*, July 1, 2012, http://www.indianexpress.com/news/china-hackers-enter-navy-computers-plant-bug-to-extract-sensitive-data/968897/.
[190] David E. Sanger, David Barboza, and Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking against U.S.," *New York Times*, February 18, 2013, http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html.
[191] "Boxun News Site Attacked Amid Bo Xilai Coverage," Committee to Protect Journalists, April 25, 2012, http://www.cpj.org/2012/04/boxun-news-site-attacked-amid-bo-xilai-coverage.php.
[192] Dennis Fisher, "Apple Phishing Scams on the Rise," *Threat Post*, June 24, 2013, http://threatpost.com/en_us/blogs/new-trojan-mac-used-attacks-tibetan-ngos-032112.
[193] Kim Zetter, "Sleuths Trace New Zero-Day Attacks to Hackers Who Hit Google," *Wired*, September 7, 2012, http://www.wired.com/threatlevel/2012/09/google-hacker-gang-returns/; "The Elderwood Project," *Symantec* (blog), September 6, 2012, http://www.symantec.com/connect/blogs/elderwood-project.

technical capability, or internal corporate access to the source code itself. Yet the Elderwood gang "seemingly has an unlimited supply" of zero-day vulnerabilities at its fingertips.

Chinese web users have also been victims of cybercrime perpetrated by hackers both inside and outside the country.

Chinese web users have also been victims of cybercrime perpetrated by hackers both inside and outside the country. Tibetans, Uighurs and other individuals and groups subject to monitoring have been frequently targeted with e-mailed programs that install spyware on the user's device.[194] Other attacks affect the broader population. In 2012, a military source reported that 8.9 million computers in China were infected with Trojan-horse viruses controlled from overseas IP addresses.[195] The hacker group SwaggSec announced in 2012 that it had broken into the database of the state-owned China Telecom, and that the company neglected to make a public statement or change its passwords. China Telecom subsequently confirmed the attack, but said any stolen data had "little value." However, a Chinese internet security expert acknowledged that China's internet was vulnerable, as many business owners and government officials lack the skills and awareness needed to defend themselves against cyberattacks.[196]

[194] Dylan Neild, Morgan Marquis-Boire, and Nart Villeneuve, "Permission to Spy: An Analysis of Android Malware Targeting Tibetans," Citizen Lab, April 2013, https://citizenlab.org/wp-content/uploads/2013/04/16-2013-permissiontospy.pdf.
[195] Jia Lei and Cui Meng, "*Ma Xiao Tian Yu E 'Wnag Luo Jun Bei Jing Sai*" [Ma Xiaotian Appeals for Suppressing 'Cyber Armament Race'], *Takungpao*, May 29, 2012, http://www.takungpao.com.hk/news/12/05/29/ZM-1484251.htm.
[196] Steven Musil, "Hackers Claim Breach of China Telecom, Warner Bros. Networks," *Cnet*, June 3, 2012, http://news.cnet.com/8301-1009_3-57446348-83/hackers-claim-breach-of-china-telecom-warner-bros-networks/.

CONCLUSION

Authoritarian regimes around the world look to Chinese methods of information control as a model, but activists can do the same. Anticipating what methods of censorship and control may be coming down the pipeline in China would be valuable for governments and internet users seeking to safeguard online freedoms against further encroachment. It is notoriously difficult to make accurate forecasts about China, but here are some technological developments worth watching:

- **Cross-platform censorship:** While online content has traditionally been separated from both telephony and radio and television broadcasting, experts say the three platforms are increasingly being brought under the same management and regulated by the same agencies. This could potentially streamline censorship and provide a more direct way of throttling dissent.
- **Interprovincial filtering:** At least one academic study has found evidence that internet censorship technology had been installed at the provincial level. Experts wonder whether this would enable officials to manipulate the information flowing between provinces—a more subtle and long-term alternative to total blackouts in areas of unrest.
- **Targeting circumventors by usage pattern:** Circumvention tools like VPN technology serve a broader commercial market in China, as well as users transmitting apolitical content like pirated movies. Rather than blocking the tools entirely, experts believe, censors are seeking to refine controls in order to block only circumventors with a specific usage pattern that indicates censorship evasion.

Ironically, this last example may provide some hope for online freedoms in China. So long as internet users defy censorship by creating content that current technology cannot trace or delete, propaganda agents and intermediary companies can adjust their methods in response. But if censors themselves are seeking to carve out exceptions, and grant privileges to pro-government or commercial groups, internet users benefit from what one study termed "collateral" freedom, "built on technologies and platforms that the regime finds economically or politically indispensable."[197] Collateral freedom is a poor substitute for full and free access to information and communication technologies. But the existence of such a phenomenon is proof that internet control runs counter to the public interest. By attempting to develop a partial, selective censorship apparatus, the CCP is acknowledging

[197] "Collateral Freedom: A Snapshot of Chinese Users Circumventing Censorship," *OpenITP*, May 21, 2013, http://openitp.org/pdfs/CollateralFreedom.pdfNews-Events/collateral-freedom-a-snapshot-of-chinese-users-circumventing-censorship.html.

that internet freedom is central to China's success as a modern nation—and keeping doors open that netizens will continue to exploit.

ABOUT FREEDOM HOUSE

Freedom House is an independent private organization supporting the expansion of freedom throughout the world.

Freedom is possible only in democratic political systems in which governments are accountable to their own people, the rule of law prevails, and freedoms of expression, association, and belief are guaranteed. Working directly with courageous men and women around the world to support nonviolent civic initiatives in societies where freedom is threatened, Freedom House functions as a catalyst for change through its unique mix of analysis, advocacy, and action.

- **Analysis:** Freedom House's rigorous research methodology has earned the organization a reputation as the leading source of information on the state of freedom around the globe. Since 1972, Freedom House has published *Freedom in the World*, an annual survey of political rights and civil liberties experienced in every country of the world. The survey is complemented by an annual review of press freedom, an analysis of transitions in the post-communist world, and other publications.
- **Advocacy:** Freedom House seeks to encourage American policymakers, as well as other government and international institutions, to adopt policies that advance human rights and democracy around the world. Freedom House has been instrumental in the founding of the worldwide Community of Democracies, has actively campaigned for a reformed Human Rights Council at the United Nations, and presses the Millennium Challenge Corporation to adhere to high standards of eligibility for recipient countries.
- **Action:** Through exchanges, grants, and technical assistance, Freedom House provides training and support to human rights defenders, civil society organizations, and members of the media in order to strengthen indigenous reform efforts in countries around the globe.

Founded in 1941 by Eleanor Roosevelt, Wendell Willkie, and other Americans concerned with mounting threats to peace and democracy, Freedom House has long been a vigorous proponent of democratic values and a steadfast opponent of dictatorships of the far left and the far right. The organization's diverse Board of Trustees is composed of a bipartisan mix of business and labor leaders, former senior government officials, scholars, and journalists who agree that the promotion of democracy and human rights abroad is vital to America's interests.

1301 Connecticut Avenue, NW, Washington, DC 20036
10025(202) 296-5101

120 Wall Street, New York, NY
(212) 514-8040

1301 Connecticut Avenue, NW, Washington, DC 20036
(202) 296-5101

120 Wall Street, New York, NY 10025
(212) 514-8040