FREEDOM
ON THE NET
2015

Freedom
House

China

	2014	2015
Internet Freedom Status	Not Free	Not Free
Obstacles to Access (0-25)	19	18
Limits on Content (0-35)	29	30
Violations of User Rights (0-40)	39	40
TOTAL* (0-100)	**87**	**88**

* 0=most free, 100=least free

Population:	1.36 billion
Internet Penetration 2014:	49 percent
Social Media/ICT Apps Blocked:	Yes
Political/Social Content Blocked:	Yes
Bloggers/ICT Users Arrested:	Yes
Press Freedom 2015 Status:	Not Free

Key Developments: June 2014 – May 2015

- In January 2015, Chinese authorities reported an upgrade to the national firewall that blocked several providers of virtual private networks in the name of "cyberspace sovereignty" (see **Blocking and Filtering**).

- The China Internet Network Information Center was found to be issuing false digital security certificates for a number of websites, including Google, exposing the sites' users to "man in the middle" attacks (see **Technical Attacks**).

- The government strengthened its real-name registration laws for blogs, instant-messaging services, discussion forums, and comment sections of websites (see **Surveillance, Privacy, and Anonymity**).

- In November 2014, the Chinese government introduced a draft counterterrorism law that would require all telecommunications companies and internet services to provide the government with "backdoor" access and copies of encryption keys (see **Surveillance, Privacy, and Anonymity**).

Introduction

The Chinese Communist Party (CCP) under general secretary and state president Xi Jinping continued to pursue "cyberspace sovereignty" as a top policy strategy during the coverage period of this report. The aim of establishing control was particularly evident in the government's attitude toward foreign internet companies, its undermining of digital security protocols, and its ongoing erosion of user rights, including through extralegal detentions and the imposition of prison sentences for online speech. China was the world's worst abuser of internet freedom in the 2015 *Freedom on the Net* survey.

The groundwork for this intensifying strategy of control was laid during the previous coverage period. In an internal speech at the National Propaganda and Ideology Work Conference in August 2013—first publicized by military and party commentators, and later revealed in full by *China Digital Times*[1]— Xi declared that "the internet has become the main battlefield for public opinion struggle." This represented considerably stronger rhetoric than that used by his predecessor, Hu Jintao, who had merely referred to "guidance" and "channeling" of public opinion online. The new terminology provided the ideological underpinning for the internet freedom decline that has continued since.[2] Lu Wei, head of the State Internet Information Office (SIIO), articulated his approach in concrete terms, proposing more licensing for online platforms, more real-name registration, more information-management training for government and private-sector agents, and tighter controls on undesirable content.[3] Lu Wei appears increasingly central to Xi's internet strategy, and was appointed in February 2014 to a panel on information technology and security policy that the president himself has chosen to lead, assuming a role usually played by the premier.[4] This high-level committee positioned internet development, governance, and security as high-priority issues for Xi's administration, along with national security and economic reform.[5]

Over the past year, the renewed emphasis on information control led to acts of unconcealed aggression against internet freedom. All of Google's content and communication services were fully blocked during the coverage period, marking an escalation in censorship from that experienced by the company's user base in mainland China in previous years. A government agency was found to be issuing false digital security certificates for a number of websites, including Google, leaving visitors to those sites vulnerable to attacks from hackers who replace webpages with unverified facsimiles in order to deliver malware or steal personal data. And the University of Toronto–based research group Citizen Lab documented massive cyberattacks on U.S. anticensorship websites that originated in the architecture of the Chinese government's own censorship apparatus, known as the Great Firewall—a previously undocumented capability that the group dubbed the Great Cannon.

As in past years, although pressure on overseas websites and companies increased, the real targets of repression were domestic internet users. Individuals imprisoned for legitimate online speech during the coverage period included renowned human rights lawyer Pu Zhiqiang, who was criminally

[1] "网传习近平8•19讲话全文：言论方面要敢抓敢管敢于亮剑,"*China Digital Times*, November 4, 2013, http://bit.ly/1weBugI.

[2] Qian Gang, "Parsing the 'public opinion struggle,'" China Media Project, September 24, 2013, http://cmp.hku.hk/2013/09/24/34085/.

[3] "State Internet Information Office Director Lu Wei outlines stronger focus on Internet governance," *China Copyright and Media* (blog), September 17, 2013, http://bit.ly/1LhwP0D.

[4] Cindy, "Xi Jinping to Head Reform Panel," *China Digital Times*, January 2, 2014, http://bit.ly/1LG51SO.

[5] Paul Mozur, "In China, Internet Czar Is Taking a Blunt Tone," *Bits* (blog), *New York Times*, October 31, 2014, http://nyti.ms/1GELosY; Shannon Tiezzi, "Xi Jinping Leads China's New Internet Security Group," *Diplomat*, February 28, 2014, http://bit.ly/1N9FBAn.

charged with inciting ethnic hatred and picking quarrels on social media, and 70-year-old journalist Gao Yu, who was jailed for seven years for supposedly leaking “state secrets” to an overseas website.

There were some examples of public activism, reflecting the vibrancy that is still common on the Chinese internet. An online petition in support of five feminists who were detained for distributing leaflets against sexual harassment on public transportation may have contributed to their release in April 2015.[6] And the environmental documentary *Under the Dome* was viewed by millions of people online before it was censored. But despite these efforts, and steady improvements in access year on year, internet control is intensifying.

Obstacles to Access

China boasts the world’s largest number of internet users, yet obstacles to access remain, including poor infrastructure, particularly in rural areas; a telecommunications industry dominated by state-owned enterprises; centralized control over international gateways; and sporadic, localized shutdowns of internet service to quell social unrest. Nationwide blocking, filtering, and monitoring systems delay or interrupt access to international websites.

Availability and Ease of Access

The authorities reported in January 2015 that there were 649 million internet users in China.[7] The average connection speed was comparatively slow at 3.8 Mbps.[8] Since 2011, internet adoption rates have slowed as the urban market approaches saturation, according to the China Internet Network Information Center (CNNIC), an administrative agency under the Ministry of Industry and Information Technology (MIIT).[9] Though the digital divide between urban and rural areas narrowed marginally in 2014, 72.5 percent of users were based in cities, and more were documented in Eastern China than in the less developed Central and Western regions combined.[10] Penetration rates vary by province, from Beijing (75 percent) to Jiangxi in the southeast (32 percent).[11] Overall internet penetration stood at 48 percent.[12] The CNNIC continued to report a gender gap among internet users, with males making up 56 percent of the total.

Mobile replaced fixed-line broadband (which had dwarfed dial-up since 2005[13]) as China’s preferred means of accessing the internet for the first time in 2012. From December 2013 to December 2014,

[6] Didi Kirsten Tatlow, “Supporters of Detained Feminists Petition for Their Release,” *Sinosphere* (blog), *New York Times*, April 1, 2015, http://nyti.ms/1K7FcKd.

[7] China Internet Network Information Center (CNNIC),中国互联网络发展状况统计报告 [The 35th Report on the Development of the Internet in China], January 2015, http://bit.ly/1MnNKyr.

[8] Akamai, *State of the Internet: Q3 2014 Report*, infographics, http://akamai.me/1LGi8U4; ChinaCache International Holdings Ltd, *China Internet Report*, 2013, http://bit.ly/1N9Jvt8.

[9] CNNIC, 中国互联网络发展状况统计报告 [The 28th Report on the Development of the Internet in China], July 2011, http://bit.ly/1GadOjH.

[10] Eastern China accounts for 41 percent of the population. CNNIC, 中国互联网络发展状况统计报告 [The 35th Report on the Development of the Internet in China], January 2015, http://bit.ly/1MnNKyr.

[11] CNNIC, 中国互联网络发展状况统计报告.

[12] CNNIC, 中国互联网络发展状况统计报告.

[13] “CNNIC Releases Internet Report: China’s Internet Users Exceed 100 Million” [in Mandarin], Xinhua, July 22, 2005, http://bit.ly/1R7Vicg.

the mobile internet population grew from 500 million to 557 million, accounting for 86 percent of all internet users.[14]

Authorities exercise tight control over cybercafes and other public access points, which are licensed by the Ministry of Culture in cooperation with other state entities.[15] By 2012, chain companies had absorbed around 40 percent of cybercafes.[16] Domestic news reports said more than 10,000 locations closed between 2011 and 2012, and cybercafes provided access for less than 20 percent of internet users in 2013.[17] In November 2014, the Chinese government reversed its policy and loosened restrictions on opening up cybercafes, lifting a 2013 requirement that they had to be run by chain stores, which had led to the proliferation of illegal establishments.[18] Though demand remained relatively high in rural areas and small towns, the number of internet users throughout China who were connecting through cybercafes and public computers remained relatively constant in 2014, at 18 percent.[19]

Costly, inefficient fixed-line broadband service has contributed to the shift toward mobile. 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.[20] The MIIT ordered that homes constructed within reach of public fiber-optic networks be connected via a selection of service providers from April 2013 onward.[21] A "Broadband China" government strategy issued in August 2013 aimed to boost penetration to 70 percent nationwide by 2020, raise third-generation (3G) mobile internet penetration to 85 percent, and increase connection speeds to 50 Mbps in cities and 12 Mbps in rural areas, with even faster Gbps speeds promised in bigger cities.[22] By the end of 2014, however, the average fixed-line broadband download speed across the country was still only 4.25 Mbps. The highest available rate was in Shanghai, which averaged 5.3 Mbps, while the lowest was in Tibet, which averaged 3.26 Mbps.[23]

Restrictions on Connectivity

Nine state-run operators maintain China's gateways to the global internet, giving authorities the ability to cut off cross-border information requests.[24] All service providers must subscribe via the gateway operators under MIIT oversight.

[14] CNNIC, 中国互联网络发展状况统计报告 [The 35th Report on the Development of the Internet in China], January 2015, http://bit.ly/1MnNKyr.

[15] 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 cybercafe license application process], Zol.com, http://bit.ly/1QmkImh.

[16] "China's 2012 Internet Café Market Down 13 percent YoY," 17173.com, April 28, 2013, http://bit.ly/1LhF78u.

[17] CNNIC, 中国互联网络发展状况统计报告 [The 31st Report on the Development of the Internet in China], 21, http://bit.ly/1K7cPM6.

[18] Many Zuo, "China eases restrictions on number of internet cafes but adds space requirements," *South China Morning Post*, November 24, 2014, http://bit.ly/1QmlcJf.

[19] CNNIC, 中国互联网络发展状况统计报告, [The 35th Report on the Development of the Internet in China].

[20] Data Center of China Internet, "*Zhong Guo Kuandai Yong hu Diaocha, 2011–2012*" [Survey of China's Broadband Users, 2011–2012], http://bit.ly/1jtteVC.

[21] Shen Jingting, "New residences required to provide fiber network connections," *China Daily*, January 9, 2013, http://bit.ly/1GaeW6R.

[22] Ministry of Industry and Information Technology, 国务院关于印发"宽带中国"战略及实施方案的通知, 2013, http://bit.ly/1RFIavO.

[23] Broadband and Development Alliance, *China's broadband speed status report* [in Mandarin], Section 6, http://bit.ly/1NbmZzX.

[24] CNNIC, 中国互联网络发展状况统计报告 [The 31st Report on the Development of the Internet in China], 21.

The government has shut down access to entire communications systems in response to specific events, notably imposing a 10-month internet blackout in the Xinjiang Uyghur Autonomous Region—home to 22 million people—after ethnic violence in the regional capital, Urumqi, in 2009.[25] Since then, authorities have enforced smaller-scale shutdowns, including one in September 2014 in Xinjiang's Yarkand (known in Chinese as Shache) County that began during the month of Ramadan and affected internet access and text-message services amid increasing tension between the Uyghur ethnic minority and the Chinese government.[26]

ICT Market

In 2011, an antimonopoly investigation accused state-owned China Telecom and China Unicom of abusing their market dominance to manipulate fixed-line broadband pricing, marking the first use of a 2008 antimonopoly law against state enterprises.[27] The telecom giants revised their inter-network pricing structures to allow rivals to access their infrastructure,[28] and customers can now choose from among 20 local, private internet service providers (ISPs),[29] but these only account for 10 percent of the market share.

State-owned China Mobile, China Telecom, and China Unicom dominate the mobile market, but other companies can provide telecommunications service by leasing network infrastructure. High prices have slowed 3G adoption in China, especially as some social-networking platforms allow users to exchange messages at low cost via 2G handsets, which accounted for 31 percent of mobile internet access in 2013, according to one report.[30] In May 2014, the government formally authorized the three major players to set pricing for services according to market forces, resulting in price cuts.[31] On February 27, 2015, the MIIT reported that it had issued licenses to China Telecom and China Unicom to operate 4G wireless networks.[32]

Regulatory Bodies

Several government and CCP agencies are responsible for internet censorship at the local and national levels, but the process has been consolidated under Xi Jinping. The SIIO was created in 2011 to streamline regulation of online content, punish violators, and oversee telecommunications

[25] See Alexa Olsen, "Welcome to the Uighur Web," *Foreign Policy*, April 21, 2014, http://atfp.co/1jmJCYH.

[26] Simon Denyer, "China's war on terror becomes all-out attack on Islam in Xinjiang," *Washington Post,* September 19, 2014, http://wapo.st/1jmJKY9.

[27] Jan Holthuis, "War of the Giants—Observations on the Anti-Monopoly Investigation in China Telecom and China Unicom," HIL International Lawyers & Advisers, Legal Knowledge Portal, March 2, 2012, http://bit.ly/1Mxc8SI; "Tighter Rules for Telecom Costs," *Shanghai Daily*, April 26, 2012, http://on.china.cn/1LJDfEV.

[28] Lu Hui, "China Telecom, China Unicom pledge to mend errors after anti-monopoly probe," Xinhua, December 2, 2011, http://bit.ly/1RFKEdz; "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://bit.ly/1GbT0bw.

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

[30] Joss Gillet and Mark Gilles, "Half a billion Chinese citizens have subscribed to the mobile internet," GSMA Intelligence, June 9, 2014, http://bit.ly/1OzT32b.

[31] Lan Xinzhen, "Full-Pricing Autonomy," *Beijing Review*, May 29, 2014, http://bit.ly/1G3MsMf; Paul Mozur and Lorraine Luk, "China to Liberalize Telecommunications Pricing," *Wall Street Journal*, May 9, 2014, http://on.wsj.com/1NFam3s. Prices were previously regulated by the government.

[32] Gerry Shih, "China issues 4G FDD licenses to China Telecom, China Unicom," Reuters, February 27, 2015, http://reut.rs/1NFav6Q.

companies.[33] Initially under the State Council Information Office, the agency was streamlined and rebranded during the coverage period of this report. On August 26, 2014, the State Council formally authorized the SIIO to regulate and supervise internet content.[34] In December 2014, it launched a new website under the English translation Cyberspace Administration of China (CAC),[35] and with a new organizational affiliation to the Office of the Central Leading Group for Cyberspace Affairs. That office, also known by the English name Central Internet Security and Informatization Leading Group, was formed in February 2014, directly under Xi, to oversee cybersecurity, making it highest authority on internet policy in China. In December 2014, the leading group took charge of the CNNIC, which issues digital certificates to websites.[36]

Two regulatory bodies, the State Administration of Radio, Film, and Television (SARFT) and the General Administration for Press and Publications (GAPP), both responsible for censorship in their respective sectors, merged in 2013 to form the State Administration of Press, Publications, Radio, Film, and Television (SAPPRFT).[37] The new regulatory body's tasks include monitoring internet-based television and online videos.

Limits on Content

The CCP propaganda department, government agencies, and private companies employ thousands of people to monitor, censor, and manipulate content. A range of issues are systematically censored, including independent evaluations of China's human rights record, critiques of government policy, and the authorities' treatment of ethnic minorities. Routine censorship is reinforced during politically sensitive events or in response to breaking news. However, even this heavily manipulated online environment provides more space for average citizens to express themselves or criticize the state than any other medium in China.

Blocking and Filtering

The Chinese government uses a sophisticated and ever-evolving censorship apparatus, incorporating both automated mechanisms and human monitors, to block and filter material that criticizes or challenges individuals, policies, or events considered integral to the one-party system. Politically sensitive events that drew censorship during the coverage period included the 25th anniversary of the Tiananmen Square crackdown and Hong Kong's prodemocracy "Occupy Central" protests, also known as the Umbrella Revolution.

Over the last several years, censors have increasingly blocked international news websites for their reporting on corruption and illicit wealth among high-level officials, as well as a range of other issues thought to challenge the government. Foreign-based news organizations with Chinese-lan-

[33] "China sets up State Internet Information Office," *China Daily*, May 4, 2011, http://bit.ly/1LMdB8M. See also Freedom House, "New Agency Created to Coordinate Internet Regulation," *China Media Bulletin*, May 5, 2011, http://bit.ly/1VR5RBG.

[34] Xinhua, "State Internet Information Office regulates internet: Beijing," *Want China Times,* August 30, 2014, http://bit.ly/1k2Rhvt; Government of China, 国务院关于授权国家互联网信息办公室 负责互联网信息内容管理工作的通知, press release, January 2014, http://bit.ly/1VR6yLu.

[35] Office of the Central Leading Group for Cyberspace Affairs (CAC) website, http://bit.ly/1OzUsFS; David Feng, "Chinese Cyber Administration Office Goes Online," *Tech Blog 86*, December 31, 2014, http://bit.ly/1LMezBS. The name SIIO is still in common usage, and Freedom House uses it accordingly elsewhere in this report.

[36] "CNNIC Undergoes Personnel Changes" [in Mandarin], *Guangming Daily,* December 27, 2014, http://bit.ly/1G3Oqwa.

[37] Romi Jain, "China keeps its telecoms sector close," *Asia Times Online*, January 29, 2014, http://bit.ly/1LMeKgL.

guage websites are a particular target. As of March 24, 2015, at least 14 of 18 news websites tracked by the nonprofit news organization ProPublica were inaccessible inside China.[38] The system responsible for such automated, technical blocking of foreign websites is commonly referred to as China's "Great Firewall." In some cases, whole domain names or internet protocol (IP) addresses are blocked, with users receiving an explicit message about illegal content. Other interventions are less visible. For example, observers have documented unusually slow speeds that indicate deliberate throttling, which delays the loading of targeted sites and services.[39]

Authorities also use deep packet inspection (DPI) to scan both a user's request for content and the results returned for any blacklisted keywords. Once these are detected, the technology signals both sides of the exchange to temporarily sever the connection. Such granular control is less noticeable to users because specific pages can be blocked within otherwise approved sites, and because the interruption appears to result from a technical error.[40] Returning fake pages, or replacing the requested site with content retrieved from an unrelated IP address using a technique known as DNS poisoning, is another routine method of disrupting access to specific content. During the coverage period, websites hosting content and services that were not explicitly banned still found themselves temporarily offline because their web address had been substituted for another on the blacklist, overwhelming them with requests from Chinese users;[41] in at least one reported case, a search for banned censorship-circumvention software was redirected to pornographic content.[42]

In practice, filtering varies depending on timing, technology, and geographical region. ISPs reportedly install filtering devices differently, in the internet backbone or even in provincial-level internal networks, a development that would potentially allow interprovincial filtering.[43] The University of Macau's new campus in southern Guangdong Province has advertised unfiltered internet access,[44] but there were no reports during the coverage period on whether this had actually taken effect. As students led political protests in Taiwan and Hong Kong in 2014, censors sought to shut off their online interaction with the mainland, disrupting mainland access to chat applications that were used to organize the demonstrations, like KakaoTalk and LINE, and censoring vocabulary specific to the ongoing political developments.[45]

Software developers, both domestic and overseas, have created applications offering access to virtual private networks (VPNs), which encrypt the user's traffic and reroute it through a server outside the firewall to circumvent technical filtering. As of November 2014, China boasted the largest number of VPN users in the world, nearly 93 million, according to GlobalWebIndex.[46]

[38] Sisi Wei, "Inside the Firewall: Tracking the News that China Blocks," ProPublica, February 13, 2015, https://projects.propublica.org/firewall.

[39] "In Tandem with Slower Economy, Chinese Internet Users Face Slower Internet This Week," *China Tech News*, November 6, 2012, http://bit.ly/1L9Pm0L.

[40] Ben Wagner et al., "Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control,'" Global Voices Advocacy, June 25, 2009, http://bit.ly/1GbWFGq.

[41] Greatfire.org, "China just blocked thousands of websites," November 18, 2014, https://en.greatfire.org/blog/2014/nov/china-just-blocked-thousands-websites.

[42] Greatfire.org, "GFW upgrade fail—visitors to blocked sites redirected to porn," January 9, 2015, https://en.greatfire.org/blog/2015/jan/gfw-upgrade-fail-visitors-blocked-sites-redirected-porn.

[43] Xueyang Xu, Z. Morely Mao, and J. Alex Halderman, "Internet Censorship in China: Where Does the Filtering Occur?" *Passive and Active Measurement*, (2011): 133–142, http://pam2011.gatech.edu/papers/pam2011--Xu.pdf.

[44] Li Xueying, "Uncensored Internet for Macau university's new campus," *Straits Times*/ANN via *Jakarta Post,* August 2, 2013, http://bit.ly/1R9D1vb.

[45] See Oiwan Lam, "Censors On, China Still Doesn't Want Anyone Talking About Tiananmen Square," Global Voices Advocacy, January 6, 2014, http://bit.ly/1Peh1BB.

[46] Jason Mander, "90 Million VPN users in China have accessed restricted social networks," GlobalWebIndex blog, November

In January 2015, Chinese authorities reported an upgrade to its national firewall that blocked several providers of VPNs, including Astrill (based in Seychelles), StrongVPN (based in the United States) and Golden Frog (registered in Switzerland). Officials claimed that the upgrade was meant to uphold "cyberspace sovereignty."[47] Even when not actively disrupted, encrypted internet activity may attract surveillance.[48]

Certain internationally popular web applications are totally blocked, isolating the Chinese public from a global network of user-generated content. According to GreatFire.org, an organization that monitors blocked content in China, 169 of Alexa's top 1,000 websites in the world were blocked in 2014, up from 62 the year before.[49] These include Google, Facebook, Flickr, SoundCloud, and WordPress.[50] In May 2014, five days before the 25th anniversary of the Tiananmen Square crackdown, Google's remaining services were fully blocked, including Google Maps, Translate, Calendar, and Scholar,[51] and they remained so as of May 2015. Google Analytics, which provides audience data to website owners, remained operational, according to the London-based *Guardian* newspaper.[52] Other social media services like the photo-sharing platform Instagram and Viber were blocked during the Umbrella Revolution protests that shook Hong Kong in the autumn of 2014.[53] In July 2014, Instagram was removed from online Android application stores run by the Chinese services Baidu, Xiaomi, Wandonjia, Qihou360, Tencent, and 91 Wireless. Users who had previously downloaded the Instagram app were still able to use it, but not if they were on China Mobile's 3G network, which had never allowed access to Instagram's servers.[54]

Many social media applications produce sanitized versions for the mainland Chinese market. In 2012, Evernote launched a separate service for the Chinese mainland, with modified terms of use containing a list of nine categories of "undesirable information." In January 2015, it disabled the public note feature, which had been used to share news and information about Hong Kong's Umbrella Revolution.[55] LinkedIn, which censors briefly blocked in 2011,[56] launched a Chinese-language version in early 2014. "We are opposed to censorship … [but] that's going to be necessary for us to achieve the kind of scale that we'd like to be able to deliver to our membership," Chief Executive Jeff Weiner told the *Wall Street Journal*. LinkedIn informed users when their content would not be visible in China.[57]

Search requests that include blacklisted keywords also trigger China's censorship apparatus, produc-

24, 2014, http://bit.ly/1VR9Y0M.

[47] "China blocks virtual private network use," BBC, January 26, 2015, http://bbc.in/1CrMgBJ; Jon Russell, "China Cracks Down On VPN Services After Censorship System 'Upgrade,'" *TechCrunch*, January 23, 2015, http://tcrn.ch/1BPJtUe.

[48] Rebecca MacKinnon, "The Shawshank Prevention," *Foreign Policy*, May 2, 2012, http://atfp.co/1OvpW1B.

[49] GreatFireChina, Twitter Post, November 25, 2014, 5:07 p.m., https://twitter.com/greatfirechina/status/537411878985539586.

[50] GreatFireChina, "Censorship of Alexa Top 1000 Domains in China," https://en.greatfire.org/search/alexa-top-1000-domains.

[51] Julie Makinen, "China broadens crackdown on Google services," *Los Angeles Times,* June 13, 2014, http://lat.ms/1qQMKtO.

[52] Maria Repnikova and Timothy Libert, "Google is returning to China? It never really left," *Guardian*, September 21, 2015, http://bit.ly/1Ku8EOi.

[53] "China blocked information of the Occupy Central in Hong Kong" [in Mandarin], September 30, 2014, https://pao-pao.net/article/192; Josh Chin and Eva Dou, "Hong Kong Protests Lead to Censorship on WeChat," *China RealTime Report*, *Wall Street Journal*, October 3, 2014, http://on.wsj.com/1hD6Sjq.

[54] Adam Pasick, "Instagram's ambiguous takedown highlights the challenge for foreign apps in China," *Quartz*, July 10, 2014, http://bit.ly/1Nbw4Ja.

[55] Catherine Shu, "Evernote's Chinese Service Disables Public Note Feature," *TechCrunch*, January 5, 2014, http://tcrn.ch/1GbZozn.

[56] Keith B. Richburg, "Nervous about unrest, Chinese authorities block web site, search terms," *Washington Post,* February 25, 2011, http://wapo.st/1Mps054.

[57] Paul Mozur, "LinkedIn Said It Would Censor in China. Now That It Is, Some Users Are Unhappy," *Wall Street Journal,* June 4, 2014, http://on.wsj.com/TbVMX2.

ing blank or severely limited results. In 2014, censorship intensified in advance of the 25th anniversary of the crackdown on student-led protests to encompass phrases like "return to Tiananmen,"[58] "89," "8 squared," and "Victoria Park," the Hong Kong site of a massive annual vigil.[59] In May, one blog reported that a user-generated encyclopedia hosted by Baidu had entries for the years 1988 and 1990, but not 1989.[60]

Even the names of prominent activists are often censored. Examples during the coverage period include "Pu Zhiqiang," after the renowned human rights lawyer was detained in Beijing in May 2014, and "Ilham Tohti," the Uyghur scholar who was sentenced to life in prison on "separatism" charges for his essays defending Uyghur rights online.[61]

The censorship backlash against forums on "constitutionalism" continued during the coverage period. Discussion of the concept was banned on at least one platform in 2014 after it became associated with a fledgling civic movement,[62] suggesting that social movements are perceived as more of a threat than opinions or discussions on their own.[63] According to one 2014 study, "even posts that praise the government are censored if they pertain to real-world collective action."[64]

Content Removal

In the past, the government has not been transparent about content controls, telling international reporters in September 2013 that "the perception that the government has placed any restrictions on the internet is untrue."[65] However, a draft cybersecurity law, released to the public outside the coverage period in July 2015, makes it clear that the authorities are tasked with imposing such restrictions. The legislation states that the "national cyberspace administration and relevant departments perform network security supervision and administration responsibilities; and where discovering information the release or transmission of which is prohibited by laws [or] administrative regulations, shall request the network operators stop transmission, employ disposition measures such as deletion, and store relevant records; for information described above that comes from outside mainland People's Republic of China, they shall notify the relevant organization to adopt technological measures and other necessary measures to block the transmission of information."[66]

[58] See "2014 Tiananmen Censorship Season Begins On Sina Weibo With 'Return to Tiananmen,'" *Fei Chang Dao* (blog), February 24, 2014, http://bit.ly/1LsX2g5; "As the 25th Anniversary of June 4, 1989 Nears, Baidu Censors '198964,'" *Fei Chang Dao* (blog), May 17, 2014, http://bit.ly/1LMjqD4.

[59] Jason Q Ng, "64 Tiananmen-Related Words China Is Blocking Online Today**,**" *Wall Street Journal*, June 4, 2015, http://on.wsj.com/1mTkmVe.

[60] "25 Years After Tiananmen, Baidu's Wikipedia has No Article for '1989,'" *Fei Chang Dao* (blog), May 3, 2014, http://bit.ly/1X0OIIl.

[61] Sean Silbert, "China sentences Uighur professor to life in prison on separatism charge," *Los Angeles Times*, September 23, 2014, http://lat.ms/1Gc2009.

[62] "25 Years After Tiananmen, Baidu's Wikipedia has No Article for '1989'"; "社评：依法审理许志永案，反对立场先行," Huanqiu, January 23, 2014, http://opinion.huanqiu.com/editorial/2014-01/4781693.html.

[63] "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, 14th ACM Conference on Computer and Communications Security, October 29–November 2, 2007), http://bit.ly/1jwIq4q; Gary King, Jennifer Pan, and Margaret E. Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression," *American Political Science Review* 107, no. 2 (May 2013): 1–18, Harvard University, http://bit.ly/1sixdlX.

[64] Gary King, Jennifer Pan, and Margaret E. Roberts, "Reverse-engineering censorship in China: Randomized experimentation and participant observation," *Science Magazine* 345, no. 6199 (2014): 1–10, Harvard University, http://bit.ly/VNPL40.

[65] Heather Timmons and Ivy Chen, "Beijing calls fears over internet crackdown 'paranoia,' briefly detains corruption-fighting blogger," *Quartz*, September 18, 2013, http://bit.ly/1PrOBDw.

[66] Cybersecurity Law (Draft), translated by China Law Translate, http://chinalawtranslate.com/cybersecuritydraft/?lang=en.

Still, censorship decisions are arbitrary, opaque, and inconsistent, in part because so many individuals and processes are involved. Blacklists periodically leak online, but they are not officially published. There are no formal avenues for appeal. Criticism of censorship is itself censored.[67]

Antipornography and antirumor campaigns are a long-standing cover for censorship of social and political content. On January 19, 2015, the SIIO announced the shutdown of 133 public accounts on the social media site Weixin—whose international version is known as WeChat—that had purportedly spread false information about the history of the CCP and the country.[68] On March 25, the SIIO published new guidelines outlining prohibited content on Weixin, specifically targeting sexually explicit material, but also banning stories of "one-night stands, wife-swapping, sexual abuse and other harmful information," according to Reuters.[69]

Mobile service providers monitor text messages and delete pornographic or other "illegal" content.[70] Users report receiving blank messages in place of banned keywords, though what content is banned appears to vary.[71]

Instant-messaging services such as TOM-Skype and QQ include programming that downloads updated keyword blacklists regularly.[72] Other companies employ human censors to delete posts, sometimes before they appear to the public.[73] Experts say staff members receive as many as three censorship directives per day by text message, instant message, phone call, or e-mail.[74] Most come from local propaganda officials. However, the CCP established party branches within four microblog company offices in 2012 to improve compliance, according to news reports.[75] In a November 2013 article published in Tibet, the local party leader pledged to establish CCP units or send political instructors to conduct ideological education in website offices.[76]

Provincial police also have authority to issue takedown notices to local companies. In April 2014, local and international media reported that Wei Yining, an internet police official in Hainan Province, had recently been sentenced to 10 years in prison for accepting more than 280 bribes to issue such notices to Hainan-based web forums Tianya and Kaidi. The bribes were paid by internet police in other jurisdictions, who should have submitted their deletion requests to Wei's department for approval, but instead paid him to contact the companies directly via instant message. One colleague in Hubei Province paid 483,000 yuan (US$78,000) in one year.[77]

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

[68] CAC, "SIIO: 133 public accounts that disseminate false information about the history of the Party and country had been closed down according to the law," http://www.cac.gov.cn/2015-01/19/c_11140517959.htm.

[69] Juliana Kenny, "China wrestles with 'vulgar' content," *Blouin News*, March 26, 2015, http://bit.ly/1VQN3rG.

[70] Agence France-Presse, "China Mobile Users Risk SMS Ban in Porn Crackdown," *ABS-CBN News,* January 14, 2010, http://bit.ly/1Ljww5q; Elaine Chow, "So about that sexting ban in China," *Shanghaiist*, January 20, 2012, http://bit.ly/1PemWqk.

[71] Elaine Chow, "An Alleged List of Banned SMS Terms from China Mobile and Co.," *Shanghaiist*, January 4, 2011, http://bit.ly/1MpvfcT.

[72] TOM-Skype is a joint venture between Skype and Chinese wireless service TOM Online. Vernon Silver, "Cracking China's Skype Surveillance Software," *Bloomberg Business*, March 8, 2013, http://bloom.bg/1jwMz8G; 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://bit.ly/1ZAQfaq; Jeffrey Knockel, "TOM-Skype Research," http://cs.unm.edu/~jeffk/tom-skype/.

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

[74] Xiao Qiang, "From 'Grass-Mud Horse' to 'Citizen': A New Generation Emerges through China's Social Media Space," (presentation, Congressional-Executive Commission on China, Washington, DC, November 17, 2011), http://1.usa.gov/19dzOZn.

[75] Qiao Long, "CCP Proposes Cells for Microblogs," Radio Free Asia, February 7, 2012, http://bit.ly/1PenOLK.

[76] Chen Qunaguo, *Seeking* Truth, "以敢于亮剑的精神确保西藏意识形态领域安全: 认真学习贯彻习近平总书记在全国宣传思想工作会议上的重要讲话精神," November 2, 2013, http://bit.ly/1GGIJQC.

[77] Josh Chin and Yang Jie, "Corruption Case Cracks Door on China's Internet Police," *China Real Time, Wall Street Journal,* April 18, 2014, http://on.wsj.com/1fg3CmV; "More Details Emerge of Internet Police Involved in Nationwide Money-For-

Other content has been suppressed by private actors. In June 2014, Beijing-based *Caixin* magazine reported that a China Central Television (CCTV) executive under investigation for bribery had asked website operators to delete posts on behalf of other companies.[78] Search engines also remove or highlight results, possibly squelching negative items about their own performance, according to one analysis.[79]

In March 2015, *Under the Dome*, a critically acclaimed documentary detailing China's air pollution that was viewed by over 150 million users on Tencent alone and praised by the environment minister, was pulled from domestic video-sharing websites after it gained widespread attention.[80]

Media, Diversity, and Content Manipulation

Online journalists regularly practice self-censorship. Editors and reporters who post banned content, or content that is critical of the CCP, its high-ranking members, or its actions, now or in the past, risk disciplinary warnings, job loss, or even criminal detention. Authoirites warned online news providers of tighter scrutiny in 2015,[81] and threatened the web portal Sina with suspension in April for failing to prevent violations.[82] In May, the agency published a list of news organizations that were "authorized to provide websites for reposting news."[83]

Propaganda officials also manipulate online content, instructing internet-based outlets to amplify content from state media. In one example from the coverage period, the State Council Information Office reportedly issued this directive: "All media must refrain from further promoting [the environmental documentary] 'Under the Dome.' Online public opinion [surrounding the documentary] must be regulated."[84]

Since 2005, propaganda units at all levels have trained and hired web commentators, known colloquially as the "50 Cent Party," to post progovernment remarks and influence online discussions.[85] These commentators also report users who have posted offending statements, target government critics with negative remarks, or deliberately muddy the facts of a particular incident.[86] Coordinated smear campaigns are used to discredit high-profile government critics.[87]

A document leaked in January 2015 revealed that there are 350,000 "Youth League Online Com-

Censorship Scheme," *Fei Chang Dao* (blog), April 21, 2014, http://bit.ly/1OvsuN3.

[78] "Caixin Report Provides Context for Baidu's 2011 Censorship of Search Results for 'CCTV Baidu,'" *Fei Chang Dao* (blog), June 16, 2014, http://bit.ly/1NFmz8f.

[79] "Caixin Report Provides Context for Baidu's 2011 Censorship."

[80] Gabriel Wildau, "China pulls smog documentary offline after internet storm," *Financial Times*, March 6, 2015, http://on.ft.com/1GGlXr8.

[81] "China's Internet Censor Increases Scrutiny on News Portals," *Bloomberg Business*, April 28, 2015, http://bloom.bg/1bPLy8l.

[82] Xinhua, "Sina faces suspension over lack of censorship," *People China*, April 11, 2015, http://bit.ly/1PrQu2V.

[83] "Government Tells People Who Is Authorized to Repost News Online," *Fei Chang Dao* (blog), May 2015, http://bit.ly/1K7qtPw.

[84] Josh Rudolph, "Minitrue: Don't Hype 'Under the Dome,'" *China Digital Times*, March 1, 2015, http://bit.ly/1Gc4goh.

[85] David Bandurski, "Internet spin for stability enforcers," China Media Project, May 25, 2010, http://cmp.hku.hk/2010/05/25/6112/.

[86] These propaganda workers are colloquially known as the 50 Cent Party due to 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), *New York Review of Books*, July 10, 2013, http://bit.ly/1bj1vTt; 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.

[87] See Murong Xuecun, "Beijing's Rising Smear Power," *New York Times*, September 21, 2014, http://nyti.ms/1OvsWuZ.

mentators" in China's higher-education institutions, tasked with swaying students against supposed Western values;[88] more recruits are being sought.[89] The work also extends beyond China's borders to social media apps that are actually banned for mainland users, such as Twitter. Approximately 2,500 "50 Cent" users on Twitter follow and retweet one another in order to create confusion and mislead the public.[90] In July 2014, it was revealed by the London-based organization Free Tibet that propagandists had opened scores of fake accounts on Twitter to glorify China's Tibet policies.[91] Other such fake accounts were created in an attempt to smear dissidents, notably the writer Hao Qun, known by his pen name Murong Xuecun, who wields considerable influence online both domestically and internationally, but whose Sina Weibo microblogging account was deleted in a 2013 purge.[92]

These methods are not always effective, however. Many government-paid commenters are more concerned about filling their quota than mounting a convincing argument, and web users are wary of content manipulation. Companies also pay for "astroturfing"—positive comments promoting products or services—which further erodes public trust in online content. (Commercial commenters are colloquially known as the "internet water army."[93]) However, in January 2015 the SIIO, MIIT, Ministry of Public Security, and SAPPRFT launched a joint campaign against "internet blackmail and paid content removal," cracking down on companies that accept fees for deleting "unfavorable" posts.[94]

In March 2014, the state news agency Xinhua announced the latest round of internet supervision training courses for officials across government institutions, including the police and the judiciary. The courses, which offer five qualifications from assistant to senior manager, cost 6,800 yuan (US$1,108).[95] Government employees also openly engage citizens in online discussions. In October 2013, an opinion-monitoring official at the *People's Daily* newspaper, an official CCP mouthpiece, said that the quantity of posts by the Weibo accounts of traditional media outlets and government officials or entities had overtaken the output of high-profile online opinion leaders with mass followings, known as Big Vs.[96]

Nationalism and xenophobia are prominent components of Chinese cyberspace, though censorship that targets rational dissent instead of inflammatory discourse arguably magnifies their impact. In March 2014, when students in Taiwan occupied the legislature to protest against a free-trade pact with China, Weibo said 60 percent of microbloggers polled called the action "irrational," but the service censored posts that compared the incident to China's 1989 student protests.[97]

[88] Sandra Fu, "Central Committee of Communist Youth League Issues an Announcement," *China Digital Times*, January 19, 2015, http://bit.ly/1jmXT7R.

[89] Xu Yangjingjing and Simon Denyer, "Wanted: Ten million Chinese students to "civilize" the Internet," *Washington Post*, April 10, 2015, http://wapo.st/1NbD9tb.

[90] "The New Generation of Fifty-Centers on Twitter," *I YouPort*, October 9, 2014, https://iyouport.com/en/archives/676.

[91] Jonathan Kaiman, "Free Tibet exposes fake Twitter account by China propagandists," *The Guardian*, July 22, 2014, http://bit.ly/1o5tPMD.

[92] Xuecun, "Beijing's Rising Smear Power."

[93] Rongbin Han, "Manufacturing Consent in Cyberspace: China's 'Fifty-Cent Army'," *Journal of Current Chinese Affairs* 44, no. 2 (2015): 105-134, http://bit.ly/1R9RKWK) Cheng Chen, et al, "Battling the Internet Water Army: Detection of Hidden Paid Posters," arXiv, November 18, 2011, http://arxiv.org/abs/1111.4297.

[94] CAC, "SIIO and other three governmental branches regulate Internet blackmail and paid content removal" [in Mandarin], January 21, 2015, http://bit.ly/1jn7ITl; Xinhua, "China Gets Tough on Online Extortion," *China Daily*, January 21, 2015, http://bit.ly/1OAfvbu.

[95] Oiwan Lam, "Chinese Government is "Winning" Internet Ideology Battle," *Global Voices Advocacy*, November 8, 2013, http://bit.ly/1Ps0fy4; Alastair Sloan, "China ramps up army of "opinion monitors," Index on Censorship, March 25, 2014, http://bit.ly/1NFCrYq.

[96] "人民網輿情監測室秘書長祝華新：網際網路生態治理晴空初現," October 30, 2013, http://bit.ly/1jxa7Kx.

[97] Andrea Chen, "Taiwan student occupation and clashes 'a failure of democracy,' mainland microbloggers say," *South China Morning Post*, March 24, 2014, http://bit.ly/1VRwuGG.

Still, political discourse can be vigorous online, even about democracy and constitutional government.[98] This is partly because the leadership redefined democratic governance as "the Chinese Communist Party governing on behalf of the people" in 2005.[99] A certain amount of open discussion also allows officials to monitor public sentiment, debunk "enemy" ideology without triggering censorship,[100] and conduct internal power struggles. Censors employed by Sina allowed "more room for discussions on democracy and constitutionalism because there are leaders who want to keep the debate going," according to one report.[101]

Domestic internet firms benefit commercially from the blocking of foreign social media, but they are obliged to prevent banned content from circulating as part of their licensing requirements. Chinese company executives also enjoy political patronage.[102]

More than half of China's internet users had registered for a microblog account by January 2013.[103] Many companies offer services, but the most prominent are Sina Weibo and Tencent's Weixin. In April 2013, news agencies were told to register official microblog accounts with their government sponsor.[104]

Weibo's distinct feature is the comment thread developed in response to individual posts; the threads are lost if the original post is censored, and the feature can also be shut off to prevent a given post from gaining traction.[105] In March 2014, Sina's prospectus to the U.S. Securities and Exchange Commission reported 129 million Weibo users active every month and 61 million active daily,[106] though a research study from Hong Kong said the majority of posts were generated by just 10 percent of users, while thousands of others were zombie accounts created for marketing purposes.[107] Sina's efforts to manage Weibo content are well documented. Staff, reportedly 150 people working 12-hour shifts,[108] delete individual posts or accounts, often within 24 hours of an offending post, but sometimes long after publication;[109] make published posts visible only to the account owner; and personally warn individual users.[110] Moreover, hundreds of terms have been automatically filtered from Weibo search results over time.[111]

[98] See Xu Qianchuan, "Constitution Debate Holds Broader Reform Implications," *Cajing*, July 16, 2014, http://bit.ly/1Ps0J7p; King, Pan, and Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression"; Ashley Esarey and Xiao Qiang, "Digital Communication and Political Change in China," *International Journal of Communication* 5 (2011): 298–319, http://bit.ly/1LKgXCU. Xiao Qiang was an advisor for this report.

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

[100] See "以敢于亮剑的精神确保西藏意识形态领域安全," November 1, 2013, http://bit.ly/1GGlJQC.

[101] See "China must crack down on critical online speech: party journal," Reuters, Sept 16, 2013, http://reut.rs/1GGsphD.

[102] Freedom House, "Tech Company Leaders Join Legislative, Advisory Bodies," *China Media Bulletin*, March 7, 2013, http://bit.ly/1R9T77X.

[103] Not all accounts are active. CNNIC, *Di 31 Ci Zhongguo Hulianwangluo Zhuangkuang Tongji Baogao* [The 31st Statistical Report on China's Internet Development," January 15, 2013, http://bit.ly/1LKj3CO.

[104] A government sponsor is required to obtain a press license. "China's Real Name Internet Part 5: 2013–2014," *Fei Chang Dao* (blog), August 20, 2014, http://bit.ly/1jn9S5k.

[105] Gady Epstein, "The Great Firewall: The Art of Concealment," *Economist*, April 6, 2013, http://econ.st/145qZuP.

[106] Securities and Exchange Commission, "Form F-1 Registration Statement Under The Securities Act of 1933, Weibo Corporation," Washington, DC, Reg. No. 333, http://1.usa.gov/1fzstAZ.

[107] Patrick Boehler, "Almost all Weibo messages are generated by just 5 per cent of users," *South China Morning Post,* April 8, 2014, http://bit.ly/1lJuxfR.

[108] Li Hui and Megha Rajagopalan, "At Sina Weibo's censorship hub, China's Little Brothers cleanse online chatter," Reuters, September 11, 2013, http://reut.rs/1LMCa5z.

[109] Keith B. Richburg, "China's 'weibo' accounts shuttered as part of internet crackdown," *Washington Post*, January 3, 2013, http://wapo.st/1ZBq82V.

[110] Xiao, "From 'Grass-Mud Horse' to 'Citizen': A New Generation Emerges through China's Social Media Space."

[111] "How a Weibo post gets censored: what keywords trigger the automatic review filters," *Blocked on Weibo* (blog), November 26, 2014, http://bit.ly/1LtbwMR; Xiao, "From 'Grass-Mud Horse' to 'Citizen': A New Generation Emerges through

Weibo was punished with restrictions on some of its functions in 2012 for failing to curb "rumors."[112] In 2013, following an intensified antirumor campaign, Weibo said 1,000 accounts had been shuttered for posting false information, out of a total 100,000 accounts that were disabled for harassment and other violations.[113] Activity on the platform dropped by an estimated 70 percent.[114] In January 2014, the CNNIC reported that 38 percent of Weibo users had migrated to Weixin.[115]

In 2015, Tencent reported a combined 500 million monthly active users for Weixin and its international equivalent.[116] Some activists prefer Weixin because users have the option to restrict updates to a closed circle of connections, and can send audio messages that bypass keyword censorship.[117] Yet the service still monitors and restricts political content. In what users described as a "massacre" in March 2014, just before the coverage period, Weixin closed dozens of accounts, including one run by investigative journalist Luo Changping.[118]

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 gaming population, 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 email 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.

Users combat censorship by opening versions of the same blog on different sites and circulating banned information directly through peer-to-peer networks, which bypass central servers. Text rendered as image, audio, or video files evades keyword sensors. Humorous neologisms, homonyms, and cryptic allusions substitute for banned keywords,[119] forcing censors to filter seemingly innocuous vocabulary like "tiger."[120] 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."[121]

China's Social Media Space". See also Tao Zhu et al., "The Velocity of Censorship: High-Fidelity Detection of Microblog Post Deletions" (paper for 22nd USENIX Security Symposium, Washington, DC, August 2013), arXiv, http://bit.ly/1G4dIdx; King-wa Fu and Michael Chu, "Reality Check for the Chinese Microblog Space: A Random Approach," *PLoS ONE* 8, no. 3 (2013), http://bit.ly/1LMCP6R.

[112] Xinhua, "China's major microblogs suspend comment function to 'clean up rumors,'" *People's Daily Online*, March 31, 2012, http://bit.ly/1RGh3kn.

[113] "Sina shuts down weibo accounts," *China Daily,* November 14, 2013, http://bit.ly/1OvymWC.

[114] Malcolm Moore, "China kills off discussion on Weibo after internet crackdown," *Telegraph,* January 30, 2014, http://bit.ly/1fDGbEW.

[115] See CNNIC, 中国互联网络发展状况统计报告, January 2014, http://bit.ly/1LMDtBB.

[116] Lulu Yilun Chen, "Tencent Climbs as Ad Surge Boosts WeChat Earnings Outlook," *Bloomberg Business*, March 18, 2015, http://bloom.bg/1Ltc8Cc.

[117] Alexa Oleson, "China's New Media Species, Now Endangered?" *Foreign Policy*, March 15, 2014, http://atfp.co/1OvyDsJ.

[118] Ben Blanchard and Paul Carsten, "China cracks down again on popular messaging app WeChat," ed. Jeremy Laurence, *Reuters*, March 14, 2014, http://reut.rs/1LjHbwM.

[119] Jason Q. Ng, "Censoring a commemoration: What June 4–related search terms are blocked on Weibo today," Citizen Lab, June 3, 2013, http://bit.ly/1LjHcB5.

[120] Anne Henochowicz, "Sensitive: PX Protests, Tigers, More," *China Digital Times*, April 2, 2014, http://bit.ly/1La8bAV.

[121] Xiao, "From 'Grass-Mud Horse' to 'Citizen': A New Generation Emerges through China's Social Media Space."

Digital Activism

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.[122] Whereas Chinese citizens traditionally trek to the seat of power to present their grievances, digital 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 do yield to public pressure. Low-level government wrongdoing, once exposed by users, is often punished, with officials frequently singled out for overspending on entertainment or designer watches, a sign of possible corruption.[123] Officials do seek to gauge, and are influenced by, the public mood.

The transformative effect of online activism in China is undeniable, and yet the final outcomes of high-pressure encounters between netizens and officials typically fall short of systemic reform or democratic decision-making. Consequently, they fail to ensure meaningful accountability.[124] Censors intervene if campaigns gain too high a profile or implicate overall CCP governance. In the past year, some nongovernmental organizations found their ability to fundraise using e-commerce platforms obstructed, including a rural library project that was forced to close in September 2014.[125]

In April 2015, a campaign to release five feminists who had been detained in March for distributing leaflets against sexual harassment on public transportation gained momentum, with an online petition signed by over 1,000 people that had circulated via private email and encrypted social-media messaging systems.[126] The women were released on April 13, but they remained under surveillance.

Violations of User Rights

A number of criminal laws and internet regulations ensnare users who post content deemed undesirable by the CCP. Authorities use antipornography and antirumor campaigns as a cover for suppressing politically sensitive material and voices, and charges typically used to silence offline dissent—subversion, separatism, and terrorism, as well as defamation and "creating a disturbance"—are regularly invoked to imprison citizens for their online activity. A bolstered "real-name registration" system remains a threat to users' privacy and anonymity, and surveillance has increased in ethnic minority areas chafing under CCP rule. Websites, hosting services, and dissidents' email accounts are routinely attacked by hackers based in China.

[122] David Barboza, "Despite Restrictions, Microblogs Catch On in China," *New York Times*, May 15, 2011, http://nyti.ms/1X1ri5y.

[123] Laura Zhou, "Watch Imprint on Quake Official's Wrist Goes Viral on Internet," *South China Morning Post*, April 24, 2013, http://bit.ly/1ZBtOBT; Jonathan Kaiman, "Chinese Police Chief Suspended after Online Storm over Teenager's Detention," *Guardian,* September 24, 2013, http://bit.ly/1jxg7mB.

[124] 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 censored. See Freedom House, "Finnish Study Analyzes Keyword Censorship during Mass Incidents," *China Media Bulletin*, December 13, 2012, http://www.freedomhouse.org/cmb/77_121312#5.

[125] Cao Haili, "李英強：從立人到福音,"*New York Times Chinese Network*, September 26, 2014, http://nyti.ms/1RGiG1n; *Global Times*, "Non-profit library closed for unauthorized branches: official," Sina English, September 23, 2014, http://bit.ly/1VRC6kg.

[126] Didi Kirsten Tatlow, "Supporters of Detained Feminists Petition for Their Release," *Sinosphere* (blog), *New York Times,* April 1, 2015, http://nyti.ms/1K7FcKd.

Legal Environment

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 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; subversion, separatism, and antiterrorism laws; and state secrets legislation to imprison citizens for online activity.

The legal grounds for these charges were strengthened in 2013. In September, the Supreme People's Court and the Supreme People's Procuratorate, the top prosecutorial body, issued a judicial interpretation entitled "Regarding the Interpretation of Various Laws Concerning the Handling of Cases of Using the Internet to Carry Out Defamation and Other Crimes," which formally defined online manifestations of crimes including defamation, creating disturbances, illegal commercial activities, and extortion.[127] Local officials had already detained online whistle-blowers for criminal defamation, which carries a possible prison term of three years under "serious" circumstances.[128] But the new interpretation defined those circumstances to cover defamatory online content that receives more than 5,000 views or is reposted more than 500 times.[129] Online messages deemed to incite unrest or protest are also subject to criminal penalties under the interpretation.

Bloggers and activists periodically use the law to defend their right to online expression. In July 2014, Wang Long,[130] a resident of Shenzhen, Guangdong Province, sued China Unicom for failing to provide access to Google services during the block that began in May 2014. A local court in Shenzhen's Futian district heard the case, the first of its kind, in September 2014.[131] Though many legal challenges lack the resources or the political backing to succeed, in April 2014, a court in Guangdong ordered the local health and family planning commission to reprocess a 2007 request submitted under open-government regulations. The commission had declined to release records about resource allocation to a lawyer based in Zhejiang, who successfully sued for it to reconsider.[132]

[127] Human Rights Watch, "China: Draconian Legal Interpretation Threatens Online Freedom," September 13, 2013, http://bit.ly/1ZBv0Ff; Megha Rajagopalan and Adam Rose, "China Crackdown on Online Rumors Seen as Ploy to Nail Critics," Reuters, September 18, 2013, http://reut.rs/1PeTbFX.

[128] 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/.; Associated Press, "Chinese prosecutors decide not to charge journalists detained for online posts in 2013," *Star Tribune,* September 10, 2015, http://strib.mn/1ZBKiK6.

[129] Human Rights Watch, "China: Draconian Legal Interpretation Threatens Online Freedom."

[130] Wang Long was detained in October 2014 after posting photos of the Hong Kong Occupy Central protests on mainland social media. See "Shenzhen man detained after posting Occupy Central pictures," *South China Morning Post,* October 1, 2014, http://bit.ly/1LjKRie.

[131] Austin Ramzy, "Lawsuit Raises Questions Over China's Internet Censorship," *Sinosphere* (blog), *New York Times*, September 5, 2014, http://nyti.ms/1BgkZ3k.

[132] David Bandurski, "Lawyer wins open information case in Guangzhou," China Media Project, April 4, 2014, http://bit.ly/1jJ7zW5.

Prosecutions and Detentions for Online Activities

Reporters Without Borders documented a total of 84 netizens in Chinese jails as of September 2015.[133]

Netizens and activists have been detained in a series of crackdowns over the last several years that were aimed at curtailing protests and perceived threats to "social and public order." Those affected have included lawyers who utilized social media to advocate for civil society, like Xu Zhiyong, and well-known online commentators and bloggers who were accused of "spreading rumors online."

On April 24, 2014, authorities detained renowned 70-year-old journalist Gao Yu, a contributor to the German news outlet Deutsche Welle, for "leaking state secrets." Official media alleged that Gao provided a secret document of the CCP Central Committee (believed to be Document No. 9, which warned officials to be vigilant about "seven subversive elements" in society, including human rights) to a foreign website, which published it in full. Her closed-door trial took place on November 21, 2014, but a verdict was not handed down until April 17, 2015, when Gao was convicted and sentenced to seven years in prison.

Pu Zhiqiang, a human rights lawyer, was detained in Beijing on May 6, 2014, on suspicion of "picking quarrels" after he attended a May 3 seminar about the 25th anniversary of the Tiananmen Square crackdown. He was formally arrested on June 13. Pu has been charged with creating a disturbance, inciting ethnic hatred, and separatism, based on 28 posts Pu made on Weibo between July 2012 and May 2014—the prosecution's only evidence.[134] In May 2015, a year after his detention, the procuratorate announced that Pu would stand trial for inciting ethnic hatred and picking quarrels.[135] A trial date was not immediately released.

The Hong Kong prodemocracy protests of September and October 2014 triggered another wave of arrests. Nearly two dozen people were detained for expressing support for the growing protests. Wang Long, the rights advocate in Shenzhen who had filed a lawsuit against China Unicom for censoring Google earlier in 2014, was detained on September 27, 2014, on charges of "creating a disturbance" after he forwarded news reports about the protests.[136]

Hundreds were detained in the ongoing campaign to crack down on alleged online rumor-mongering, and in August 2014 state authorities announced that they had arrested four people and detained another 81.[137] Dong Rubin, a Yunnan-based blogger with 50,000 followers who is known for his criticism of party officials, police brutality, and environmental hazards, was sentenced to six and a half years in prison in July 2014.[138]

[133] Two of those imprisonments occurred after the coverage period ended on May 31. Other cases go unreported. See Reporters Without Borders, "2015: Netizens Imprisoned," Press Freedom Barometer, accessed September 23, 2015, http://bit.ly/1GuFfjv.

[134] Chris Buckley, "Comments Used in Case Against Pu Zhiqiang Spread Online," *Sinosphere* (blog), *New York Times*, January 29, 2015, http://nyti.ms/1GGuHNN.

[135] Chris Buckley, "Chinese Rights Lawyer Detained in 2014 Will Stand Trial," *New York Times*, May 15, 2015, http://nyti.ms/1X1tYQT.

[136] Andrew Jacobs, "Detentions of Hong Kong Protest Sympathizers Reported in Mainland," October 1, 2014, *New York Times*, http://nyti.ms/1R9X2Si.

[137] "85 people 'arrested or detained' as China steps up clampdown on internet rumours," *South China Morning Post,* August 9, 2014, http://bit.ly/1hDskF4.

[138] Tabitha Kinder, "China: 'Rumor Mongering' Lands Dong Rubin in Jail for Six Years," *International Business Times*, July 23, 2014, http://bit.ly/1La9aBh.

As in past years, religious and ethnic minorities faced particularly harsh treatment for online activity. In July 2014, a 22-year-old Uyghur man was detained for "rumor-mongering" following violent clashes in Xinjiang's Yarkand (Shache) County; he had alleged in an online post that Chinese security forces killed thousands of people. The man, a resident of Urumqi who was not publicly identified, uploaded the article onto an overseas website.[139] Internet service was shut down in Yarkand, and international observers were denied access to the area.

In January 2014, professor, writer, and Uyghur rights advocate Ilham Tohti was detained in a raid on his Beijing home. He was later indicted for allegedly spreading rumors, inciting ethnic hatred, and conducting separatist activities on a website he founded.[140] Separatism charges carry a possible death penalty in extreme cases. In September 2014, a court sentenced Tohti to life imprisonment.[141] Seven of his students, who had helped him with the website, were also convicted on separatism charges and sentenced to between three and eight years in prison in December 2014.[142]

In August, Tibetan blogger Dawa Tsomo was detained "for violating China's internet rules and regulations" after she had criticized the government's mishandling of the welfare and living conditions of Tibetans still living in Kyegudo, the site of a devastating 2010 earthquake. Her whereabouts following the detention were unknown.[143]

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.[144] At least two Uyghur website managers, Memetjan Abdulla and Gulmire Imin, were jailed for life in the aftermath of ethnic violence in Tibet in 2008 and Xinjiang in 2009, when local courts—often after closed trials—imprisoned at least 17 individuals involved with websites that reported on Tibetan or Uyghur issues.[145]

Though the people imprisoned represent a tiny percentage of the overall user population, their harsh sentences have a chilling effect on the close-knit activist and blogging community and encourage self-censorship in the broader public. 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.[146]

Chinese authorities abolished the extrajudicial sentence known as reeducation through labor in 2013 after domestic calls for reform.[147] However, individuals can be detained without trial under similarly

[139] Xin Lin, "China Holds Uyghur Netizen Over Yarkand Massacre Claims," trans. Luisetta Mudie, Radio Free Asia, August 11, 2014, http://bit.ly/1Ps7kP8.

[140] Tania Branigan, "China charges Uighur scholar Ilham Tohti with separatism," *Guardian,* July 30, 2014, http://bit.ly/1K7GmFv; Miao Deyu, "The Case Against Ilham Tohti," *Guardian*, May 7, 2014, http://bit.ly/1NFIJXK.

[141] Damien Grammaticas, "China jails prominent Uighur academic Ilham Tohti for life," BBC, September 23, 2014, http://bbc.in/1uocWkg.

[142] Celia Hatton, "China jails students of Uighur scholar Ilham Tohti," BBC, December 9, 2014, http://bbc.in/1LjI7kQ.

[143] "Tibetan Woman Blogger Detained for 'Political' Postings," trans. Dorjee Damdul, Radio Free Asia, August 7, 2014, http://bit.ly/1jxjxFK.

[144] 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://1.usa.gov/1LKqeuV.

[145] Committee to Protect Journalists, "China," *Attacks on the Press in 2011*, http://bit.ly/1RGln2Q.

[146] Chinese Human Rights Defenders (CHRD), *We Can Beat You to Death With Impunity: Secret Detention & Abuse of Women in China's "Black Jails,"* October 21, 2014, http://bit.ly/1OAn0iN.

[147] Xinhua, "Victims of Re-education Through Labor System Deserve Justice," *Global* Times, January 28, 2013, http://bit.ly/1NFKggC.

poor conditions in drug rehabilitation and "legal education" centers.[148] Internet users have also fallen victim to forced psychiatric detention. The whereabouts of at least one detainee, Li Qidong, who officials hospitalized in Liaoning in 2009 after he criticized the government in online articles, remain unknown.[149]

State agents also abduct and hold individuals in secret locations without informing their families or legal counsel. In 2012, 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.[150] In April 2014, the families of 17 Sina employees responsible for screening the company's e-publication content were informed that the workers were abroad on business for a month, but a local news outlet reported in May that they had been detained.[151] Dozens of human rights lawyers, including many representing clients in freedom of speech cases, disappeared or were held in undisclosed locations in 2015.[152]

Surveillance, Privacy, and Anonymity

Users hoping to avoid repercussions for their online activity face a 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,[153] especially since some verification is done through a little-known, government-linked contractor.[154]

In 2012, the National People's Congress Standing Committee approved new rules to strengthen the legal basis for real-name registration by websites and service providers.[155] 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.[156] Comment sections of major news

[148] CHRD, *We Can Beat You to Death With Impunity: Secret Detention & Abuse of Women in China's "Black Jails"*; Amnesty International, "China's 'Re-education Through Labour' Camps: Replacing One System of Repression with Another?" December 17, 2013, http://bit.ly/1LtdZa4.

[149] CHRD, *The Darkest Corners: Abuses of Involuntary Psychiatric Commitment in China*, 2012, http://bit.ly/1MxV3YP.

[150] The amendment took effect on January 1, 2013. Observers praised other aspects of the measure, including tentative steps toward increasing police accountability for surveillance. Committee to Protect Journalists, "China's New Law Sanctions Covert Detentions," March 14, 2012, http://cpj.org/x/49d9.

[151] Long Jian, "'为什么要屏蔽你？" *Infzm*, May 29, 2014, http://bit.ly/1VR3LXX.

[152] Associated Press, "Lawyer kidnapped hours after release of Chinese journalist working for German weekly," *U.S. News*, July 10, 2015, http://bit.ly/1Gcm1DR.

[153] Danny O'Brien, "China's name registration will only aid cybercriminals," Committee to Protect Journalists blog, December 28, 2012, https://cpj.org/x/5177.

[154] William Farris, "Guangzhou Daily Looks Into the Economics of the Weibo Real Name System," Google+, February 28, 2012, http://bit.ly/1Psal1W; *Guangzhou Daily*, "实名制数亿元市场仅两家瓜分 被指收费不透明," *News 163*, September 2, 2012, http://bit.ly/1VR4b0k; "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.

[155] "National People's Congress Standing Committee Decision Concerning Strengthening Network Information Protection," *China Copyright and Media* (blog), December 28, 2012, http://bit.ly/1RGoSqc.

[156] Joe McDonald, "China Real-Name Registration Is Now Law in Country," *Huffington Post*, December 28, 2012, http://huff.to/1NFLFnw.

portals, bulletin boards, blog-hosting services, and email providers already enforced some registration.[157] The MIIT also required website owners and internet content providers to submit photo identification when they apply for a license, whether the website is personal or corporate.[158] Nevertheless, the 2012 rules extended regulation to the business sector who must gain users' consent to collect their personal electronic data, and outline the "use, method, and scope" of its collection. The rules offer no protection against law enforcement requests for these records.[159]

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.[160] Sina's 2014 report to the U.S. Securities and Exchange Commission noted the company's exposure to potentially "severe punishment" by the Chinese government as a result of its noncompliance.[161] Implementation of the real-name policy also makes it harder for the state's hired commentators to operate undetected. One study reported officials encouraging commentators to use pseudonyms and fake documents to hide their affiliation with the propaganda department.[162] In summer 2014, the SIIO issued interim rules for anyone "employing instant messaging tools as public information services," requiring service providers to verify user identities and register them with a government agency.[163]

In January 2015, the SIIO announced that the government would truly begin enforcing real-name registration on all websites beginning on March 1. Alibaba Group Holding Ltd., Tencent Holdings Ltd., Baidu Inc., Sina Corp. affiliate Weibo Corp., and other companies were reported to have deleted more than 60,000 accounts on various platforms because they did not conform to the new, stricter regulations.[164]

A draft antiterrorism law was made public for consultation in November 2014. Among the provisions is a requirement for technology firms to provide the government with surveillance "back doors" and supply law enforcement agencies with encryption keys and user data. All online service providers and telecommunication companies would be required to store user data within China's borders.[165] As of May 2015, the draft law was still under deliberation.[166] In late 2015, outside the coverage period of this report, news reports said Chinese officials were seeking backdoor access to the data of Chinese users in direct requests to American technology companies.[167] Regulations for the Administration of

[157] "Ministry of Culture Will Curb Trend of Internet Indecency in 2009" [in Mandarin], *Net Bar China*, January 6, 2009, http://bit.ly/1LKuY3H; Chen Jung Wang, "Real Name System Intimidates High School BBS," CNHubei, November 29, 2009, http://bit.ly/1OAp7CY; "Internet Society of China: Real Name System for Bloggers is Set," Xinhua, October 22, 2006, http://www.itlearner.com/article/3522.

[158] Elinor Mills, "China seeks identity of Web site operators," *CNET News*, February 23, 2010, http://cnet.co/bXIMCp.

[159] Tim Stratford et al., "China Enacts New Data Privacy Legislation," Covington & Burling LLP, January 11, 2013, http://bit.ly/RRiMaM.

[160] C. Custer, "How to Post to Sina Weibo without Registering Your Real Name," *Tech in Asia*, March 30, 2012, http://bit.ly/1NFM0GP.

[161] See Securities and Exchange Commission, "Form F-1 Registration Statement Under The Securities Act of 1933, Weibo Corporation."

[162] Han, "Manufacturing Consent in Censored Cyberspace."

[163] "China's Real Name Internet Part 5: 2013–2014," *Fei Chang Dao*.

[164] Paul Carsten, "China censorship sweep deletes more than 60,000 Internet accounts," ed. Robert Birsel, Reuters, February 27, 2015, http://reut.rs/1AR2geU.

[165] Erika Kinetz, "China plays down US concerns over anti-terror legislation," Associated Press, March 4, 2015, http://bit.ly/1jnhK6R.

[166] Michael Martina, "China says deliberation of anti-terrorism law goes ahead," Reuters, March 16, 2015, http://reut.rs/1Av7Txc.

[167] Paul Mozur, "China Tries to Extract Pledge of Compliance From U.S. Tech Firms," *New York Times*, September 16, 2015, http://nyti.ms/1VRGvE1.

Commercial Encryption dating to 1999, and related rules from 2006, already require a government regulator to approve encryption products used by foreign and domestic companies.[168]

Internet commerce is undermining online anonymity. Many users voluntarily surrender personal details to enable financial transactions on social media sites. Mobile phone purchases have required identification since 2010, so providing a phone number is a common way of registering with other services.[169] One analyst estimated that 50 percent of microblog users had exposed their identification numbers to providers by 2012, simply by accessing the platform from their mobile phone.[170] Though not consistently enforced in the past, a crackdown on real-name registration for existing mobile subscriptions began in early 2015.[171]

China's "second generation" national ID cards—which are administered by police—are required to be digitally embedded with fingerprints; the first generation of cards became defunct in 2013.[172] The State Council aims to link credit, social security, and other personal information to these biometric databases. Writer Mo Zhixu laid out some possible implications, saying "ID numbers culled online will soon become useless for repeated use"; "relatives and friends will not … dare, to lend their ID numbers to anyone else"; and "personal credit information will necessarily include information about internet use."[173] In 2013, a Uyghur blogger reported that he was unable to join a Weixin page about sports using his national ID number, which identifies his birthplace as Xinjiang; he was only able to register with the number of a Han Chinese friend.[174]

Chinese providers are required to retain user information for 60 days, and submit it to the authorities upon request without judicial oversight or notification of the user.[175] In 2010, the National People's Congress amended the State Secrets Law,[176] obliging telecommunications operators and ISPs to cooperate with authorities investigating leaked state secrets or risk losing their licenses.[177] An amendment to the Criminal Procedure Law that took effect in 2013 introduced a review process for allowing police surveillance of suspects' electronic communications, which the Ministry of Public Security permits in many types of criminal investigation, but the wording of the amendment was vague about the procedure for the review.[178]

Privacy protections under Chinese law are minimal. In the words of one expert, the law explicitly au-

[168] Adan Segal, "The Cyber Trade War," *Foreign Policy,* October 25, 2014, http://atfp.co/1Qq5LzN.

[169] "Mobile phone real-name system implemented today, SIM card purchasers have to present their ID documents" [in Mandarin], *News 163*, October 1, 2010, http://bit.ly/aIyYL4.

[170] Song Yanwang, "Internet Clean-Up Regulations Conceal Obscure Issues. Weibo's New Real-Name Registration Rule Poses Challenge for Telecom Operator" [in Mandarin], *Net China*, March 15, 2012, http://net.china.com.cn/txt/2012-03/15/content_4875947.htm.

[171] "移动发狠招手机不实名将被停机 电信联通表示没听说过," May 20, 2015, http://bit.ly/1jnhXa1.

[172] Cao Yin, "Efforts Stepped Up to Curb Fraudulent ID Card Use" [in Mandarin], *China Daily,* August 15, 2013, http://bit.ly/1G4jzzC; Zhou Dawei, "Do We Really Need to Fingerprint 1.3bn People?" *News China Magazine,* January 2012, http://bit.ly/1Qq5nBa.

[173] Andy Yee, "How Social Commerce Tightens China's Grip on the Internet," Global Voices, May 22, 2013, http://bit.ly/1OvBcet.

[174] *Midnight Café* (blog), http://bit.ly/1NbSf1U; Oiwan Lam, "China: Real Name Registration May Threaten Ethnic Minorities," Global Voices Advocacy, June 24, 2013, http://bit.ly/1OAqvpp.

[175] OpenNet Initiative, "China," August 9, 2012, http://opennet.net/research/profiles/china-including-hong-kong.

[176] Central People's Government of the People's Republic of China, "Presidential order of the People's Republic of China, No. 28" [in Mandarin], April 29, 2010, http://bit.ly/1LMMtXc.

[177] Jonathan Ansfield, "China Passes Tighter Information Law," *New York Times*, April 29, 2010, http://nyti.ms/1LMMx9j.

[178] Luo Jieqi, "Cleaning Up China's Secret Police Sleuthing," *Caixin*, January 24, 2013, http://bit.ly/1LjK1BT.

thorizes government access to privately held data, and "systematic access" to "data held by anyone" is a realistic possibility once e-government strategies are fully implemented.[179]

Real-name registration is just one aspect of the pervasive surveillance of internet and mobile phone communications in China. The DPI technology used for censorship can monitor users, and personal text- and instant-message exchanges have been cited in court documents. One academic study reported that when users entered blacklisted search terms on Baidu, their IP addresses were automatically sent to a location in Shanghai affiliated with the Ministry of Public Security.[180] Cybercafes check photo identification and record user activities, and in some regions, surveillance cameras in cybercafes have reportedly transmitted images to the local police station.[181] Given the secrecy surrounding such capabilities, however, they are difficult to verify.

As with censorship, surveillance disproportionately targets individuals and groups perceived as antigovernment. In January 2015, the Xinjiang government issued a new regulation requiring real-name registration for Uyghurs attempting to purchase mobile phones, computers, and other electronic devices with storage, communication, and broadcast features. Stores selling such equipment are required to install software that provides police with real-time electronic records on transactions.[182]

Intimidation and Violence

Allegations of torture and extralegal harassment are widespread among Chinese detainees, particularly political prisoners, a category that encompasses the majority of freedom of expression cases. In May 2015, Human Rights Watch reported "physical and psychological torture during police interrogations, including being hung by the wrists, being beaten with police batons or other objects, and prolonged sleep deprivation" in a review of hundreds of ordinary criminal cases. "Political prisoners … have experienced much of what is described in this report and often worse," the report said.[183]

Internet users also risk being held under house arrest. In such cases, including the extralegal house arrest of poet Liu Xia (wife of Liu Xiaobo) since 2010, internet and mobile phone connections are often severed to prevent the individual from contacting supporters and journalists.[184] While there are several cases of long-term house arrest, the circumstances and degree of confinement can be adjusted arbitrarily over time. Some groups attempt to monitor the number of dissidents known to be held under house arrest, but there are no statistics showing how many were targeted specifically for online activity.[185]

Law enforcement officials frequently summon individuals for questioning in relation to online activity, an intimidation tactic referred to euphemistically as being "invited to tea."[186] Activists have also been

[179] Zhizheng Wang, "Systematic Government Access to Private-Sector Data in China," *International Data Privacy Law* 2, no. 4 (2012): 220–229, http://bit.ly/1Pf4jT8.

[180] Becker Polverini and William M. Pottenger, "Using Clustering to Detect Chinese Censorware" (presentation, Eleventh Annual Workshop on Cyber Security and Information Intelligence Research, 2011), http://bit.ly/1Ra1XCx.

[181] Naomi Klein, "China's All-Seeing Eye," NaomiKlein.org, May 14, 2008, http://bit.ly/2nf29.

[182] Bai Tiantian, "Xinjiang asks real-name registration for cellphones, PCs," *Global Times*, January 29, 2015, http://bit.ly/1NFNqRo.

[183] Human Rights Watch, "Tiger Chairs and Cell Bosses: Political Torture of Criminal Suspects in China," May 13, 2015, https://www.hrw.org/report/2015/05/13/tiger-chairs-and-cell-bosses/police-torture-criminal-suspects-china.

[184] PEN America, "Chinese Writers React to Crackdown," February 25, 2011, http://bit.ly/1OvBtOi.

[185] CHRD, "Deprivation of Liberty and Torture/Other Mistreatment of Human Rights Defenders in China," June 30, 2013, http://bit.ly/1NFNC37.

[186] China Blog Staff, "'Sorry, no comment - we might get invited to tea,'" *China Blog, BBC*, December 9, 2013, http://bbc.

instructed to travel during sensitive political events, effectively keeping them away from their normal online and offline activities.

In July 2015, at least 159 lawyers were interrogated, detained, or disappeared. One human rights lawyer, Wang Yu, reported on July 9 that her internet service and power had been cut off, and shortly thereafter, that people were trying to break into her home. She remained in incommunicado detention as of October.[187]

Technical Attacks

China is a global source of cyberattacks, accounting for 41 percent of the attack traffic observed worldwide by Akamai in 2014.[188] The survey traced the attacks to computers in China using IP addresses, meaning the machines themselves may have been controlled from elsewhere.

Even attacks found to have originated in China can rarely be traced directly to the state, but the scale and targets of the illegal cyber activity have led many experts to conclude that Chinese military and intelligence agencies either sponsor or condone it. 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 2015, China-based attacks targeted international companies including Google, Yahoo, Microsoft, and Apple.[189]

Hackers, known in Chinese 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. From March 25 to March 31, 2015, the hosting service GitHub faced a DDoS attack that crippled its services. Sources indicate that the assault originated in China.[190] The monitoring organization Citizen Lab analyzed the incident and found that "while the attack infrastructure is co-located with the Great Firewall, the attack was carried out by a separate offensive system, with different capabilities and design, that we term the 'Great Cannon.' The Great Cannon is not simply an extension of the Great Firewall, but a distinct attack tool that hijacks traffic to (or presumably from) individual IP addresses, and can *arbitrarily replace unencrypted content as a man-in-the-middle*."[191]

In March 2015, it was revealed that the CNNIC was issuing false digital security certificates for numerous domains, including several owned by Google. This security breach allows for man-in-the-middle (MITM) attacks, in which attackers can impersonate the site for which the certificate was intended, thus acquiring personal and private information.[192] Yahoo faced a MITM attack during

in/1LKxQ0k.

[187] "China's New Crackdown on Civil Rights," *Washington Post*, July 15, 2015, http://wapo.st/1Qq7Jjv.

[188] Akamai, *State of the Internet: Q3 2014 Report,* infographics, http://akamai.me/1LGi8U4

[189] "China Collecting Apple ICloud Data, Attack Coincides with Launch of New Iphone," GreatFire.org blog, October 20, 2014, http://bit.ly/1t5o2dN.

[190] Sebastian Anthony, "GitHub battles 'largest DDoS' in site's history," *ArsTechnica*, March 30, 2015, http://bit.ly/19AxkWX.

[191] Bill Marczak et al., "China's Great Cannon," Citizen Lab, April 10, 2015, https://citizenlab.org/2015/04/chinas-great-cannon/.

[192] Dan Goodin, "Google warns of unauthorized TLS certificates trusted by almost all OSes," *ArsTechnica*, March 24, 2015, http://bit.ly/1EE2uoX.

the 2014 Hong Kong protests,[193] and Microsoft Outlook faced one in January 2015.[194] In April 2015, Google and Mozilla both announced that they would revoke authority of root certificates belonging to the CNNIC,[195] meaning that sites with those certificates would not be recognized by the browsers, potentially interrupting users' connections to a range of sites, including banks and e-commerce platforms.[196]

Another well-documented tactic is spear-phishing, in which customized email messages are used to trick recipients into downloading malicious software by clicking on a link or a seemingly legitimate attachment.[197] Tibetans, Uyghurs, and others subject to monitoring are frequently targeted with emailed programs that install spyware on the user's device.[198] Other cyberattacks affect the broader population.[199]

[193] Netresec, "Verifying Chinese MITM of Yahoo," *Netresec* (blog), October 1, 2014, http://bit.ly/1k3GUYg.

[194] Michael Kan, "Microsoft's Outlook.com faces brief man-in-the-middle attack in China," *PC World*, January 19, 2015, http://bit.ly/1Pse8fT.

[195] Lucian Constantin, "Like Google, Mozilla set to punish Chinese agency for certificate debacle," *PC World,* April 2, 2015, http://bit.ly/1jxt7IX.

[196] Dan Goodin, "Google Chrome will banish Chinese certificate authority for breach of trust," *ArsTechnica*, April 1, 2015, http://bit.ly/1Hlskkq.

[197] Dennis Fisher, "Apple Phishing Scams on the Rise," *Threat Post*, June 24, 2013, http://bit.ly/1OvBTV2.

[198] Dylan Neild, Morgan Marquis-Boire, and Nart Villeneuve, "Permission to Spy: An Analysis of Android Malware Targeting Tibetans," research brief, Citizen Lab, April 2013, http://bit.ly/1OvBOAO.

[199] "Recent Data Breach Events in China," *Privacy and Information Security Law Blog*, December 31, 2013, http://bit.ly/1hDw3Ci.