Freedom House

China

	2015	2016
Internet Freedom Status	Not Free	Not Free
Obstacles to Access (0-25)	18	18
Limits on Content (0-35)	30	30
Violations of User Rights (0-40)	40	40
TOTAL* (0-100)	**88**	**88**

* 0=most free, 100=least free

Population:	**1.371 billion**
Internet Penetration 2015 (ITU):	**50 percent**
Social Media/ICT Apps Blocked:	**Yes**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- A draft cybersecurity law could step up requirements for internet companies to store data in China, censor information, and shut down services for security reasons, under the auspices of the Cyberspace Administration of China (see **Legal Environment**).
- An antiterrorism law passed in December 2015 requires technology companies to cooperate with authorities to decrypt data, and introduced content restrictions that could suppress legitimate speech (see **Content Removal** and **Surveillance, Privacy, and Anonymity**).
- A criminal law amendment effective since November 2015 introduced penalties of up to seven years in prison for posting misinformation on social media (see **Legal Environment**).
- Real-name registration requirements were tightened for internet users, with unregistered mobile phone accounts closed in September 2015, and app providers instructed to register and store user data in 2016 (see **Surveillance, Privacy, and Anonymity**).
- Websites operated by the *South China Morning Post, The Economist* and *Time* magazine were among those newly blocked for reporting perceived as critical of President Xi Jinping (see **Blocking and Filtering**).

Introduction

China was the world's worst abuser of internet freedom in the 2016 *Freedom on the Net* survey for the second consecutive year. Harsh punishments for expression and a deteriorating legal environment are significantly undermining civil society activism on the internet.

"Cyberspace sovereignty" has been a top policy strategy for the Chinese Communist Party (CCP) under its general secretary, President Xi Jinping. Over the past year, the renewed emphasis on information control took the form of laws that sought to codify existing strategies of censorship and surveillance. The National People's Congress drafted a cybersecurity law which could strengthen requirements for internet companies to censor content, shut down their services, register their users' real names, and provide security agencies with user data stored in mainland China. An antiterrorism law passed in December 2015 also introduced scope for abuse, requiring companies to provide technical support to authorities seeking to access encrypted data, and some content controls. An amendment to the criminal law separately penalized spreading alleged misinformation on social media.

Free expression and privacy were undermined through heightened pressure on companies providing internet services and content to comply with censorship orders and user data requests. Regulators introduced new rules for online news outlets, audiovisual content, and digital publishing. Service providers continued to implement real-name registration of all customers, closing down avenues for anonymous communication, and in August 2016, the registration policy was extended to apps which rely on internet connectivity to provide other services. The state even floated a proposal to purchase a one percent share in major Chinese internet companies like Baidu and Tencent in April 2016, another potential avenue of control. Companies who refuse to cooperate are shut out. The website of *South China Morning Post,* Hong Kong's largest English-language newspaper, *The Economist* and *Time* magazine were among those newly blocked in 2015 and 2016.

As in past years, dozens of domestic internet users were investigated for digital crimes from disseminating misinformation to promoting tools to circumvent censorship, and one Uyghur teenager was reported to have been imprisoned for life for watching banned videos on a cellphone.

Against the backdrop of stricter internet control across all platforms, digital activism has been gradually waning. While some individuals are still outspoken, observers noted a decline in the lively discussion of social causes which used to characterize popular microblogs. And in one high profile case, collective action was channeled to further policies that could be used to control information. Internet users successfully forced regulators to impose restrictions on advertising by search engines, after the death of a student who railed against Baidu for promoting an expensive and unproven medical treatment in a sponsored search result. Yet when those regulations on online advertising materialized in late 2016, they also imposed restrictions on the way search engines manage prohibited content.[1]

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-

1 State Administration for Industry and Commerce, SAIC, 国家工商行政管理总局令, July 4, 2016, http://www.saic.gov.cn/zwgk/zyfb/zjl/xxzx/201607/t20160708_169638.html

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 2016 that there were 688 million internet users in China,[2] and the International Telecommunication Union estimated internet penetration at 50 percent in 2015.[3] 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).[4] Though the digital divide between urban and rural areas narrowed marginally in 2014, 71.6 percent of users are based in cities, according to the most recent government figures.[5] Penetration rates significantly vary by province, from Beijing (76.5 percent) to Yunnan in the southwest (37.4 percent).[6] The CNNIC continued to report a small gender gap among internet users, with males making up 53 percent of the total.

Mobile replaced fixed-line broadband as China's preferred means of accessing the internet for the first time in 2012. From December 2014 to December 2015, the mobile internet population grew from 557 million to 620 million, accounting for 90 percent of all internet users.[7]

Though demand is 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 2015, at 17.5 percent.[8]

Costly and inefficient fixed-line broadband service has contributed to the shift toward mobile. 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.[9] A "Broadband China" government strategy issued in 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.[10]

The reality is more complicated. At the end of 2015, the CNNIC reported that the average domestic fixed-line broadband download speed across the country increased from 4.25 Mbps to 8.34 Mbps in 2014. The highest available rate was in Shanghai, which averaged 11.3 Mbps, while the lowest was in

2 China Internet Network Information Center (CNNIC),中国互联网络发展状况统计报告 [The 37th Report on the Development of the Internet in China], January 2016, http://www.cnnic.cn/hlwfzyj/hlwxzbg/201601/P020160122469130059846.pdf.

3 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," http://bit.ly/1cblxxY; CNNIC reported 50.3 percent 中国互联网络发展状况统计报告.

4 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.

5 CNNIC, 中国互联网络发展状况统计报告.

6 CNNIC, 中国互联网络发展状况统计报告.

7 CNNIC, 中国互联网络发展状况统计报告

8 CNNIC, 中国互联网络发展状况统计报告, [The 37th Report on the Development of the Internet in China].

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

10 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.

Tibet, which averaged 6.21 Mbps.[11] By contrast, Akamai, which measures access to the global internet, registered slower average speeds of 3.7 Mbps, down from 3.8 Mbps in 2014.[12]

In Shanghai, customers of Shanghai Telecom experienced lack of bandwidth and slow connections to overseas websites in 2015. In response, the company offered customers an "International nitrogen cylinder plan" which tripled the cost of access to overseas websites, possibly to offset the cost of more affordable access to domestic content.[13]

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.[14] All service providers must subscribe via the gateway operators under MIIT oversight. In March 2016, MIIT announced a draft regulation on domain name management (*hulianwang yuming guanli banfa*). The regulation requires that all domain name holders must go through a real-name registration process, and domain names managed by overseas institutions will not be connected.[15] Foreign media worried that the measure could potentially block all foreign websites,[16] but MIIT clarified that the regulation only applies to websites with Chinese domain names.[17]

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.[18] Since then, authorities have enforced smaller-scale shutdowns, including in March 2016, when network disruptions were reported in western Sichuan province after a Tibetan woman set herself on fire and burned to death in an act of protest against Chinese rule of Tibet.[19]

Some disconnections are more targeted. In November 2015, residents of Xinjiang reported that mobile service was temporarily shut down for those using circumvention tools, those who had not registered their connections using their real names, and those who downloaded foreign messaging software.[20]

Uyghurs, Tibetans, and others who express their opinions about Chinese rule of disputed territory are frequently targeted on the pretext that they threaten national security. For that reason, the introduction in 2015 of legal provisions that could enable network disruptions to prevent terrorism and

11 Broadband and Development Alliance, *China's broadband speed status report* [in Mandarin], http://chinabda.cn/kdfzbg/252261.shtml

12 Akamai, *State of the Internet: Q3 2015 Report*, infographics, https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-state-of-the-internet-report-q3-2015.pdf; Akamai, State of the Internet: Q4 2014 Report, infographics http://akamai.me/1LGi8U4

13 Oiwan Lam, Shanghai Telecom Triples Cost of Access to Overseas Websites, August 11 2015, Global Voices, https://globalvoices.org/2015/08/11/shanghai-telecom-triples-cost-of-access-to-overseas-websites/

14 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.

15 域名管理新规征求意見 調整域名管理體系, http://chinese.gmw.cn/tech/2016-03/28/content_19481218.htm

16 域名须在华注册！中国拟再度收紧网管, http://bit.ly/2fh69aE.

17 工信部回应域名管理新政:不影响外企正常业务http://tech.163.com/16/0330/20/BJEBUA2T000915BF.html.

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

19 Nithin Coca, "The slow creep and chilling effect of China's censorship," The Daily Dot, August 29, 2016, http://www.dailydot.com/layer8/china-tibet-xinjiang-censorship/.

20 Paul Mozur, "China cuts mobile service of Xinjiang residents evading internet filters," New York Times, November 23, 2015, http://www.nytimes.com/2015/11/24/business/international/china-cuts-mobile-service-of-xinjiang-residents-evading-internet-filters.html?_r=0.

protect cybersecurity was cause for concern. Article 84 of the antiterrorism law passed in December introduced fines and detentions of up to 15 days for telecommunications operators and ISP personnel who fail to "stop transmission" of terrorist or extremist content, "shut down related services," or implement "network security" measures to prevent the transmission of such content.[21] A draft cybersecurity law issued for public comment in July 2015 would also provide legal grounds for officials to instruct network operators to stop transmission to protect public security (see Content Removal and Legal Environment).

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.[22] The telecom giants revised their inter-network pricing structures to allow rivals to access their infrastructure,[23] and customers can now choose from among many small local, private internet service providers (ISPs).[24]

State-owned China Mobile, China Telecom, and China Unicom dominate the mobile market. In 2014, the government formally authorized the three major players to set pricing for services according to market forces, resulting in price cuts.[25] Private capital was allowed to enter the network leasing business during the coverage period. By November 2015, the MIIT had issued 42 network leasing licenses to private companies.[26] In some cities, municipal governments proposed regulations to ensure telecommunication market diversity so that residents within a single community could have a choice of telecommunications providers.[27]

Despite the gradual lifting of longstanding market control, network leasing represents only a small part of the telecommunication business. Licenses for basic telecommunications services are still monopolized by the three state-owned enterprises, and no other companies are involved in other key services such as public network infrastructure construction.[28] In May 2016, China Broadcast Network

21 Drew Foerster, American Bar Association, "China's Legislature Gears Up to Pass a Sweepingly Vague Cybersecurity Law," May 2, 2016, http://www.americanbar.org/publications/blt/2016/05/02_foerster.html; "Counter-Terrorism Law (2015)," *China Law Translate,* December 27, 2015, http://bit.ly/2eZydih.

22 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.

23 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.

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

25 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.

26 工信部支持民资进入转售业务 打破垄断发文还不够, [MIIT supports private capital entering network leasing business, more antimonopoly policy is needed] http://it.sohu.com/20151230/n432995626.shtml.

27 重庆出台电信新规 想用哪家宽带用户可自主选择, March 2, 2016 http://cq.cqnews.net/html/2016-03/02/content_36455828.htm

28 中国广电成第四大运营商 业内称其仅拿到半个牌照 , May 6, 2016, http://finance.sina.com.cn/chanjing/gsnews/2016-05-06/doc-ifxryhhi8426724.shtml

(CBN) received a license for basic telecommunications business from MIIT,[29] but since it only provides landline service, it does not represent a threat to the three dominant players.[30]

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.[31] In practice, control can be difficult to enforce. The Ministry of Culture reported 14,000 illegally-operated internet cafés (*hei wangba*) in operation nationwide as of 2014.[32] In November 2014, the Chinese government loosened restrictions on opening new cybercafes, lifting a 2013 requirement that they had to be run by chain stores.[33]

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 (State Internet Information Office) SIIO was created in May 2011 to streamline regulation of online content, punish violators, and oversee telecommunications companies.[34] On August 26, 2014, the State Council formally authorized the SIIO to regulate and supervise internet content.[35] In December 2014, it launched a new website as the Cyberspace Administration of China (CAC) and Office of the Central Leading Group for Cyberspace Affairs.[36] After the coverage period of this report, Lu Wei, who commentators referred to as China's internet czar, was unexpectedly replaced as head of the CAC by Xu Lin, a former deputy of Xi Jinping.[37]

The CAC has an organizational affiliation to the Central Internet Security and Informatization Leading Group that was formed in February 2014 to oversee cybersecurity directly under Xi Jinping, making it the highest authority on internet policy in China.[38] In December 2014, the leading group took charge of the CNNIC, which issues digital certificates to websites.[39]

Two regulatory bodies, the State Administration of Radio, Film, and Television (SARFT) and the Gen-

29 广电国网获得基础电信业务经营许可, May 10, 2016, http://www.sarft.gov.cn/art/2016/5/10/art_114_30759.html

30 中国广电获批基础电信业务牌照 暂难撼动三大运营商, May 6, 2016, http://finance.sina.com.cn/roll/2016-05-06/doc-ifxryhhi8423048.shtml

31 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.

32 Jamie Fullerton, China Has Had Enough of Its Illegal Internet Cafés, December 8 2015, http://motherboard.vice.com/read/china-has-had-enough-of-its-illegal-internet-cafs

33 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.

34 "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.

35 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.

36 Office of the Central Leading Group for Cyberspace Affairs website, http://bit.ly/1OzUsFS; David Feng, "Chinese Cyber Administration Office Goes Online," *Tech Blog 86*, December 31, 2014, http://bit.ly/1LMezBS.

37 China File, "A Grim Future for Chinese Web Freedom," *Foreign Policy, July 1, 2016,* http://foreignpolicy.com/2016/07/01/a-grim-future-for-chinese-web-freedom-lu-wei-internet-china/

38 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.

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

eral 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).[40] The body's tasks include monitoring internet-based television and online videos. In addition, the Central Propaganda Department oversees the ideological inclination of online content.

In March 2016, Xinhua reported the establishment of the non-profit Cyber Security Association of China to promote online security.[41] It is made up of more than 200 member technology and cybersecurity companies, research institutions, and headed by Fang Binxing, who is recognized as the developer of the Great Firewall.[42]

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, discussions of politically and socially sensitive topics, and the authorities' treatment of ethnic minorities. Routine censorship is reinforced during politically sensitive events or in response to breaking news. During the coverage period, online entertainment and user-generated news reports were subject to heightened censorship and punishment. The heavily manipulated online environment still provides space for average citizens to express themselves or criticize the state than any other medium in China, but the frequency and the scale of digital activism were weakened over the years.

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. The most censored news topics in 2015 were health and safety, economics, official wrongdoing, media censorship, the reputation of the party or officials, and civil society.[43] During a military parade in September, an image of Winnie the Pooh in a toy car was heavily censored because the image was used as a spoof of President Xi Jinping.[44] In the aftermath of a series of deadly explosions at a container storage station at the port of Tianjin on August 12, 2015, websites and social media accounts were closed and at least two internet users were detained for posting misinformation online.[45]

Over the last several years, censors have increasingly blocked international news websites, especially those with Chinese-language websites, for their reporting on corruption and illicit wealth among

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

41 Xinhua, "China's first national NPO in cyber security founded," March 25, 2016, http://news.xinhuanet.com/english/2016-03/25/c_135223674.htm.

42 Austin Ramsy, "Architect of China's 'Great Firewall' Bumps Into It, "*New York Times,* April 7, 2016, http://www.nytimes.com/2016/04/07/world/asia/china-internet-great-firewall-fang-binxing.html.

43 Sarah Cook, "China's most censored news topics in 2015," Freedom House, January 2016, https://freedomhouse.org/article/china-media-bulletin-issue-no-111-january-2016.

44 Tessa Wong, The military parade posts China censored, BBC, 3 September 2015, http://www.bbc.com/news/world-asia-china-34137519

45 天津爆炸受害业主连日请愿 网民因造谣被行政拘留, August 17, 2015, Radio Free Asia, http://www.rfa.org/mandarin/yataibaodao/meiti/yf1-08172015100130.html

high-level officials, as well as a range of other issues thought to challenge the government. At least 15 of 18 global news websites tracked by the nonprofit news organization ProPublica were inaccessible inside China as of mid-2016.[46] Websites of *The Economist* and *Time* magazines were newly blocked during the coverage period of this report, apparently in reprisal for critical coverage of Xi Jinping.[47]

In April 2016, the International Consortium of Investigative Journalists released the Panama Papers, confidential documents containing the identities of shareholders of more than 214,000 offshore companies. The documents named relatives of at least eight current or former members of China's top leaders, including Deng Jiagui, brother-in-law of Xi Jinping. Discussion of the Papers was quickly purged from Chinese websites.[48]

In March 2016, the website of *South China Morning Post*, the largest English newspaper in Hong Kong, was blocked and social media accounts affiliated with the paper were disabled.[49] The paper has faced periodic censorship before, including during Umbrella Revolution protests that shook Hong Kong in autumn 2014.[50] The reason for the latest incident was not clear, though the paper had reported on allegations that Chinese security agents abducted Hong Kong-based booksellers to face criminal charges in China, after publishing books perceived as critical of Xi Jinping.[51] It had also published a column linking Xi's political strategy to Mao Zedong's Cultural Revolution, according to international news reports.[52] The block came a few months after the Alibaba Group, a Chinese e-commerce company, purchased media assets owned by the SCMP group, including the *South China Morning Post*, in December 2015, prompting concerns about its editorial independence.[53] In mid-2016, the site was still blocked.

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.[54]

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

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

47 Josh Horwitz, "The Economist's website is now censored in China—and all it took was one satirical cover," *Quartz,* April 7, 2016, http://qz.com/655995/the-economists-website-is-now-censored-in-china-and-all-it-took-was-one-satirical-cover/; Emily Feng, "China Blocks Economist and Time Websites, Apparently Over Xi Jinping Articles," *New York Times,* April 9, 2016, http://www.nytimes.com/2016/04/09/world/asia/china-blocks-economist-time.html.

48 Tom Phillips, All mention of Panama Papers banned from Chinese websites, April 5, 2016, The Guardian, http://www.theguardian.com/news/2016/apr/05/all-mention-of-panama-papers-banned-from-chinese-websites

49 中国网信办回应《南华早报》中文帐号被删, March 11, 2016, BBC, http://www.bbc.com/zhongwen/simp/china/2016/03/160311_china_scmp; http://www.reuters.com/article/hongkong-china-newspaper-idUSL1N16J06R.

50 Patrick Frater, "China Extends Media Blocking as Hong Kong Protests Swell," *Variety,* 2014, http://variety.com/2014/biz/asia/china-extends-media-blocking-as-hong-kong-protests-swell-cyberwarfare-alleged-1201319136/

51 中国网信办回应《南华早报》中文帐号被删, March 11, 2016, BBC, http://www.bbc.com/zhongwen/simp/china/2016/03/160311_china_scmp.

52 Heather Timmons and Zheping Huang, "Hong Kong's SCMP is being blocked in China for cheering on Xi Jinping," March 10, 2016, http://qz.com/635915/hong-kongs-scmp-is-being-blocked-in-china-for-cheering-on-xi-jinping/

53 David Barboza, "Alibaba Buying South China Morning Post, Aiming to Influence Media," *New York Times*, December 12, 2015, http://www.nytimes.com/2015/12/12/business/dealbook/alibaba-scmp-south-china-morning-post.html?_r=0.

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

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.[55] 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.

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.[56]

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.[57]

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. In 2014, China boasted the largest number of VPN users in the world, nearly 93 million, according to Global Web Index.[58]

In January 2015, Chinese authorities reported an upgrade to its national firewall that blocked several providers of VPNs, including the U.S.-based StrongVPN and Golden Frog, which is registered in Switzerland. Officials claimed that the upgrade was meant to uphold "cyberspace sovereignty."[59] Users of the Seychelles-based service Astrill have reported connectivity problems in the past two years, and the company announced the possibility of its service being disrupted during the two political meetings. In mid-2016, users in Beijing and Shanghai reported having been unable to use Astrill since early March.[60] Separately, a 2015 amendment to the criminal law offered possible legal grounds for prosecuting circumvention tool developers.[61]

Certain 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, 138 of Alexa's top 1,000 websites in the world were blocked in 2016.[62] These include YouTube, Google, Facebook, Flickr, SoundCloud, and WordPress.[63] Services operated by Google including Google Maps, Translate, Calendar, and Scholar were blocked in 2014;[64] Google Analytics, which provides audience data to website owners, remained operational, according to the London-based

55 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.

56 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.

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

58 Jason Mander, "90 Million VPN users in China have accessed restricted social networks," GlobalWebIndex blog, November 24, 2014, http://bit.ly/1VR9Y0M.

59 "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.

60 翻不过"长城" 两会期间VPN失, June 9, 2016, 参考网，http://www.fx361.com/page/2016/0309/166807.shtml

61 Oiwan Lam, China Is Blocking Circumvention Tools With Help of Cloud Service Providers, Global Voices, January 20 2016, https://globalvoices.org/2016/01/20/china-is-blocking-circumvention-tools-with-help-of-cloud-service-providers/

62 GreatFireChina, https://en.greatfire.org/analyzer.

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

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

Guardian newspaper.[65] Other social media services like the photo-sharing platform Instagram and Viber were blocked during the 2014 Umbrella Revolution.[66] Instagram had already been removed from online Android application stores run by the Chinese services Baidu, Xiaomi, Wandonjia, Qihou360, Tencent, and 91 Wireless in July 2014.[67]

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 the Umbrella Revolution.[68] LinkedIn, which censors briefly blocked in 2011,[69] launched a Chinese-language version in early 2014.

Search requests that include blacklisted keywords also trigger China's censorship apparatus, producing blank or severely limited results. For example, in recent years, the number 535, signifying "May 35th," a popular way to refer to the June 4 anniversary of the Tiananmen Square crackdown, has gone missing on the Chinese internet.[70] In mid-2015, users reported being unable to make digital financial transfers if the amount contained sensitive numbers such as 6.4 yuan, 64 yuan or 89.64 yuan.[71]

Content Removal

The government has generally not been transparent about content controls, telling international reporters in 2013 that "the perception that the government has placed any restrictions on the internet is untrue."[72] Laws passed or pending during the coverage period were more explicit about restrictions implemented in the name of security which could also threaten legitimate speech.

The antiterrorism law passed in December 2015 instructed companies to delete terrorist or extremist content or "close down relevant websites" at the authorities' request, and also to implement "precautionary measures" against the transmission of such content, with possible administrative detentions for noncompliance (see Restrictions on Connectivity and Legal Environment). While international law supports restrictions on content that incites violence in some circumstances, ethnic and religious minority groups in China have been subject to rights violations on grounds that their legitimate dissent amounts to a terrorist or security threat. A draft cybersecurity law released to the public in July 2015 separately stated that the CAC or relevant departments, "where discovering information the release or transmission of which is prohibited by laws [or] administrative regulations, shall re-

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

66 "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 Real Time Report*, *Wall Street Journal*, October 3, 2014, http://on.wsj.com/1hD6Sjq.

67 Instagram內地「被下架」, July 10, 2014, Mingpao, http://bit.ly/2fjRZUk.

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

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

70 Oiwan Lam, Why the Numbers 64, 89 and 535 Are Missing From the Chinese Internet, Global Voices, June 4, 2015, https://globalvoices.org/2015/06/04/a-special-day-when-some-numbers-are-missing-in-the-chinese-internet/

71 Tiananmen Anniversary Makes Money Transfers in China Trickier, June 3, 2015, http://www.bloomberg.com/news/articles/2015-06-03/tiananmen-anniversary-makes-money-transfers-in-china-trickier

72 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.

quest 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."[73] That law was still pending in mid-2016 (see Legal Environment).

Antipornography and antirumor campaigns are a long-standing cover for government censorship of social and political content. On June 8, 2015, the CAC announced that 100 websites and 20,000 social media accounts were shut down during an "anti-internet blackmail and paid content removal" campaign. However, legitimate accounts were also affected: Sina Weibo and Tencent Weibo accounts of human rights lawyer Liu Xiaoyuan were closed on June 4, 2015.[74] Another purge in early 2016 wiped out 580 accounts, including some operated by outspoken celebrities like businessman Ren Zhiqiang, on grounds they had "abused their own influence to attack the party and the government."[75] Ren, a former property developer, had criticized Xi Jinping's media policy to more than 30 million followers in February, and was threatened with expulsion from the party in May.[76]

Censors targeted online entertainment in the past year. In June 2015, the Ministry of Culture announced its 23rd illegal internet "culture activities" list, which focused on animation and cartoons online; eight websites were shut down.[77] In August, 120 songs were banned by the Ministry of Culture for "containing content that promotes sex, violence or crime, or harms public morality," adding them to the list of content for online portals to monitor and delete.[78] SAPPFRT targeted popular drama series after the agency's head of the television drama management division announced that they would be regulated as broadcast television shows.[79] At least six digital series were removed, two of them permanently, due to content deemed to violate the regulations, including violence, indecency, and superstition.[80] In November, SAPPFRT launched a campaign to purge television set top boxes which can receive overseas television signals through the internet, including VOA and the BBC.[81] In April 2016, the regulator required Apple to withdraw the company's iBooks and iTunes stores six months after their launch in China, according to the *New York Times*.[82]

Mobile service providers monitor text messages and delete pornographic or other "illegal" content.[83] Users report receiving blank messages in place of banned keywords, though what content is banned

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

74 中国专项整治网络违规 维权律师微博账户被删, June 9, Radio Free Asia, http://www.rfa.org/mandarin/Xinwen/8-06092015115226.html

75 Anne Henochowicz, "Social Media Purge Goes Far Beyond Ren Zhiqiang," *China Digital Times,* March 1, 2016, http://chinadigitaltimes.net/2016/03/social-media-purge-goes-far-beyond-ren-zhiqiang/

76 Edward Wong, "China Puts a Tycoon, Ren Zhiqiang, on Probation for Criticizing Policies," May 3, 2016, http://www.nytimes.com/2016/05/03/world/asia/china-ren-zhiqiang.html.

77 文化部關停8家違法動漫網站 首次公布動漫"黑名單, June 8, 2015, http://culture.people.com.cn/BIG5/n/2015/0608/c1013-27121959.html

78 Hu Xin, The Day the Music Died: China Blacklists 120 Songs for 'Morality' Violations, August 12 2015, http://blogs.wsj.com/chinarealtime/2015/08/12/the-day-the-music-died-china-blacklists-120-songs-for-morality-violations/

79 "太子妃"被下架 郑晓龙:网剧与电视剧审查标准应一致 January 22, 2016 http://ent.people.com.cn/n1/2016/0122/c1012-28076699.html

80 "太子妃"等热门网剧下架 传广电总局勒令删改重审, People.cn, January 21, 2016, http://media.people.com.cn/n1/2016/0121/c40606-28072084.html

81 广电总局禁令又来了，直播看不了了，电视盒子这是要死了么, Huxiu.com, http://www.huxiu.com/article/131762/1.html

82 Paul Mozur and Jane Perlez, "Apple Services Shut Down in China in Startling About-Face," *New York Times,* April 22, 2016, http://www.nytimes.com/2016/04/22/technology/apple-no-longer-immune-to-chinas-scrutiny-of-us-tech-firms.html?_r=0.

83 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.

appears to vary.[84] Instant-messaging services such as TOM-Skype and QQ include programming that downloads updated keyword blacklists regularly.[85] Other companies employ human censors to delete posts, sometimes before they appear to the public.[86] Experts say staff members receive as many as three censorship directives per day by text message, instant message, phone call, or e-mail.[87] Most come from local propaganda officials.

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.

Authorities warned online news providers of tighter scrutiny in 2015,[88] and threatened the Sina web portal with suspension in April for failing to prevent violations.[89] In May, the agency published a list of news organizations that were "authorized to provide websites for reposting news."[90] Formerly outspoken media outlets under the Nanfang Daily Group, including *Southern Weekend*, *Southern Metro Daily*, and *21st Century Business Herald*, were overhauled in late 2015 to comply with instructions from the propaganda department in Guangdong, reducing the diversity of critical reporting published both in print and on their respective websites.[91] In February 2016, Xi Jinping visited three key state media outlets, the People's Daily, Xinhua Agency, and CCTV, and emphasized the leadership of the Party in state media.[92] In Xi's speech on media policy, he highlighted three points: putting the party first, controlling media of all forms, and making the party's message more appealing.[93]

Not all media remain submissive. Just weeks after Xi Jinping delivered a speech demanding absolute loyalty from the media, Caixin reported on its English-language website that the CAC ordered the removal of an interview they posted on the Chinese website on the issue of free speech.[94] However, that report was later replaced with an unrelated article.[95]

Propaganda officials also manipulate online content, instructing internet-based outlets to amplify

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

85 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/.

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

87 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.

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

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

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

91 中共南方报业传媒集团党委关于巡视整改情况的通报, http://gdjct.gd.gov.cn/xunshizhenggai2015/31829.jhtml

92 时事大家谈：习近平访三大官媒，强调官媒姓党 VOA, February 23, 2016, http://www.voachinese.com/content/VOAWeishi-IssuesandOpinions-20160222-why-xi-jinping-visited-government-news-outlets/3201386.html

93 Xi Jinping visits flagship state media, lays out vision for party control. China Media Bulletin Issue No. 113 March 2016 https://freedomhouse.org/article/china-media-bulletin-issue-no-113-march-2016

94 Chinese magazine challenges government over censorship, http://www.theguardian.com/world/2016/mar/08/chinese-magazine-challenges-government-censorship-organ

95 "Article About Government Censorship of Article About Politician's Complaints of "Frightening" Censorship of Article About Chilling Effects on Speech Gets Censored," *Fei Chang Dao,* March 13, 2016, http://blog.feichangdao.com/2016/03/article-about-government-censorship-of.html.

content from state media. Since 2005, propaganda units at all levels have trained and hired web commentators, known colloquially as the "50 Cent Party," to post pro-government remarks and influence online discussions.[96] 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.[97] Coordinated smear campaigns are used to discredit high-profile government critics.[98]

The work also extends beyond China's borders to social media apps that are actually banned for mainland users, such as Twitter. One 2014 analysis identified over 2,500 "50 Cent" users spreading misinformation on Twitter.[99] In November 2015, the People's Daily was found to have a large percentage of inactive followers, leading observers to conclude that the fake accounts were used to create a perception of popularity. More than 58 percent of the account's supporters had posted fewer than 5 times themselves.[100]

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").[101]

In recent years, "spreading positive energy among society" has become a major propaganda strategy.[102] Local authorities have started to mobilize *ziganwu*, or volunteer commentators, to promote the government's image and refute negative online depictions of the party or government officials.[103] While the 50 Cent Party is maintained by economic interest, *ziganwu* are mobilized by ideology. A document leaked in January 2015 revealed hundreds of thousands of "youth league online commentators" in China's higher-education institutions, tasked with swaying students against supposed Western values.[104] More recruits were being sought.[105] In May 2015, documents leaked online indicated the league had millions of recruits.[106] Nationalism and xenophobia are prominent components of Chinese cyberspace, though censorship that targets rational dissent instead of inflammatory dis-

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

97 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.

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

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

100 克里斯蒂安•谢泼德,中国官媒Twitter账号被疑"僵尸粉"过多, FT中文网 http://m.ftchinese.com/story/001064972

101 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.

102 Oiwan Lam, Chinese Authorities Think Internet Companies Should Reward Netizens Who 'Spread Good News', Global Voices, December 11, 2015, https://globalvoices.org/2015/12/11/chinese-authorities-think-the-internet-could-use-more-positive-energy/

103 Local Chinese Authorities Use Internet Slang 'Ziganwu' in Their Propaganda Recruitments, Global Voices June 15, 2015 https://globalvoices.org/2015/06/15/local-chinese-authorities-use-internet-slang-ziganwu-in-their-propaganda-recruitment/

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

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

106 How China's Online Civilization Army Turned a Youth Street Fight into a Patriotic Struggle, July 30, 2015, Global Voices, https://globalvoices.org/2015/07/30/how-chinas-online-civilization-army-turned-a-youth-street-fight-into-a-patriotic-struggle/

course arguably magnifies their impact. In extreme cases, online quarrels have resulted in real world violence.[107]

Government employees also openly engage citizens in online discussions. In March 2014, the state news agency Xinhua announced a round of internet supervision training courses for officials across government institutions, including the police and the judiciary. The courses offered five qualifications from assistant to senior manager costing 6,800 yuan (US$ 1,108).[108]

Still, political discourse can be vigorous online, even about democracy and constitutional government.[109] This is partly because the leadership redefined democratic governance as "the Chinese Communist Party governing on behalf of the people" in 2005.[110] A certain amount of open discussion also allows officials to monitor public sentiment, debunk "enemy" ideology,[111] 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 2013 report.[112]

Domestic internet firms benefit commercially from the blocking of foreign social media since they gain market share, but they are obliged to prevent banned content from circulating as part of their licensing requirements. Chinese company executives also enjoy political patronage.[113] About a third of mobile internet users used domestic microblogging applications like Sina Weibo and Tencent's Weixin in 2015,[114] though Weibo in particular has suffered due to censorship requirements, and its use to promote social and political causes has declined.[115] 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.[116] During the two meetings (annual plenary sessions of the National People's Congress (NPC) and the National Committee of the Chinese People's Political Consultative Conference (CPPCC) in 2016, the comment function on many official Weibo accounts was disabled by the company's account maintenance team.[117]

Sina's efforts to manage Weibo content are well documented. Staff, reportedly 150 people working

107 How China's Online Civilization Army Turned a Youth Street Fight into a Patriotic Struggle, July 30, 2015, Global Voices, https://globalvoices.org/2015/07/30/how-chinas-online-civilization-army-turned-a-youth-street-fight-into-a-patriotic-struggle/

108 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.

109 Xu Qianchuan, "Constitution Debate Holds Broader Reform Implications," *Caijing*, 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.

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

111 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.

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

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

114 China Internet Network Information Center (CNNIC),中国互联网络发展状况统计报告 [The 37th Report on the Development of the Internet in China], January 2016

115 How China stopped its bloggers Angus Grigg, http://www.afr.com/technology/social-media/how-china-stopped-its-bloggers-20150701-gi34za

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

117 中国两会微博评论被关闭 民众不满遭"噤声", March 7, 2016, Radio Free Asia, http://www.rfa.org/mandarin/yataibaodao/meiti/yf2-03072016102954.html

12-hour shifts,[118] delete individual posts or accounts, often within 24 hours of an offending post, but sometimes long after publication;[119] make published posts visible only to the account owner; and personally warn individual users.[120] Moreover, hundreds of terms have been automatically filtered from Weibo search results over time.[121]

Weibo's fall from popularity began when it was punished with restrictions on some of its functions in 2012 for failing to curb "rumors."[122] 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.[123] Activity on the platform dropped by an estimated 70 percent;[124] one 2014 study said that approximately 5 percent of Weibo users were still active.[125] In January 2014, the CNNIC reported that 38 percent of Weibo users had migrated to Weixin.[126] In 2015, Tencent reported a combined 500 million monthly active users for Weixin and its international equivalent.[127] Weixin users have the option to restrict updates to a closed circle of connections, and can send audio messages that bypass keyword censorship, though it is also subject to monitoring.[128]

On June 1, 2015, internet police units from local governments started a "speech inspection campaign" on major social media platforms including Weibo and Weixin. The campaigns, which built on existing practices but enlisted more police to enforce them, were intended to detect "illegal and harmful information" and "educate and warn" those who violate the law.[129] Separately, the antiterrorism law passed in December 2015 barred social media users from sharing information about acts of terror that could lead to copycat incidents, or spreading "cruel" or "inhuman" images.[130]

Regulations passed or proposed during the coverage period had the potential to further strengthen state control of companies sharing digital content:

- In June 2015, the State Council drafted "Methods of Regulating Audio and Video programming on the Internet (revised version)" (*hulianwang deng xinxi wangluo chuanbo shiting*

118 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.

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

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

121 "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 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.

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

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

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

125 活跃度下降 新浪微博只有5%用户发内容, April 11 2014, http://tech.163.com/14/0411/16/9PIIGA13000915BF.html

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

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

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

129 第二批139家网警执法账号集中上线, August 13 2015, http://media.people.com.cn/n/2015/0813/c40606-27453939.html-voices/

130 Ben Blanchard, "China passes controversial counter-terrorism law," Reuters, December 28, 2015, http://www.reuters.com/article/us-china-security-idUSKBN0UA07220151228.

jiemu guanli banfa).[131] The draft proposed that all internet content providers offering video or audio broadcasting services must have staff responsible for content censorship, or face fines of up to 30,000 RMB. In addition, the regulation restricted news broadcasting online to city-level radio and television stations, essentially banning user-generated news content. It had yet to be finalized by the end of the coverage period.

- In February 2016, the State Administration of Press, Publication, Radio, Film and Television (SAPPRFT) and the Ministry of Industry and Information Technology (MIIT), jointly issued the Online Publication Services Administrative Provisions, which came into effect on March 10, 2016. The provisions clarified restrictions on foreign investment in online publishing activities, and listed requirements for domestic companies to obtain an online publishing permit. As well as compliance with censorship, the requirements included at least eight full time editorial or publishing staff, potentially increasing the cost of sharing content online.[132]
- In April 2016, regulators sought feedback from major Chinese internet companies on a proposal that the state purchase a one percent share in major Chinese internet companies like Baidu and Tencent.[133] Observers said this could strengthen state influence over content distributed by the platforms, but details of how it might work remained unclear at the end of the coverage period.

Despite technical filtering, enforced self-censorship, and manipulation, the internet is a primary source of news and a 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 emails to subscribers in China with news, instructions on circumvention technology, or copies of banned publications. Civil society organizations involved in charity, education, healthcare, 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 can evade keyword sensors. Humorous neologisms, homonyms, and cryptic allusions substitute for banned keywords, forcing censors to filter seemingly innocuous vocabulary like "tiger."[134] 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."[135]

131 信息网络传播视听节目管理办法公开征求意见, June 12 2015, People's Daily, http://legal.people.com.cn/n/2015/0612/c42510-27143264.html

132 Hogan Lovells, "Are Foreigners Banned from Publishing on the Internet in China," May 2016, http://f.datasrvr.com/fr1/716/75489/Final_Publishing_on_Intranet.pdf

133 China Wants to Own Small Stake in Web Firms, http://www.wsj.com/articles/china-wants-to-own-small-stake-in-web-firms-1461781500; http://www.rfa.org/mandarin/yataibaodao/meiti/ql2-05212016120813.html

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

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

Digital Activism

Social media platforms such as Weibo used to be a vibrant space for revealing government official wrongdoings and organize activism for different social causes. Whereas Chinese citizens traditionally trek to the seat of power to present their grievances, digital technologies can offer a way to overcome the geographic, financial, and physical challenges of such petitioning, and microblogs generated a strong sense of empowerment among many Chinese users.[136] Moreover low-level government wrongdoing, once exposed by users, has been punished, with officials frequently singled out for overspending on entertainment or designer watches, a sign of possible corruption.[137]

Against the background of stricter controls across all platforms and public punishments for outspoken internet users, however, activism has been gradually waning since 2013.[138] The word "netizen"—a translation of the Chinese *wangmin*, or citizen of the internet—conveys the legitimate sense of civic engagement associated with online exchanges, but the term was less common in China by mid-2015.[139]

Some collective action still takes place. In March 2016, human rights activists used the internet to organize demonstrations of support for workers in a Shuangya mountain coalmine in Heilongjiang, who were on strike for unpaid wages, though in mid-2016, the campaign had yet to achieve results.[140]

In April 2016, college student Wei Zexi died of a rare form of cancer after receiving questionable treatment from a hospital he found via a promoted search result in Baidu's search engine.[141] Following Wei's death, many Chinese internet users expressed disdain for Baidu's advertising business, referring to the company using a homophone for Baidu meaning "100 poisons." In response to the fury online, the CAC imposed new restrictions on the way search engines promote content in June 2016, outside the coverage period of this report. The regulations also prohibit search engines from providing links to banned content and require them to report websites carrying banned content when they learn of it.[142]

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 in-

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

137 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.

138 中國立法嚴格管控 部落客噤聲接受再教育 http://www.storm.mg/article/57176

139 How China stopped its bloggers Angus Grigg, http://www.afr.com/technology/social-media/how-china-stopped-its-bloggers-20150701-gi34za

140 维权人士发起联署声明支持双鸭山矿工, March 16, 2016, Radio Free Asia, http://www.rfa.org/mandarin/yataibaodao/renquanfazhi/yf1-03162016103722.html

141 China Investigates Baidu After Student's Death From Cancer, New York Times, http://www.nytimes.com/2016/05/04/world/asia/china-baidu-investigation-student-cancer.html;

142 Bloomberg News, "China Tightens Internet Rules for Baidu and Other Search Engines," June 25, 2016, https://www.bloomberg.com/news/articles/2016-06-25/china-tightens-internet-rules-for-baidu-and-other-search-engines.

voked to imprison citizens for their online activity. 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, well-known online commentators accused of spreading rumors online, and even engineers developing internet circumvention tools. 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.

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.

In 2013, 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.[143] Local officials had already detained online whistleblowers for criminal defamation, which carries a possible prison term of three years under "serious" circumstances.[144] 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.[145] Online messages deemed to incite unrest or protest are also subject to criminal penalties under the interpretation.

The legal grounds for criminalizing digital activity were bolstered during the coverage period. Effective November 1, an amendment to the criminal law introduced criminal penalties up to seven years in prison for those who disseminate misinformation on social media.[146] Separately, in December 2015, an antiterrorism law increased pressure on private companies to provide the government with user data and introduced some content restrictions which could limit free expression (See Restrictions on Connectivity, Content Removal, and Surveillance, Privacy, and Anonymity).

In July 2015, the National People's Congress issued a draft cybersecurity law to consolidate the

143 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.

144 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.

145 Human Rights Watch, "China: Draconian Legal Interpretation Threatens Online Freedom."

146 刑法修正案下月起正式实施 微信、微博造谣最高获刑七年, October 28, 2015, Xinhuanet, http://news.xinhuanet.com/legal/2015-10/28/c_1116970714.htm

role of the CAC, which it identified as the principle agency responsible for implementing many of the law's provisions.[147] The draft codified existing restrictions, strengthening self-regulation and real-name registration requirements for internet companies and requiring them to assist security agencies with investigations; and permitting the government to shut down internet connections at times of public security emergencies, and implement censorship (see Content Removal).[148] Caixin's English-language news website commented that the law remains vague and gives government too much control of the internet.[149] A second draft was under consideration in June 2016 but had not been released to the public.[150]

Bloggers and activists occasionally use the law to defend their right to online expression. In December 2014, Liang Zhuqiang from Guangzhou province was detained on charge of inciting state subversion in relation to a QQ group discussing his family's misfortune during the Cultural Revolution. In June 2015, the People's Procuratorate in Guangzhou dismissed the case for lack of evidence. In December, Liang received RMB 41,090 (US$ 6,400) in state compensation for his wrongful detention.[151]

Prosecutions and Detentions for Online Activities

Reporters Without Borders documented a total of 84 netizens in Chinese jails as of September 2015.[152] As of December 2015, 49 journalists were jailed in China, 35 of them internet journalists, according to the Committee to Protect Journalists.[153]

Religious and ethnic minorities face particularly harsh treatment for online activity. In November 2015, Radio Free Asia reported that a Uyghur teenager sentenced to life imprisonment in Xinjiang had "simply watched videos on his cellphone," citing his father. He was detained with classmates at school in 2014, aged 17, for what the news report described as "internet access offences," and was unable to prove that he was a minor at the time of the trial, which may have contributed to the severity of his sentence.[154] At least one other Uyghur man was detained for watching videos on a cellphone; he was reported to have died in custody in June 2016.[155] In 2014, a court sentenced professor, writer, and Uyghur rights advocate Ilham Tohti to life imprisonment in relation to activities on a Uyghur community website he founded.[156] Separately, a court in Guangdong sentenced Liu Mouling

147 Drew Foerster, American Bar Association, "China's Legislature Gears Up to Pass a Sweepingly Vague Cybersecurity Law," May 2, 2016, http://www.americanbar.org/publications/blt/2016/05/02_foerster.html.

148 Gillian Wong, China to Get Tough on Cybersecurity, July 9 2015, The Wall Street Journal, http://www.wsj.com/articles/china-to-get-tough-on-cybersecurity-1436419416

149 Proposed Law Gives Gov't Too Much Control of Internet, Experts Say, July 30, 2015 Caixin Online, http://english.caixin.com/2015-07-30/100834587.html

150 "China moves closer to adopting controversial cybersecurity law," Reuters, June 27, 2016, http://www.reuters.com/article/us-china-cyber-lawmaking-idUSKCN0ZD1E4.

151 男子涉煽动颠覆国家政权被捕，检方因证据不足不起诉并赔偿, December 20, 2015, the Paper, http://www.thepaper.cn/newsDetail_forward_1411135_1

152 Other cases go unreported. Reporters Without Borders, "2015: Netizens Imprisoned," Press Freedom Barometer, accessed September 23, 2015, http://bit.ly/1GuFfjv.

153 2015 prison census: 199 journalists jailed worldwide, https://cpj.org/imprisoned/2015.php

154 Radio Free Asia, "Uyghur Teenager Serving Life Sentence Is Victim of China's Strike Hard Campaign: Father," November 16, 2015, http://www.rfa.org/english/news/uyghur/uyghur-teenager-serving-life-sentence-is-victim-of-chinas-strike-hard-campaign-11162015141753.html

155 Radio Free Asia, "Jailed for Watching Islamic Video, Uyghur Dies in Police Custody," June 13, 2016, http://www.rfa.org/english/news/uyghur/custody-06132016142251.html.

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

to 10 years in prison in September for activities in support of the banned Falun Gong spiritual group, which included accessing related websites.[157]

As in past years, police and prosecutors also targeted individuals who criticized the party or the leadership online. In one high profile example, human rights lawyer Pu Zhiqiang was given a suspended three-year prison sentence on December 22, 2015.[158] He 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., and later 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.[159] Other cases involving criticism of the authorities were documented in 2015 and 2016:

- On June 30, 2015, Liang Qinhui from Guangzhou, who writes online under the name Jiandao, was charged for inciting subversion of the state in relation to a number of online articles criticizing the Communist Party.[160] Liang, who was first arrested on February 4, was sentenced to 18 months in prison on April 8, 2016.

- On April 6, 2016, Tianyou, a well-known online writer in Shenzhen, was detained for five days based on an article about China's first lady Pen Liyuan.[161] Tianyou, a former Sina Weibo user with several hundred thousand followers, had his account closed in 2014.

- On April 20, 2016, human rights defender Wang Jing from Jilin was sentenced to four years and ten months on charge of picking quarrels.[162] Wang is an independent journalist who writes articles for the overseas website *64Tianwang*.

In a more unusual development, Lefu Chen, a Shanghai network engineer, was detained for 28 days on charge of "destroying computer information systems" in June 2015.[163] Commentators said he had publicly promoted circumvention tools before his arrest.[164] Separately in April 2016, police held a Jinan resident in administrative detention for 15 days under the antiterrorism law after he used circumvention tools to download and view ISIS propaganda videos.[165]

Digital activism was also grounds for detention. Police in Inner Mongolia detained at least five herders for up to ten days each in March 2016 for inciting unrest on WeChat, according to the New York-based Southern Mongolian Human Rights Information Center.[166] More than 100 herders had gathered to protest mining activities they said polluted grazing lands.

157 被告人刘某玲犯利用邪教组织破坏法律实施罪一案一审刑事判决书, http://wenshu.court.gov.cn/content/content?DocID=6052790d-3882-4fec-a130-d262b38734b2

158 中國維權律師浦志強 判刑3年緩刑3年, http://news.ltn.com.tw/news/world/paper/942887

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

160 网络作家"尖刀""煽颠罪"移送法院, June 30, 2015, Radio Free Asia, http://www.rfa.org/mandarin/yataibaodao/renquanfazhi/ql1-06302015102048.html

161 曾批彭麗媛如武則天 深圳作家被拘, http://udn.com/news/story/7331/1618493

162 "保护记者委员会"谴责中国重判记者王晶入狱, http://www.rfa.org/mandarin/Xinwen/1-04262016110404.html

163 研究翻墙软件被刑拘 陈乐福取保候审获释June 30, 2015, Free Radio Asia, http://www.rfa.org/mandarin/Xinwen/7-06302015115424.html

164 http://twister.net.co/?p=515; https://twitter.com/wenyunchao/status/608037838131761153

165 中国首次动用"反恐法" 济南男子翻墙观看ISIS视频被拘, http://www.rfa.org/mandarin/yataibaodao/shaoshuminzu/xl3-04272016101815.html

166 SMHRIC, "Crackdown escalates, more herders arrested for "inciting illegal gatherings via the Internet," March 24, 2016, http://www.smhric.org/news_595.htm; 微信声援被抓牧民 5名内蒙古牧民亦被扣, http://chinaexaminer.bayvoice.net/gb/people/2016/03/25/227309.htm

Authorities reported "punishing" nearly 200 internet users for spreading rumors in connection with major news events in 2015.[167] At least some were detained. Examples during the coverage period include human rights activist Wang Jianyin, who in June 2015 was detained for ten days in Nanjing for posting his opinion on the Tiananmen Square crackdown.[168] Kong Xiangde, an internet user from Anhui Province, was detained for ten days for allegedly posting misinformation about the judge who tried the case of Bo Xilai, the Chongqing party chief purged in 2012.[169] On July 6, an internet user from Guangzhou posted alleged misinformation about an explosion at a local nuclear plant on Weibo. He was detained for five days.[170]

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.[171]

In a more positive development in November 2015, the authorities reduced the seven year sentence of 70-year-old journalist Gao Yu, a contributor to the German news outlet Deutsche Welle, by two years and permitted her to serve the sentence at home.[172] Authorities detained Gao in April 2014 and tried her in November that year for leaking state secrets to a foreign website.

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.[173]

Chinese authorities abolished the extrajudicial sentence known as reeducation through labor in 2013 after domestic calls for reform.[174] However, individuals can be detained without trial under similarly poor conditions in drug rehabilitation and "legal education" centers.[175]

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 main-

167 China 'Punishes' Nearly 200 People for Spreading Rumors, August 31, 2015, the Wall Street Journal, http://blogs.wsj.com/chinarealtime/2015/08/31/china-punishes-nearly-200-people-for-spreading-rumors/

168 南京维权人士涉六四言论被捕 南宁异议人士六四绝食拘十日, June 5 2015, Radio Free Asia, http://www.rfa.org/mandarin/yataibaodao/renquanfazhi/ql1-06052015104649.html

169 安徽籍男子编造"薄熙来案一审审判长自杀"谣言，被行拘十日, June 11, the Paper, http://www.thepaper.cn/www/v3/jsp/newsDetail_forward_1340833

170 广州网民散布"大亚湾核电站爆炸"谣言被拘留5天, July 9, 2015, China News Net, http://www.chinanews.com/gn/2015/07-09/7395257.shtml

171 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.

172 The Initium, November 24, 2015. https://theinitium.com/article/20151124-dailynews-Gaoyu/

173 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.

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

175 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.

tained vague language that is open to abuse by police and security agents.[176] Dozens of human rights lawyers, including many representing clients in freedom of speech cases, disappeared or were held in undisclosed locations in 2015.[177]

Surveillance, Privacy, and Anonymity

In December 2015, China passed an antiterrorism law pending since November 2014.[178] The law contained no requirement for technology firms to provide the government with surveillance "back doors" and supply law enforcement agencies with encryption keys and user data, controversial specifications that were included in a public draft.[179] The law also dropped the requirement that online service providers and telecommunication companies store their user data within China's borders,[180] though localization requirements may be implemented as part of the pending cybersecurity law.[181] In late 2015, the China Information Technology Security Evaluation Center requested U.S. technology companies pledge not to harm the national security of China, including storing data on Chinese users within China, in language similar to the antiterrorism law, but it is not clear if any did so.[182] The antiterrorism law did require companies to offer technical support to decrypt information at the request of law enforcement agencies. Regulations for the Administration of Commercial Encryption dating to 1999, and related rules from 2006, separately require a government regulator to approve encryption products used by foreign and domestic companies.[183]

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,[184] especially since some verification is done through a little-known, government-linked contractor.[185]

In 2012, the National People's Congress Standing Committee approved new rules to strengthen the

176 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.

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

178 http://www.nytimes.com/2015/12/28/world/asia/china-passes-antiterrorism-law-that-critics-fear-may-overreach.html

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

180 反恐法对互联网企业的冲击有多大？December 29, 2015, http://www.globalview.cn/html/societies/info_8191.html

181 "China moves closer to adopting controversial cybersecurity law," Reuters, June 27, 2016, http://www.reuters.com/article/us-china-cyber-lawmaking-idUSKCN0ZD1E4.

182 Paul Mozur, 中国要求美国科技公司服从政府管控, September 17 2015, The New York Times, http://cn.nytimes.com/technology/20150917/c17pledge/; Netizen Report: China Joins Russia in Crusade to Keep User Data at Government's Fingertips, September 24 2015, Global Voices, https://globalvoices.org/2015/09/24/netizen-report-china-joins-russia-in-crusade-to-keep-user-data-at-governments-fingertips/

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

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

185 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.

legal basis for real-name registration by websites and service providers.[186] 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.[187] Comment sections of major news portals, bulletin boards, blog-hosting services, and email providers already enforced some registration.[188] The MIIT also requires website owners and internet content providers to submit photo identification when they apply for a license, whether the website is personal or corporate.[189] 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.[190]

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.[191] 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.[192] 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.[193] In summer 2014, authorities 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.[194] The government announced plans to begin enforcing real-name registration on all websites beginning on March 1, 2015. Alibaba, Tencent, Baidu, Sina Weibo, 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.[195]

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

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

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

188 "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.

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

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

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

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

193 Han, "Manufacturing Consent in Censored Cyberspace."

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

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

services.[196] 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.[197]

Though not consistently enforced in the past, a crackdown on real-name registration for existing mobile subscriptions began in early 2015,[198] and was further tightened during the coverage period. Batches of unregistered mobile phone accounts were scheduled for closure starting in September 2015,[199] causing residents in Beijing to line up for registration in late August; about 40 percent of mobile phone users were not registered according to the real-name requirements.[200] Also in September, multiple virtual network operators in Fujian started to strengthen registration, requiring users to upload a photo showing their face and national identification card.[201]

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.[202] 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."[203]

Chinese providers are required to retain user information for 60 days, and submit it to the authorities upon request without judicial oversight or notifying users.[204] In 2010, the National People's Congress amended the State Secrets Law,[205] obliging telecommunications operators and ISPs to cooperate with authorities investigating leaked state secrets or risk losing their licenses.[206] 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.[207]

In January 2016, the deputy chief of the State Post Bureau announced that a mobile phone app will be developed this year to ensure real-name registration of express deliveries. Consumers will have to use the app to provide their mobile phone number and national ID number before sending out express mail. This signaled a wider trend that could undermine privacy. In June 2016, outside the

196 "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.

197 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.

198 "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.

199 "史上最严"实名制要来：不实名按批次停机, August 27, 2015, http://news.mydrivers.com/1/444/444390.htm3

200 北京：9月起手机实名认证 补办登记排长队, August 30, 2015, CCTV.com, http://news.cntv.cn/2015/08/30/VIDE1440864239598471.shtml

201 福建省虚拟运营商实行实名认证 老用户也将进行认证, September 29 2015, http://www.mnw.cn/news/fj/995822.html?pooc

202 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.

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

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

205 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.

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

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

coverage period of this report, CAC issued regulations requiring app providers from the mainland to adopt real-name registration for their users and keep user activity logs for 60 days. The regulation will take effect from August 1, 2016.[208]

Privacy protections under Chinese law are minimal. In the words of one expert, the law explicitly authorizes 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.[209]

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.[210] 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.[211] Given the secrecy surrounding such capabilities, however, they are difficult to verify. During the coverage period the public security bureau in Lianyungang, Jiangsu Province developed a new mobile phone application for real-name registration in cybercafes. All 426 cybercafes in the city adopted the application, which was planned for use nationwide.[212]

As with censorship, surveillance disproportionately targets individuals and groups perceived as anti-government. 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 were required to install software that provides police with real-time electronic records on transactions.[213]

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.[214]

208 He Huifeng, Nectar Gan, All mainland app providers ordered to keep user logs for months to curb spread of 'illegal information', June 28, 2016, South China Morning Post, http://www.scmp.com/news/china/policies-politics/article/1982756/all-mainland-app-providers-ordered-keep-user-logs

209 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.

210 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.

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

212 江苏连云港警方首创网吧实名认证App, September 20, 2015, Xinhuanet, http://news.xinhuanet.com/politics/2015-09/20/c_128248099.htm

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

214 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.

During the coverage period, family members of online journalists and activists were subject to criminal investigations apparently launched in retaliation for digital activity. In August, 2015, two brothers of the Radio Free Asia journalist Shohret Hoshur, who is based in the U.S., were charged with endangering state security and leaking state secrets. Shohret Hoshur, who covers news affecting Uyghurs in Xinjiang, told the International Federation of Journalists that his brothers are not politically active and had been detained in relation to his work.[215] Separately, in March 2016, German-based journalist Chang Ping and New York-based digital rights activist Wen Yunchao reported family members had been detained in connection with their alleged roles commenting on, or distributing, an anonymous online letter calling for Xi Jinping's resignation.[216]

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.[217] While there are several cases of long-term house arrest, the circumstances and degree of confinement can be adjusted arbitrarily over time. Dissident and human rights lawyer Gao Zhisheng, who published an online letter criticizing the jailing of activist Guo Feixiong in April 2015, stopped communicating with supporters in December 2015, indicating a possible escalation of his punishment.[218] Gao has been under house arrest since 2014. 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.[219]

Law enforcement officials frequently summon individuals for questioning in relation to online activity, an intimidation tactic referred to euphemistically as being "invited to tea."[220] In December 2015, human rights activist Xu Lin reported having been abducted by plain clothed security agents in Guangzhou for eight hours in relation to songs about defending human rights he had composed and distributed online.[221] In a separate case, Lifa Yao, an independent candidate for the local people's congress election in Hubei, was "invited to tea" with security agents so that he could not participate in online lectures on local elections he organized through QQ in August 2015.[222] Activists have also been instructed to travel during sensitive political events, effectively keeping them away from their normal online and offline activities.

University professors were subject to disciplinary proceedings in reprisal for online activity during the coverage period. In Guangdong, a professor in the English department was fired for posting

215 China's Great Media Wall: The fight for freedom, International Federation of Journalists, http://www.ifj.trynisis.com/fileadmin/documents/IFJ_2016_English.pdf

216 Agence France-Presse, "Dissidents say China relatives released in letter probe," *Daily Mail,* March 30, 2016, http://www.dailymail.co.uk/wires/afp/article-3515212/China-dissidents-brother-denies-politics-arrest-media.html. Wen Yunchao contributed to the China chapter of the 2015 edition of *Freedom on the Net.*

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

218 Dissident Chinese Lawyer 'Incommunicado' After Online Anger Over Activist's Sentence, December 2, 2015, Radio Free Asia, http://www.rfa.org/english/news/china/china-gaozhisheng-12022015095428.html

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

220 China Blog Staff, "'Sorry, no comment - we might get invited to tea,'" *China Blog, BBC*, December 9, 2013, http://bbc.in/1LKxQ0k.

221 徐琳：12.17因《大撒币之歌》传唤记, December 26, 2015, http://www.boxun.com/news/gb/pubvp/2015/12/201512260204.shtml

222 大陆民间自发人大普选网路视屏研讨会遭遇国保干扰, http://chinaexaminer.bayvoice.net/gb/truth/2015/08/28/166158.htm

"improper" opinions on the internet in July 2015.[223] In October, Shaanxi university lecturer Feng Honglian, known online as Wumian, was informed by the university that her classes were terminated and she was not allowed to leave campus; she had mobilized internet users to demonstrate in front of local government building in March. State security agents told her not to speak out online in exchange for keeping her job.[224] Also in October 2015, a professor from Hunan University was not allowed to continue his class after he created a website promoting Chinese political reform.[225]

Technical Attacks

China is a global source of cyberattacks, accounting for 28 percent of the DDoS attack traffic observed worldwide by Akamai in 2015.[226] The survey traced the attacks to computers in China using IP addresses, meaning the machines themselves may have been controlled from elsewhere. Symantec reported China was the world's largest originator of malicious bot activities (46 percent) in 2015.[227]

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. Hackers based in China were also suspected of carrying out major global cyberattacks during the coverage period, including one against the United States government Office of Personnel Management in which attackers stole the fingerprints of 5.6 million federal employees;[228] and one in December against the Australian Weather Bureau.[229] In October 2015, attacks targeted seven U.S. companies in the wake of the U.S.-China Cyber-Agreement, which Xi Jinping signed in September on a visit to the U.S.[230] Both countries promised not to conduct cyber-enabled theft in the agreement.[231]

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. In one 2015 example, the U.S.-

223 编造政治谣言、发表言论过激博文，广东一英语系副主任被撤职, November 12 2012, the Paper, http://www.thepaper.cn/newsDetail_forward_1395720

224 西安著名网民"无眠"被学校停课 变相监控, October 1, 2015, Radio Free Asia, http://www.rfa.org/mandarin/Xinwen/5-10012015122455.html

225 湖南大学教授个人网站介绍"联邦制"被停课, October 16 2015, Radio Free Asia, http://www.rfa.org/mandarin/yataibaodao/renquanfazhi/ql2-10162015101124.html

226 Akamai, Akamai's state of the internet Q4 2015 report. https://www.stateoftheinternet.com/downloads/pdfs/2015-Q4-cloud-security-report.pdf

227 Symantec Internet Security Threat Report, https://www.symantec.com/security-center/threat-report

228 US government hack stole fingerprints of 5.6 million federal employees, September 23, 2015, the Guardian, https://www.theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprints

229 Robert Hackett, Chinese Hackers Infiltrated Australian Weather Bureau Computers, Report Says, December 2m 2015, Fortune, http://fortune.com/2015/12/02/chinese-hack-australian-computers/

230 美国网络安全公司称，有中国政府背景黑客继续攻击7家美国企业, October 19 2015, Radio Free Asia, http://www.rfa.org/mandarin/yataibaodao/meiti/hc-10192015120641.html; https://www.crowdstrike.com/blog/the-latest-on-chinese-affiliated-intrusions-into-commercial-companies/

231 Adam Segal, The Top Five Cyber Policy Developments of 2015: United States-China Cyber Agreement, Council on Foreign Relations, January 4, 2016, http://blogs.cfr.org/cyber/2016/01/04/top-5-us-china-cyber-agreement/

based website *64Tianwang* suffered repeated cyberattacks throughout the year.[232] It reports on corruption and human rights abuses in China.

In March 2015, the hosting service GitHub faced a DDoS attack that crippled its services. Sources indicate that the assault originated in China.[233] 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*."[234]

Yahoo faced a MITM attack during the 2014 Hong Kong protests,[235] and Microsoft Outlook faced one in January 2015.[236] In April 2015, Google and Mozilla both announced that they would revoke authority of root certificates belonging to the CNNIC,[237] 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.[238]

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.[239] Tibetans, Uyghurs, and others subject to monitoring are frequently targeted with emailed programs that install spyware on the user's device.[240] In December 2015, Reuters reported that attacks attributed to Chinese authorities had targeted Hotmail accounts operated by overseas Tibetans, Uyghurs, and others using phishing software in the past; Microsoft, which owns Hotmail, will inform victims of suspected government hacking attempts going forward, the report said.[241]

232 六四天网、中国舆论监督网再遭攻击, August 18 2015, Radio Free Asia, http://www.rfa.org/mandarin/yataibaodao/meiti/ql2-08182015102821.html

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

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

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

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

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

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

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

240 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.

241 Joseph Menn, "Microsoft failed to warn victims of Chinese email hack: former employees," Reuters, December 31, 2015, http://www.reuters.com/article/us-microsoft-china-insight-idUSKBN0UE01Z20151231