

Flygtningenævnets baggrundsmateriale

Bilagsnr.:	598
Land:	Kina
Kilde:	Freedom House
Titel:	Freedom of the Net 2020 - China
Udgivet:	14. oktober 2020
Optaget på baggrundsmaterialet:	6. januar 2021

Document #2039060

Freedom House

Freedom on the Net 2020 - China

NOT FREE

10

/ 100

A [Obstacles to Access](#) 8 / 25B [Limits on Content](#) 2 / 35C [Violations of User Rights](#) 0 / 40

LAST YEAR'S SCORE & STATUS

10 / 100 Not Free

Scores are based on a scale of 0 (least free) to 100 (most free)

Overview

Conditions for internet users in China continued to deteriorate, confirming the country's status as the world's worst abuser of internet freedom for the sixth consecutive year. Censorship and surveillance were pushed to unprecedented extremes as the government enhanced its information controls, including in response to persistent antigovernment protests in Hong Kong and the coronavirus pandemic that began in the city of Wuhan. Indeed, at the center of the official cover-up that enabled COVID-19 to spread globally were the regime's restrictions on internet freedom, particularly police interrogations of and forced retractions by medical professionals who shared early reports on social media of a SARS-like illness in the city. The intensified internet controls and systematic surveillance evident during the coverage period affected hundreds of millions of internet and mobile phone users, resulting in increased self-censorship. Despite the tighter constraints and risk of criminal penalties, investigative journalists, video bloggers, and ordinary internet users took courageous action to trace the origins of the COVID-19 pandemic, report from within the locked-down city of Wuhan, share information on other sensitive topics, and archive deleted news reports.

China's authoritarian regime has become increasingly repressive in recent years. The ruling Chinese Communist Party (CCP) is tightening its control over the state bureaucracy, the media, religious groups, universities, businesses, and civil society associations. The CCP leader and state president, Xi Jinping, has consolidated personal power to a degree not seen in China for decades, but his actions have also triggered rising discontent among elites within and outside the party. The country's human rights advocates continue to seek avenues for protecting basic rights, despite intensifying restrictions.

Editor's Note: Tibet and Hong Kong are not covered in this report. Certain territories that are assessed separately in Freedom House's Freedom in the World report are excluded from the relevant country reports in Freedom on the Net, as conditions in such territories differ significantly from those in the rest of the country.

Key Developments, June 1, 2019 – May 31, 2020

- According to government figures, China added 49 million new internet users during the coverage period, including 50 million subscribers to fifth-generation (5G) technology for mobile networks—the most in the world (see A1).
- The full spectrum of internet controls were put into effect to police information about the coronavirus outbreak and the government's response to it, including localized internet shutdowns, restrictions on the use of virtual private networks (VPNs), content removals, account closures, criminal penalties, and hundreds of user arrests (see A3, B1, B2, C2, C3, and C7).
- The Hong Kong protests, the 30th anniversary of the 1989 Tiananmen Square massacre, critical reporting on CCP leaders, and the mass detention of Uighur and other Muslims in Xinjiang were among the most heavily censored topics during the coverage period (see B2).
- As a result of intensifying controls, the online presence of independent civil society, human rights documentation, and prodemocracy viewpoints declined. Encouraged by authorities, the volume and aggressiveness of nationalistic voices increased, contributing to more self-censorship (see B4 and B7).

- Despite authorities’ reduced tolerance for online mobilization and the associated threat of criminal penalties, investigative journalists, video bloggers, and their sources took significant risks to trace the origins of the COVID-19 pandemic, identify those responsible for the initial cover-up, and report from within the locked-down city of Wuhan. Many ordinary internet users devised creative methods to share or archive deleted reports (see B4 and B8).
- A wide array of individuals were targeted with legal and extralegal reprisals—including arbitrary detention, torture, and draconian prison terms—for their online activity. In addition to users who shared information about COVID-19 or criticized the government’s response to the pandemic, online journalists, critics of Xi Jinping, supporters of Hong Kong prodemocracy protests, operators of human rights websites, members of ethnic and religious minority groups, and anticensorship activists were imprisoned (see C3 and C7).
- New evidence emerged of Chinese technology companies systematically aiding government surveillance, including through the development of mandatory or semimandatory propaganda and public health mobile phone applications that were found to collect data and transfer it to authorities. Chinese technology firms are also creating “key individual” databases through which security forces in different parts of the country can target certain people for particular scrutiny (see C5 and C6).

A Obstacles to Access

China added a reported 49 million new internet users between June 2019 and March 2020, as well as 50 million 5G subscribers, the most in the world. However, the country’s internet infrastructure and regulatory environment remain tightly controlled by the government and Chinese Communist Party (CCP). In June 2020, after the coverage period, new measures requiring cybersecurity audits for suppliers of “critical information infrastructure operators” came into effect.

A1 0-6 pts

Do infrastructural limitations restrict access to the internet or the speed and quality of internet 5 / connections? **6**

According to the government’s China Internet Network Information Center (CNNIC), there were 904 million internet users in China—representing 64.6 percent of the population—as of March 2020.¹ That figure represents an increase of 49.1 million since June 2019. The number of users reaching the internet via mobile devices grew from 847 million to 897 million between December 2019 and March 2020.

Internet speeds in China ranked below global averages in 2020. The country had a mean download speed of 2.09 Mbps, according to tests conducted by Cable.co.uk, earning it a rank of 200 among the 221 countries tested,² although Chinese government sources reported significantly higher broadband speeds. The speed of the country’s fourth-generation (4G) technology for mobile networks is higher, averaging 24.02 Mbps as of late 2019, although only there were only 128 million 4G users as of March 2020.³ Connection speeds in China are slowed by the government’s extensive censorship apparatus (see B1), which filters all cross-border traffic and makes the loading of content from foreign-hosted websites sluggish.⁴ Internet speeds can vary significantly in different parts of the country. According to government data, the fastest available connections were in Shanghai,⁵ while the slowest were in less prosperous and more heavily censored regions such as Xinjiang.⁶ Nevertheless, in April 2020, Chinese state media reported that broadband services covered more than 98 percent of all administrative villages in China.⁷

Chinese companies have been at the forefront of building and deploying 5G networks. In June 2020, after the coverage period, the Ministry of Industry and Information Technology (MIIT) announced plans to build 600,000 5G base stations by the end of 2020.⁸ As of March 2020, China was home to an estimated 50 million 5G subscribers, the most in the world.⁹

A2 0-3 pts

Is access to the internet prohibitively expensive or beyond the reach of certain segments of the 1 / population for geographical, social, or other reasons? **3**

Internet access is relatively affordable for the average user, but other digital divides limit access for certain populations.

To reduce costs for consumers, state-owned mobile providers China Telecom, China Mobile, and China Unicom cancelled the national data roaming fee as of July 2018.¹⁰ In January 2020, at the urging of the government,¹¹ the three companies further lowered their rates to 5.1 renminbi (\$0.72) per GB.¹²

Though the digital divide between urban and rural areas narrowed marginally in previous years, 71.8 percent of users are based in cities, according to March 2020 government figures.¹³ The CNNIC reported that same month that 51.9 percent of all internet users were male.¹⁴ As of March 2020, 496 million people did not have access to the internet, and 59.8 percent of those lived in rural areas.¹⁵

A3 0-6 pts

Does the government exercise technical or legal control over internet infrastructure for the purposes of 1 / restricting connectivity? **6**

The Chinese government maintains control over China’s gateways to the global internet, giving authorities the ability to cut off cross-border information requests in order to restrict connectivity or access to content hosted on servers outside the country.¹⁶ This arrangement is the foundation for the “Great Firewall,” as the country’s comprehensive internet censorship system is informally known. All service providers must subscribe via the gateway operators, which are overseen by the MIIT. In June 2020, after the coverage period, new Cybersecurity Review Measures came into effect.¹⁷ Under these rules, ¹⁸ all critical information-infrastructure operators must submit purchases of network products and services to a thorough national security review conducted by a government agency.¹⁹

The government has shut down access to entire communications systems in response to specific events. The most dramatic example occurred in 2009, when authorities imposed a 10-month internet blackout in Xinjiang—home to 22 million people—after ethnic violence in the regional capital, Urumqi.²⁰ Since then, the practice has continued sporadically on a smaller scale. In May 2019, several regions reportedly experienced temporary network shutdowns caused by government tests of a new, simplified mechanism for restricting connectivity.²¹ The “one button” shutdown tests affected citizens in Guangdong Province, Shanghai, and Chongqing, among other metropolitan areas, and may have been conducted as a preemptive censorship measure ahead of the 30th anniversary of the Tiananmen Square crackdown on June 4, 1989. In early March 2020, as parts of the country were placed under lockdown due to COVID-19, several reports emerged of localized, temporary connectivity restrictions in districts of Wuhan and in other parts of Hubei province, either in residential or commercial areas.²²

Human rights activists and their families are sometimes subject to targeted network disconnections. For instance, Ding Zilin, one of the founders of Tiananmen Mothers, a group of activists who lost loved ones during the Tiananmen Square protests, was closely monitored in the weeks leading up to the June 4 anniversary in 2019, and her mobile phone connection was reportedly cut off.²³

Network shutdowns are often explained as national security precautions. The cybersecurity law and Article 84 of a 2015 antiterrorism law introduced fines and detentions of up to 15 days for telecommunications firms and internet service providers (ISP), as well as relevant personnel, who fail to restrict certain forms of content including “shut [ting] down related services”(see B3 and C2).²⁴

A4 0-6 pts

Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers? 1 / 6

State-owned China Mobile, China Telecom, and China Unicom dominate the mobile market,²⁵ though the government has authorized new players to enter the sector over the past few years.²⁶ In January 2019, BT (formerly British Telecom) became the first foreign telecommunications company to receive permission to provide internet services across the country.²⁷ Similarly, in August 2019, the Beijing municipal government announced that it would allow foreign firms to invest in virtual private network (VPN) services for other foreign companies operating in the city on a trial basis, although their share would be capped at 50 percent.²⁸

Authorities exercise tight control over cybercafés and other public access points, which are licensed by the Ministry of Culture in cooperation with other state entities.²⁹ In practice, restrictions can be difficult to enforce. Overall, internet cafés are no longer as popular as they once were, although many remain gathering venues for video gamers. The total number of cybercafes was estimated to be between 130,000 and 150,000 in late 2019,³⁰ but the coronavirus outbreak caused many to close temporarily or go out of business, further weakening the industry.³¹

A5 0-4 pts

Do national regulatory bodies that oversee service providers and digital technology fail to operate in a 0 / free, fair, and independent manner? 4

Several government and CCP agencies are responsible for internet regulation at the local and national levels, but the system has been consolidated during Xi Jinping’s tenure, with relevant bodies placed under tighter party control.

The Cyberspace Administration of China (CAC)³² and the CCP’s Office of the Central Leading Group for Cyberspace Affairs—launched in 2014 and reorganized as the Central Cyberspace Affairs Commission in March 2018—oversee the telecommunications sector and regulate internet content.³³ The cybersecurity law in effect since 2017 identified the CAC as the principle agency responsible for implementing many of its provisions.³⁴ The CAC reports to the Central Cyberspace Affairs Commission, a party entity that is headed directly by Xi Jinping, making it the highest authority on internet policy in China.³⁵ Since 2014, the commission has also overseen the CNNIC, an administrative agency under the MIIT that issues digital certificates to websites.³⁶

The CCP has exerted greater control over state regulation of the press, film, radio, and television industries in recent years, including online video and streaming services. Since administrative restructuring occurred in March 2018, more agencies involved in media regulation, including online content, have been directly subordinated to the CCP’s Central Propaganda Department, although several continue to report to the State Council. Regardless, the Propaganda Department plays the leading role with regard to the political and ideological inclination of online content.

Zhuang Rongwen has served as director of the CAC since mid-2018³⁷ and continued in that position during the coverage period, while simultaneously serving as deputy director of the CCP’s Central Propaganda Department.³⁸ Both entities are extremely active issuing rules and instructions regarding technical, legal, administrative, or content dimensions of internet activity in China and ensuring party control.

B Limits on Content

The Chinese government and technology firms deployed the full spectrum of content controls to police information about the coronavirus outbreak and the government’s response, including VPN restrictions, automated deletions, large-scale content removals, and social media account closures. The tighter constraints, increased risk of penalties, and more dominant nationalistic voices encouraged self-censorship and diminished the space for online public mobilization on human rights. Nevertheless, investigative journalists, video bloggers, and ordinary internet users took significant risks to trace the origins of the COVID-19 pandemic, report from within the locked down city of Wuhan, share information on other sensitive topics, and archive deleted news reports.

B1 0-6 pts

Does the state block or filter, or compel service providers to block or filter, internet content? 0 / 6

The Chinese government’s Great Firewall is the world’s most sophisticated internet censorship apparatus. The resources targeted for blocking, including major social media platforms, usually contain criticism of individuals, policies, or events that are considered integral to the one-party system. The breadth of the affected content is constantly growing, leaving Chinese users with access only to a highly censored, monitored, and manipulated version of the internet.

According to GreatFire.org—an anticensorship group tracking filtering in China—as of mid-2020, at least 171 out of the top 1,000 most visited websites and social media platforms around the world were blocked in China.³⁹ Many international news outlets and their Chinese-language websites are blocked. For example, the *New York Times*, Reuters, and the *Wall Street Journal* have been unavailable for years, while the websites of the British Broadcasting Corporation (BBC) were blocked in 2018⁴⁰ and those of the *Washington Post* and the *Guardian* were blocked in June 2019. In October 2019, Quartz reported that its website was blocked in China. The websites of most privately owned and independent Chinese-language news services from Taiwan, Hong Kong, and the Chinese diaspora—such as *Liberty Times* (Taiwan), *Apple Daily* (Hong Kong/Taiwan), *Initium* (Hong Kong), China Digital Times (United States), and New Tang Dynasty TV (United States)—are also blocked, with the exception of a few that closely follow the CCP line. A wide range of other websites that might provide information of interest to Chinese users are also blocked, including those of human rights groups such as Amnesty International, Human Rights Watch, and Freedom House.

Most international social media and messaging platforms are completely blocked in China, including Facebook, WhatsApp, Twitter, Instagram, YouTube, Telegram, Snapchat, Line, and Pinterest, among others.⁴¹ The popular discussion forum Reddit was blocked in August 2018,⁴² while all languages of Wikipedia were blocked in late April 2019, ostensibly as part of the censorship sweep associated with the Tiananmen Square crackdown anniversary.⁴³ Previously, only the Chinese-language version of Wikipedia and individual pages on sensitive topics were inaccessible.⁴⁴ A number of Google services—including Maps, Translate, Calendar, Scholar, and Analytics—remained blocked in 2020. The long-standing blocks on international communications platforms have enabled the exponential growth of local services such as Tencent’s WeChat and Sina Weibo, which are subject to the government’s strict censorship demands (see B2).

Blocks on global search engines also severely limit the content available on the Chinese internet. Google’s search engine has been blocked since 2012,⁴⁵ while the Yahoo search function was blocked in September 2018.⁴⁶ Microsoft’s Bing has generally remained accessible due to its compliance with the government’s censorship requirements.⁴⁷ Nevertheless, Bing accounts for only 2.4 percent of the search engine market in China, which is dominated by the Chinese companies Baidu and Sogou, with their market share as of May 2020 being 71.5 percent and 16.7 percent respectively.⁴⁸

A minority of Chinese internet users (albeit tens of millions of users) are able to access blocked websites with circumvention tools, such as VPNs, that reroute traffic through a server outside the Great Firewall to bypass censorship. VPNs are also essential to businesses operating in China. However, the government has intensified its restrictions on these tools since new regulations in 2017 placed a ban on the use of unlicensed VPNs.⁴⁹ Service providers are barred from setting up VPNs without government approval, and illegal VPN operations have been increasingly targeted for closure or blocking.⁵⁰ Blocks on VPNs typically escalate ahead of high-profile events, such as the 70th anniversary of the founding of the People’s Republic on October 1, 2019.⁵¹ There were also reports of slower connectivity in mid-February as the Chinese government cracked down on free discussion of the coronavirus outbreak.⁵² VPN providers have reported growing technical sophistication deployed in the VPN blocking incidents of the past year.⁵³

B2 0-4 pts

Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content? 0 / 4

The government requires locally hosted websites and internet companies to proactively monitor their content and remove banned material, and they can face severe punishment for failure to comply. Thus, in addition to blocks that occur at the network level, some mobile phone devices and content providers—including foreign-owned ones—were revealed over the past year to be restricting access to banned sites or content. In October 2019, Quartz reported that Apple had since 2017 been blocking a list of sites generated by Tencent on its iPhone browser, restricting websites deemed politically sensitive by the CCP in much the same manner as it would combat malware or phishing content internationally.⁵⁴ In November 2019, news emerged that the stock image firm Shutterstock had implemented a new feature of its search functions for users with a mainland China IP address—removing from search results images

associated with Chinese-government-banned keywords; the effort prompted an employee petition criticizing the change.⁵⁵ In December 2019, Reuters reported that Refinitiv—a financial information provider that distributes news to investors on a trading and analytics platform—had restricted access within China during the summer of 2019 to hundreds of stories about the Hong Kong protest movement or that otherwise cast the Chinese government in an unfavourable light.⁵⁶

Private companies are required to delete significant amounts of information and close user accounts. This results in the outright elimination of certain content from the internet, as opposed to blocking, which leaves the affected sites accessible to users outside China or to those using circumvention tools.⁵⁷ The scale of content removals, website closures, and social media account deletions continued to expand over the past year, reaching new types of platforms and topics that were previously uncensored.

The CAC regularly launches “rectification” and “clean-up” campaigns to pressure websites and social media platforms to more effectively police content. In the context of these campaigns, the CAC has reported several rounds of large-scale website closures and social media account deletions, including: over 11,000 website and 737,000 social media account and chat group closures in 2019; ⁵⁸ 816 website closures and 33,000 social media account or chat group deletions during the first quarter of 2020 for publishing information which had an “extremely vile impact on society;”⁵⁹ and deletion of 6,126 articles and closure of 18,576 accounts in March and April for spreading “fake news,” “rumor mongering,” and harming the reputation of Communist Party figures.⁶⁰ Separately, in 2019, Baidu reported deleting over 53 billion items of “harmful” information from its search engine results,⁶¹ an increase from 50 billion in 2018.⁶²

The terms used by the CAC and reports of accounts and websites closed show that such mass removals and “rectification” campaigns target content recognized internationally as problematic, but also legitimate information on political, religious, and social issues deemed undesirable to the regime. Anecdotal evidence indicates that many accounts of ordinary users sharing information about the emerging coronavirus outbreak and early government attempts to cover it up were shuttered. This fits with a longer-term trend of censors increasingly targeting “self-media,” a category that includes independent writers, bloggers, and social media celebrities. Competing with official state propaganda, self-media accounts have become a major source of independent news for Chinese users. Overall, tens of thousands of these types of accounts have been shut down in the past two years, delivering a major blow to one of the few remaining avenues for independent and critical news and analysis.⁶³

The government tightly regulates which media outlets and journalists are permitted to conduct and publish original reporting, with many websites and popular web portals barred from independent reporting and restricted to republishing content from state-run media or otherwise approved news outlets. Over the past year, the CAC has shut down several news websites and online photo services for violating this or other vague provisions. Thus, in November 2019, the CAC shut down the news website Business Times for conducting journalistic work without a permit,⁶⁴ and closed the financial news aggregator Wallstreetcn.com for breaching cybersecurity laws, without specifying the particular offense.⁶⁵ The following month, the CAC shut down two of China's largest online photo services—C Photos and Visual China Group—for operating without a permit and “illegally” partnering with foreign news organizations.⁶⁶

The authorities apply pressure to Chinese internet companies to tightly enforce censorship regulations or risk suspensions, fines, blacklisting, closure, or even criminal prosecution of relevant personnel. Such pressure has intensified under the cybersecurity law that took effect in 2017. During the coverage period, several major news and online portals were subject to short-term punitive suspensions, leading them to intensify their own efforts to control content. In early 2020, the CAC placed major internet companies like Sina Weibo, Tencent, and Bytedance under tightened supervision and management⁶⁷ in order to create a “good online environment” after ordering them to remove content that involved independent reporting on COVID-19.⁶⁸ From June 10 to 17, 2020, the CAC imposed a suspension of the trending topics list for the popular Sina Weibo microblogging service, saying messages on the platform had been “disrupting online communication order” and “spreading illegal information.”⁶⁹

As the number of smartphone users in China has skyrocketed in recent years, mobile phone apps have increasingly become a focus for censorship, content deletion, and forced removals. In June 2019, companies producing music apps for the Android system—including Lizhi FM, Ximalaya FM, NetEase Cloud Music, and Soul—were punished by the CAC for hosting content considered sexually suggestive or which promoted “historical nihilism” and “superstition,” common euphemisms for historical content diverging from official narratives and unofficial religious or spiritual content.⁷⁰ In November 2019, executives in charge of ByteDance's news aggregator Jinri Toutiao, one of China's largest mobile news apps with 120 million daily users,⁷¹ were told by the CAC to punish personnel after the app's search engine was found to direct users to content criticizing the late Communist Party military hero Fang Zhimin.⁷² In April 2020, the CAC ordered Baidu to further “rectify” the mobile app version of the search engine and remove “illegal” content.⁷³ In February, the CAC ordered app stores to remove Pipi Gaoxiao, a short-video sharing platform, apparently because of clips circulating about the coronavirus outbreak.

During the coverage period, Apple continued to remove apps at the apparent request of the Chinese government, including the app of the Quartz news outlet due to its coverage of the Hong Kong protest movement.⁷⁴ Hundreds of VPN services were expelled from Apple's iPhone App Store in China since 2017⁷⁵ (though many others remain available in the country).⁷⁶ As of August 2020, a website run by the anticensorship group Greatfire.org, which tracks the availability of apps in different countries, had identified 3,487 apps that were unavailable in Apple's China store compared to other app stores, including 148 news apps in China, as well as entertainment, gaming sports, weather, and travel apps.⁷⁷

Faced with increasing state demands, major content-hosting companies have hired more human censors to purge “illegal” material and avoid penalties. Entire departments are often dedicated to content moderation and removals, with personnel controlling content on major apps—like the microblogging platforms Sina Weibo,⁷⁸ China’s top news app Jinri Toutiao,⁷⁹ and live-streaming app Kuaishou⁸⁰—numbering in the thousands. Many companies now outsource their content-removal activities to so-called censorship factories, which pay low-wage workers to identify and delete content deemed objectionable.⁸¹ This new industry has grown rapidly, with one company, Beyondsoft, employing 8,000 workers.⁸² In addition to the growing ranks of human content reviewers, automation is playing an increasingly important role in censorship. The University of Toronto-based research group Citizen Lab in August 2019 revealed image-filtering capabilities on the popular social media platform WeChat that targeted users’ creative efforts to circumvent text-based censorship through image-based commentary.⁸³ People.cn, the online version of the official CCP newspaper *People’s Daily*, has been improving its artificial intelligence-assisted censorship capabilities.⁸⁴ Given the outlet’s close ties to the party and its presumed knowledge of the government’s red lines, People.cn’s censoring services have become a lucrative side business. Other websites and mobile apps, such as Jinri Toutiao, have outsourced their content review activity to People.cn. According to news reports, People.cn’s chairman predicted that content moderation in China will grow to employ one million people over the next three to five years.⁸⁵ As of March 2020, Alibaba and Tencent had also emerged as industry leaders in content moderation and censorship technologies that intentionally target political content, selling the systems to other Chinese companies as well as foreign clients. The systems reportedly err on the side of caution for potentially politically sensitive content, such as even positive references to Xi Jinping.⁸⁶

Security officials have increasingly resorted to harassing and coercing users to delete content, particularly from Twitter, which is blocked in China. A small but savvy community of internet users access Twitter via circumvention tools, enabling participation in the types of conversations that are heavily censored within the Great Firewall. Official media outlets like the *People’s Daily*, China Global Television Network, and Xinhua News Agency actively use Twitter to reach global audiences, as do a growing number of Chinese diplomats and government spokespeople, even as most Chinese internet users are unable to access the platform. Over the past two years, numerous users faced reprisals for their Twitter activities (see C3 and C7), with many forced to delete their posts en masse.⁸⁷

The Chinese authorities have attempted to justify the country’s censorship system by claiming that it targets pornographic or violent content. However, independent studies have repeatedly found that content related to politics, religion, economics, and social movements are a primary focus.

Censored topics often involve breaking news related to the reputation of the party or officials, official wrongdoing, foreign affairs, health and safety, and civil society activism.⁸⁸ Any negative or unauthorized content related to President Xi is heavily censored. There is also consistent and systematic censorship of content that violates long-standing taboos on subjects such as the 1989 June 4th massacre, Taiwanese independence, repression of minorities in Xinjiang and Tibet, and the banned spiritual group Falun Gong. The CCP’s Propaganda Department and its local subsidiaries issue almost daily instructions to news websites and social media platforms on what content to restrict.⁸⁹

One of the most censored topics during the coverage period was the coronavirus pandemic, which first emerged in the city of Wuhan in Hubei Province in December 2019. A brief period of relatively free discussion of the virus took place between January 19 and February 1, 2020. However, the Chinese government and government-owned technology firms then deployed the full spectrum of content-control tools to constrain talk of the virus and its effects.⁹⁰ Users of social media platforms like WeChat had their accounts blocked for publishing even innocuous questions about the state of the viral outbreak.⁹¹ Government directives warned online news platforms that using material taken from self-media accounts was prohibited.⁹² Following the death of the whistleblowing doctor Li Wenliang in early February, censorship instructions were sent out to online platforms warning them against sensationalizing coverage.⁹³ Other censorship directives included orders to websites to delete an article analysing how the Chinese economy could be affected by the World Health Organization (WHO) declaring a pandemic,⁹⁴ and restrictions on content showing law enforcement agents using excessive force while taking actions to prevent the spread of the virus.⁹⁵ Research conducted by the University of Toronto’s Citizen Lab between January and May 2020 identified more than 2,000 keywords related to COVID-19 that triggered censorship on WeChat, likely affecting tens of millions of posts;⁹⁶ the same research team also found evidence of virus-related censorship on the live-streaming platform YY as early as December 2019.⁹⁷ The researchers found that the thematic focus of censored keywords evolved over time, having been initially centered on the outbreak in China and then shifting to refuting global criticism of the Chinese government, and U.S. domestic politics, among other topics.

As more aspects of daily life moved online due to social distancing during the pandemic, online classes on subjects like politics, history, and obstetrics and gynecology were also subject to censorship.⁹⁸ As activists sought to use Zoom to commemorate the 1989 Tiananmen Square massacre in early June 2020, the company terminated sessions or accounts of organizers at the behest of the Chinese government.⁹⁹

Other sensitive events and news developments during the coverage period provoked high levels of censorship, including the 30th anniversary of the Tiananmen Square massacre on June 4, 1989, in which the military opened fire on peaceful prodemocracy protesters in Beijing,¹⁰⁰ and other politically sensitive anniversaries; critical or independent reporting on political and business elites;¹⁰¹ continuing protests against a proposed extradition law and in favour of greater democratic freedoms in Hong Kong, as well as Beijing and Hong Kong governments’ responses;¹⁰² the worsening human rights crisis and mass detention of Muslim minorities in Xinjiang;¹⁰³ and the

May 2020 annual meetings of the National People’s Congress (NPC) and the Chinese People’s Political Consultative Conference (CPPCC), with online discussion of a new national security law for Hong Kong being particularly curtailed.[104](#)

B3 0-4 pts

Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, 0 / or an independent appeals process? 4

Censorship decisions are arbitrary, opaque, and inconsistent, due to weak rule of law in China’s political system and because so many individuals and processes are involved. The impact of content restrictions may vary depending on factors like timing, technology, and geographic region. ISPs reportedly install filtering devices differently, including in the internet backbone or even in provincial-level internal networks.[105](#) Lists of prohibited websites and sweeping censorship directives are periodically leaked, but not officially published. There are no formal avenues for appeal. Criticism of censorship is itself censored.[106](#) There is also no transparency and a lack of opportunity of appeal for users within private companies’ day-to-day censorship in China.

A recent example of the arbitrariness of regulatory decision-making and the ease with which permissions can be reversed was the rollout in September 2019 of a new web browser, Kuniao, reportedly approved by the Ministry of Industry and Information Technology. The browser purported to allow users to bypass internet censorship, though critics suggested that it simply reduced the scope of censorship, rather than allowing people to fully circumvent controls.[107](#) Within two days of its launch, Kuniao’s website crashed from the high demand and was subsequently blocked entirely. Online references to the browser were also deleted, indicating a reversal of the official position on it.[108](#)

Article 84 of a 2015 antiterrorism law introduced fines and detentions of up to 15 days for telecommunications firms and internet service providers, as well as relevant 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.[109](#) The cybersecurity law in effect since 2017 also provides legal grounds for officials to instruct network operators to stop transmission of certain content to protect public security, among other restrictions (see A3 and C2). In July 2019, the Cyberspace Administration of China further introduced draft regulations that would penalize the social credit of internet service and content providers and the responsible personnel if they are deemed to be “seriously untrustworthy” because they did not take necessary actions to prevent the circulation of banned content.[110](#) It appeared that as of October 2020, the regulations had not yet been approved or implemented.

The CAC and other bodies routinely introduce new rules and guidelines to further refine online restrictions, with an increasing focus on user-generated content. For example, in January 2019, the industry group China Netcasting Services Association released new rules to increase censorship and vetting of content on popular platforms for sharing short videos.[111](#) They include 100 detailed categories of banned content, including many forms of potential humor and satire.[112](#) The rules also require at least one human reviewer for every 1,000 videos posted per day.[113](#)

B4 0-4 pts

Do online journalists, commentators, and ordinary users practice self-censorship? 0 / 4

Self-censorship among ordinary users and journalists continued during the coverage period, particularly in response to the increased risk of account closures, real-world reprisals, and legal penalties for online commentary (see B2, C3, and C7). Various forms of online intimidation and verbal abuse by nationalistic netizens against government critics or others perceived to have harmed the reputation of China also contributed to self-censorship during the coverage period.

There is evidence that WeChat users are increasingly self-censoring to preempt the closure of their accounts or other penalties, as the platform continues to shut down people’s personal accounts for sharing information on political, social, religious, or current affairs topics in chat groups.[114](#) With over a billion daily active users, WeChat is relied on for messaging, banking, ride hailing, ordering food, booking travel, and more.[115](#) The app’s critical role in daily life in China, alongside platform moderators’ growing propensity to close accounts rather than delete objectionable posts, has increased pressure on users to self-censor.

Research on the types of content removals on WeChat public accounts (accounts that broadcast post to a large group of followers as distinct from personal accounts used for instant messaging and other functionalities) in 2018 found that the majority of deletions were initiated by the accounts themselves, as opposed to WeChat administrators.[116](#) Self-censorship is pervasive among members of persecuted groups, especially Uighurs, whose WeChat activities are closely monitored. Many block their own family members living abroad to avoid being detained for their foreign contacts.[117](#) In addition to encouraging pervasive self-censorship, this blunt form of punishment has narrowed avenues for civic mobilization and further suppressed online activism (see B8).

Despite these pressures, various examples emerged during the coverage period of internet users speaking out on sensitive topics. Following the November 2019 publication by the *New York Times* of a trove of internal documents on how Chinese authorities built the system of repression in Xinjiang, reports emerged of various Sina Weibo users expressing support and admiration for a local party secretary who was himself investigated for having released between 7,000 and 20,000 detainees from local reeducation camps.[118](#)

More widespread instances of overcoming self-censorship emerged in late January and February 0, when netizens and journalists initially defied government restrictions, shared information and spoke out against censorship during the coronavirus lockdown. Following the outbreak of the coronavirus in Wuhan, netizens openly criticized the

authorities’ initial cover-up of the outbreak and efforts to stifle open discussion of the government response to the crisis, while citizen journalists posted unvarnished videos of events on the ground. In early February, as news of the death of Dr. Li Wenliang spread, the hashtag “I want free speech” began to trend on Weibo, garnering millions of views before being censored within hours.¹¹⁹ Prominent voices also spoke out, with the noted Wuhan-based writer Fang Fang publishing an online diary recounting her experiences living in the city under lockdown, despite repeatedly encountering censorship.¹²⁰

B5 0-4 pts

Are online sources of information controlled or manipulated by the government or other powerful 0 / actors to advance a particular political interest? 4

The government has significant control over digital news media and other information sources. Online discussion is subject to extensive manipulation, and user-generated content is highly regulated. Websites and social media accounts, other than those operated by official news outlets, are not legally allowed to produce news content, though the definition of news is unclear. Propaganda officials systematically instruct internet outlets to amplify content from state media and downplay news that might generate public criticism of the government.¹²¹

On March 1, 2020, new rules called the Provisions on the Governance of the Online Information Content Ecosystem came into effect.¹²² These provisions place online content in three categories: encouraged positive content, discouraged negative content, and illegal content. Encouraged material includes “spreading Party doctrine,” while negative categories include “excessive celebrity gossip” and sensationalist headlines. The illegal category includes terrorist and obscene content, as well as information “harming the nation’s honor and interests,” “subverting” the CCP regime, or challenging the government’s social, ethnic, religious, or economic policies.¹²³ According to the rules, the encouraged content must be actively promoted in prominent online locations such as on web portal home pages, pop-up windows, hot topic lists, default search results, and other “key areas that can easily attract attention.”¹²⁴ They also call for the use of algorithms by online content providers to promote officially approved “mainstream values.”¹²⁵ Most actions required by the provisions have already been occurring for many years, but the new regulations consolidate them into a single set of rules.¹²⁶

Paid web commentators, known informally as the 50 Cent Party, are employed to post progovernment remarks and influence online discussions.¹²⁷ Such commentators are known for reporting users who post offending statements, deliberately muddying the facts of particular incidents,¹²⁸ and coordinating smear campaigns against government critics.¹²⁹ According to a 2017 study, progovernment web commentators are strategically deployed to distract the public from certain issues, with about 80 percent of their posts dedicated to “cheerleading” the government’s activities.¹³⁰ Since 2017, content manipulation and disinformation campaigns have increasingly extended even to platforms that are blocked in China, demonstrating an effort to influence online discourse internationally.¹³¹ The Oxford Internet Institute reported that in 2019, the Chinese government displayed “new-found interest in aggressively using Facebook, Twitter, and YouTube” to spread propaganda and disinformation.¹³²

In addition to paid commentators, local authorities have mobilized *ziganwu*—volunteer commentators motivated by ideology rather than money—to promote the government’s image online.¹³³ This activity forms part of a propaganda strategy to “spread positive energy among society.”¹³⁴ A document leaked in 2015 revealed hundreds of thousands of “youth league online commentators” in China’s higher education institutions, tasked with turning students against supposed Western democratic values.¹³⁵ In 2016, a handful of *ziganwu* were appointed to a social media division of the Communist Youth League.¹³⁶ The league’s new media working group uses Weibo, WeChat, and other social media platforms to tailor political messages for younger audiences.¹³⁷

The government encourages Chinese tech companies to engage in “party-building” efforts to strengthen the “ideological security” of their firms.¹³⁸ Alibaba, Weibo, Jingdong, Baidu, Sohu, Qihoo 360, and LeTV have had CCP branches within their companies since at least 2016, and many smaller enterprises have followed suit.¹³⁹ According to Chinese state media, as of 2018, Alibaba had a CCP committee, nearly 200 party branches, and 7,000 CCP members; its founder Jack Ma is himself a CCP member.¹⁴⁰ One Tencent office projects the number of party members among its employees (over 8,000 in 2018) on the wall, alongside a monthly schedule of party education training sessions offered to employees.¹⁴¹ During the coverage period, senior members of the Ministry of Propaganda and the Central Cyberspace Affairs Commission gave speeches at tech companies encouraging employees to study and help implement government policy.¹⁴²

Government pressure has also led private companies to promote state propaganda through their services. In April 2019, Bytedance signed a strategic cooperation agreement with the Press and Publicity Bureau of the Ministry of Public Security to help deepen the “influence and credibility” of public security bureaus across China.¹⁴³

B6 0-3 pts

Are there economic or regulatory constraints that negatively affect users’ ability to publish content 0 / online? 3

Growing censorship demands, new licensing requirements, and data-localization mandates have made it more expensive to run an internet company in China. While large companies have been able to absorb the rising operational costs, it is increasingly difficult for new and smaller players to enter and stay in the market. Arbitrary regulatory decisions have also contributed to an unstable investment climate for China’s technology sector.¹⁴⁴

Independent news media have been hit especially hard. Under new CAC regulations on managing internet news and information services that came into effect in 2017,¹⁴⁵ only traditional media or state-controlled enterprises may obtain a license to gather or disseminate news in any online format.¹⁴⁶ Regulations in effect since 2016 place restrictions on foreign investment in online publishing and require at least eight full-time editorial or publishing staff members.¹⁴⁷ In addition, CAC rules have made it harder for both independent media and individual bloggers, journalists, and writers to sustain themselves financially.¹⁴⁸ Commercial media outlets such as *Caixin*, known for relatively aggressive and investigative reporting, have suffered from falling profits due to censorship and ad hoc directives requiring major news portals and other aggregators to favor state media. *Caixin* was forced to introduce a paywall in 2017.¹⁴⁹

B7 0-4 pts

Does the online information landscape lack diversity? 1 / 4

China's online information landscape is significantly less diverse than it was even six years ago due to increasing censorship, especially of content produced by civil society activists, investigative journalists, and “self-media.” The robust censorship of critical viewpoints and foreign information sources has also empowered nationalist and conservative voices, contributing to their being disproportionately represented in Chinese cyberspace.¹⁵⁰ Nevertheless, the internet still provides a narrow avenue for critical discussion and enables the sharing of information on some important social and political issues, particularly when users devise creative workarounds.

The stringent penalization of groups perceived as a political threat—including organizations, websites, and social media accounts that address human rights and social subjects such as labor activism, public health, and gender equality—has effectively diminished the space for civil society in recent years.¹⁵¹ While groups that work on less sensitive issues have a vigorous online presence, organizations and topics that were tolerated in previous years—such as feminist groups—have faced increasing scrutiny. In some cases, netizens have been able to evade censorship through the use of wordplay to disguise discussion and expressions of support for activists, such as the prodemocracy protesters in Hong Kong.¹⁵²

Many members of ethnic, religious, and linguistic marginalized groups attempt to use the internet to disseminate banned content, but these views remain underrepresented online and those who post them risk severe reprisals, including imprisonment and torture, if they are identified as the source of content deemed politically sensitive. Amid the human rights crisis in Xinjiang, for example, Uighur-language content and relevant news reporting have been heavily censored and many ordinary Uighur users detained, while Islamophobic commentary is permitted to circulate widely.¹⁵³ In August 2020, after the coverage period, authorities banned the popular Mongolian-language social media platform Bainu amid protests in Inner Mongolia among parents and students over an abrupt and sharp reduction in the number of school subjects to be taught in Mongolian, and their replacement by Mandarin classes.¹⁵⁴

Other, mostly Han Chinese religious and linguistic minority populations are also disproportionately silenced or restricted. Keywords related to the persecuted Falun Gong spiritual group consistently appear on leaked lists of prohibited terms. Reference to the banned Church of the Almighty God spiritual groups are also reportedly marked as politically sensitive by censors employed by mobile phone operators, with users facing account deactivation for sharing religious information.¹⁵⁵ Following the coronavirus outbreak in January 2020, reports emerged of Christian congregations being prevented from conducting live-streamed meetings and of individual parishioners being compelled to delete religious imagery from their social media accounts.¹⁵⁶ Many Cantonese live-streamers using ByteDance's popular Douyin app (the Chinese version of TikTok, which has 400 million daily active users)¹⁵⁷ have been banned for not broadcasting in Mandarin, possibly because the company does not have enough Cantonese-speaking content moderators and is therefore worried that they will not be able to identify objectionable speech.¹⁵⁸

LGBT+ content has been heavily restricted on China's internet since 2017, when the China Netcasting Services Association labelled homosexuality as “abnormal sexual behavior.”¹⁵⁹ The courts have upheld the restrictions despite multiple legal challenges.¹⁶⁰ Access to the overseas fan fiction site Archive of Our Own was blocked in China in February 2020, seemingly for LGBT+ content related to a prominent Chinese actor.¹⁶¹

Despite the tight censorship system, tens of millions of internet users—including from among persecuted minorities—bypass censorship with circumvention technology or creative workarounds. According to a survey by GlobalWebIndex published in 2019, 29 percent of Chinese netizens use VPNs.¹⁶² Researchers found that more than 50 percent of respondents said their motivation was to access entertainment content, but many Chinese also use VPNs to reach news and overseas social media platforms.¹⁶³ Although hundreds of VPN services have been banned since 2017 or expelled from Apple's iPhone App Store in China,¹⁶⁴ various options remain available in the country.¹⁶⁵

Within the Great Firewall, netizens deploy humorous neologisms, homonyms, and cryptic allusions to substitute for banned keywords, forcing censors to filter seemingly innocuous terms like “rice bunny,” which is pronounced “mi tu” in Mandarin and has become a well-known alternative for the intermittently censored #MeToo hashtag.¹⁶⁶ The cartoon character Winnie the Pooh has also been systematically censored since it became a meme used to caricature Xi Jinping.¹⁶⁷ In early 2020, netizens used the term “F4” to refer to the four politicians seen as responsible for the coronavirus outbreak: the governor and party secretary of Hubei province and the mayor and party secretary of Wuhan.¹⁶⁸ During antiextradition protests in Hong Kong in mid-2019, netizens used the phrase “Pearl of the Orient” to discuss developments in the city in order to evade online censors.¹⁶⁹

Although the space for investigative journalism has shrunk dramatically over the past decade,¹⁷⁰ some intrepid reporters continue to expose wrongdoing by companies and officials, focusing on topics that are less likely to draw censorship online and occasionally triggering national conversations. During 2019, journalists broke stories on a chemical plant explosion, corruption in Inner Mongolia, and trafficking in pangolins, many of which circulated online in China.¹⁷¹ In the early weeks of the coronavirus outbreak, investigative journalists, video bloggers, and their sources took significant risks to trace the origins of the pandemic, identify those responsible for the initial cover-up, and report from within the locked-down city of Wuhan.¹⁷² Even after the reporting was censored, internet users devised creative methods—including replacing Chinese characters with emojis and translating an article profiling a doctor in Wuhan into Korean¹⁷³—in order to share important articles or archive deleted materials.¹⁷⁴

B8 0-6 pts

Do conditions impede users’ ability to mobilize, form communities, and campaign, particularly on 1 / political and social issues? 6

The role of social media in providing a vibrant space for activism in China has waned significantly due to stricter internet controls under Xi Jinping.¹⁷⁵ Growing censorship of popular apolitical platforms such as dating, video-sharing, live-streaming, and blockchain applications in recent years has effectively closed avenues users had exploited to disseminate information and mobilize around topics that could not be discussed elsewhere.

A November 2018 CAC regulation requires internet companies “of public-opinion nature” or which have “the capacity for social mobilization” to undergo “voluntary” assessments of how effective they are at preventing “security risks.”¹⁷⁶ Under the regulation, which includes a mechanism for on-site inspections, companies are obliged to keep detailed records of user data, such as real names, internet protocol (IP) addresses, activity logs, and the type of device used (see C6).¹⁷⁷

Activists continue to face harassment, arrest and mistreatment in detention at the hands of the police.¹⁷⁸ Yet while overt activism on political issues is exceedingly rare, China’s #MeToo movement continues to demonstrate that citizens can organize around select social causes, and that their efforts sometimes have a real-world impact. Despite heavy censorship of the global campaign, #MeToo encouraged a number of Chinese students to speak out online about their experiences with sexual harassment (see B7), leading to a few instances of positive change. China’s new Civil Code, released in June 2020, bans sexual harassment,¹⁷⁹ a move seen as a response to numerous cases of professors harassing female students on college campuses across China.¹⁸⁰

Some internet users are finding alternative ways to mobilize and to communicate with one another and the outside world. In August 2019, dozens of short videos by Uighurs emerged on the video-sharing platform Douyin, typically showing a Uighur with a photo of a loved one, who had ostensibly been detained, while silently crying or making mourning gestures. Although many of the clips were deleted within China, they nevertheless spread globally, as Uighur activists shared them on international social media platforms.¹⁸¹

Amid the pandemic, netizens have also used GitHub—a global code-sharing site that is not blocked in China—to save and share material related to the coronavirus and the Chinese government’s response to it. However, the reach of some such repositories was restricted after police detained activists in China managing them.¹⁸² In February and March 2020, Chinese netizens also organized themselves on social media platforms to secure assistance for people who had contracted the coronavirus in Wuhan, as well as frontline healthcare workers.¹⁸³ In other cases, businesses and civil society organizations also made use of the internet to organize support for people in Wuhan.¹⁸⁴ Before new censorship requirements were placed on blockchain platforms in January 2019, users turned to blockchain’s decentralized public ledgers to embed, share, and preserve critical information that is censored on other systems.¹⁸⁵ In March 2020, some users were again able to resort to an Ethereum blockchain transaction to preserve a profile of a Wuhan doctor recalling the days in late 2019 when suspicions of a new SARS-like illness first emerged.¹⁸⁶

C Violations of User Rights

A wide array of individuals were subject to legal and extralegal reprisals—including arbitrary detention, torture, and draconian prison terms—for their online activity. These included users who shared information about COVID-19 or criticized the government’s response to it, online journalists, critics of Xi Jinping, supporters of Hong Kong’s prodemocracy protests, operators of human rights websites, members of ethnic and religious minority groups, and anticensorship activists. New evidence emerged of Chinese technology companies systematically aiding government surveillance, including via provision of “key individual” database technologies and data transfers to police from propaganda and public health mobile phone applications.

C1 0-6 pts

Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that 0 / lacks independence? 6

Article 35 of the constitution guarantees freedoms of speech, assembly, association, and publication, but such rights are subordinated to the CCP’s status as the ruling power. The constitution cannot 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 cases involving freedom of expression. Regulations issued by government and CCP agencies establish censorship guidelines. These are highly secretive, subject to constant change, and cannot be challenged in the courts (see B3). Prosecutors exploit vague provisions in China’s criminal code; antiterrorism laws, laws

governing printing and publications; subversion, and separatism; and state-secrets legislation to imprison citizens for online activity. Trials and hearings typically lack due process. It can take years for cases to move through the court system, and pretrial detention is often long-lasting.

Some detentions, including administrative detentions authorized by public security bureaus, do not require approval by a court.¹⁸⁷ The form of administrative detention known as “reeducation through labor” was abolished in 2013 in response to domestic and international calls for reform,¹⁸⁸ but individuals can be detained without trial under similarly poor conditions in drug rehabilitation¹⁸⁹ and “residential surveillance at a designated location.”¹⁹⁰ Under residential surveillance orders, state agents have abducted and held individuals in secret locations without informing their families or legal counsel.¹⁹¹ In November 2019, a woman was released from an extrajudicial psychiatric detention following her imprisonment without trial in July 2018 for live-streaming herself throwing ink on a picture of Xi Jinping, and denouncing the Communist Party.¹⁹²

C2 0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities? 0 / 4

Numerous laws and regulations place strict limits on the activities of internet users and the companies that provide information and communication technology services. The sweeping cybersecurity law that took effect in 2017 increased censorship requirements; mandated data localization; and codified real-name registration requirements for internet companies and obliged them to assist security agencies with investigations.¹⁹³ The law also consolidated the role of the CAC, which it identified as the principle agency responsible for implementing many of its provisions.¹⁹⁴

Laws prohibiting offenses including defamation, creating disturbances, illegal commercial activities, and extortion have implication for online speech.¹⁹⁵ Defamation has been interpreted to include “online rumors,” content deemed false, or online expression that “seriously harms” public order or state interests.¹⁹⁶ It carries a possible three-year prison sentence under “serious” circumstance, defined to apply when the content in question receives more than 5,000 views or is reposted more than 500 times.¹⁹⁷ Online messages deemed to incite unrest or protests are subject to criminal penalties under provisions punishing citizens for “picking quarrels and provoking trouble.” Crimes such as “subversion” and “separatism” can draw sentences as severe as life in prison, with members of religious and ethnic minorities periodically receiving life sentences when charged.¹⁹⁸ Article 300 of the criminal code punishes “using heterodox religion to undermine implementation of the law” and is often invoked against members of banned religious groups such as Falun Gong, whose members exercise their right to free expression and access to information online.¹⁹⁹ A 2015 amendment to the criminal code increased the maximum penalties from 15 years to life imprisonment.²⁰⁰ The same 2015 legislation introduced penalties of up to seven years in prison for the dissemination of misinformation on social media.²⁰¹

Separately, the 2015 antiterrorism law also barred social media users from sharing information about acts of terrorism or spreading “inhuman” images that could encourage copycat attacks.

In February 2020, in the wake of the coronavirus outbreak, China’s top judicial and law enforcement agencies released new guidelines for judges, prosecutors, and others working in the legal system urging strong action against crimes seen as weakening disease control efforts and undermining the CCP’s authority during the pandemic. Among the ten categories of crimes listed for tighter enforcement was “spreading false information and rumours online.” Besides false information related to the virus itself, the provisions also covered speech deemed to be “disrupting social order, especially maliciously attacking the party and government, taking the opportunity to incite subversion of state power, or overthrow of the socialist system.”²⁰² In addition to calling for punishment of individual users for proscribed speech under relevant provisions of the Criminal Law, the guidelines also warn that network service providers who refuse regulator demands to stop the spread of “false” or other “illegal” information should be prosecuted under the criminal code for not performing “the obligation of information network security management.”²⁰³

C3 0-6 pts

Are individuals penalized for online activities? 0 / 6

Chinese citizens are regularly jailed for their online activities, including advocates of political reform, human rights workers, members of ethnic and religious minorities, and ordinary users who express dissent or mock or criticize CCP leaders, particularly Xi Jinping. Chinese citizens’ risk of being detained or imprisoned for accessing or sharing information online or via smartphone has increased considerably over the past several years. Rapid advances in surveillance technology and growing police access to user data have helped facilitate the rise in arrests and prosecutions (see C6).²⁰⁴

During the coverage period, police detained hundreds of users accused of “spreading rumors” or government criticism related to the coronavirus outbreak. Judges also imposed several long prison sentences on both prominent activists and ordinary users. Though the people imprisoned represent a tiny percentage of the overall user population, prosecutions have a chilling effect on activism and encourage self-censorship in the broader public. This is especially true among communities like Uighur Muslims, where the proportion of detained netizens is greater than among the wider Chinese population.

The culpability of government and party officials in covering up the first evidence of a new pandemic heightened regime insecurity, prompting security agencies to be especially aggressive in punishing users for sharing information about the coronavirus or online criticism of the government’s handling of the crisis. A variety of internet users in

China faced detention, prosecution, and imprisonment over the past year. Perhaps most prominent among them was Li Wenliang, the doctor who in late December 2019 first raised concerns on WeChat about the emergence of a SARS-like illness in Wuhan.²⁰⁵ He and seven of his colleagues were detained by local police for “spreading rumors,” and Li was compelled to sign a letter “admitting” that he had made “false comments” about the virus.²⁰⁶

As of early May 2020, China Human Rights Defenders had documented 897 cases of people being punished for publishing material related to COVID-19.²⁰⁷ with punishments including verbal warnings, fines, administrative detention, and criminal charges. In February 2020, prodemocracy activist Ren Ziyuan was detained for 15 days for criticizing the government's response online²⁰⁸, while activist Tan Zuoren was visited by the police and had his social media accounts frozen for his online comments.²⁰⁹ Police detained women's rights and labour activist Li Qiaochu in February after she tweeted in late January about the Chinese government's attempts to coverup the outbreak of the coronavirus.²¹⁰

Detentions continued throughout the spring. In May, prominent constitutional lawyer Zhang Xuezhong was temporarily detained by police after publishing a WeChat post (which was later deleted) criticizing the Chinese government's response to the coronavirus outbreak and calling for greater political reforms in China.²¹¹ That same month, police in Shanghai arrested citizen journalist Zhang Zhan, who had posted a YouTube video criticizing the government's response to the outbreak;²¹² Zhang was charged in June with “picking quarrels and provoking trouble.”²¹³ Others faced more severe charges. In late January, the academic and former political prisoner Guo Quan was arrested on charges of “inciting subversion” for critical remarks he made online about the government's handling of the virus.²¹⁴

Professional and citizen journalists in China are frequently imprisoned for their work and online writings or video posts, including those who reported on the pandemic and lockdown in Wuhan. According to the Committee to Protect Journalists (CPJ), at least 49 journalists were behind bars in China as of December 2019.²¹⁵ In an unusually harsh sentence for an ethnic Chinese journalist, Chen Jieren was sentenced to 15 years in prison in April 2020 for publishing material critical of the Communist Party and exposing corruption in Hunan Province via WeChat.²¹⁶ In early 2020, security forces in Wuhan detained three citizen journalists—Fang Bin, Chen Qiushi and Li Zehua—who had filmed and uploaded videos of themselves from within the city during the coronavirus lockdown; their videos ran counter to official narratives and were disseminated widely within and outside China.²¹⁷ As of September 2020, Li Zehua and Chen Qiushi had both been released, with Chen reportedly under tight surveillance at his parents home in Shandong Province.²¹⁸

Criticism or questioning the authority of Xi Jinping remains a dangerous online activity. During the coverage period, several activists, lawyers, and a CCP member faced detention or prosecution for overt or veiled critiques of Xi's leadership. Prominent rights lawyer Xu Zhiyong was detained in Guangdong Province on February 15.²¹⁹ Xu had been on the run from authorities since December, when he attended a dinner meeting of activists, but the nationwide effort to track him down appeared to accelerate after he published on social media and blog platforms a scathing letter²²⁰ calling for President Xi Jinping to step down over the government's mishandling of the coronavirus.²²¹ The following month, property tycoon and party member Ren Zhiqiang was placed under investigation for “serious violations” after publishing an online critique of Xi's response to the pandemic. After the coverage period, in July 2020, he was expelled from the CCP and in September, sentenced to 18 years in prison on corruption charges; many experts interpreted the punishment as a warning to Xi's many critics within the party not to challenge his authority.²²² In May, Shandong poet Lu Yang was detained after releasing a video online calling on Xi to step down, and then charged with “inciting subversion.”²²³

In other instances, prosecutions continued for netizens who had been arrested in previous years. In June 2020, rights lawyer Chen Jiahong was put on trial behind closed doors in Guangxi province on charges of “inciting subversion;”²²⁴ Chen had been detained in April 2019 after posting a video online criticizing Xi's abolition of term limits in early 2018 and calling for democratic reforms.²²⁵ In a possible indication of the kinds of punishments awaiting the above detainees, blogger Liu Yanli was sentenced to four years in prison in April 2020 for making critical remarks concerning past and present government leaders.²²⁶ And on June 17, 2020, a court in Jiangsu Province sentenced human rights lawyer Yu Wensheng to four years in prison for “inciting subversion” after he posted an online call²²⁷ in January 2018 for constitutional reforms and democratic elections.²²⁸

At least 30 netizens and grassroots activists in mainland China have been harassed or detained by police for making statements online in support of the antiextradition bill and prodemocracy protest movement in Hong Kong, according to data collected by Chinese Human Rights Defenders.²²⁹ In August 2019, Chongqing-based activist Huang Yang was detained and later placed under surveillance at his home after he expressed support for the protests on his social media account.²³⁰ In September 2019, police threatened activist Chen Siming of Hunan Province for making similar statements online, while Zhejiang Province-based activist Wei Xiaobing was given 15 days of administrative detention in June 2019 for sharing Facebook posts and tweets in support of the movement.²³¹ Police also arrested prominent feminist activist Sophia Huang in October 2019 after she posted online about her support for the Hong Kong protesters.²³² though she was later released in January 2020.²³³

A number of other online activists and website administrators faced penalties during the coverage period. In July 2019, Huang Qi, founder of the human rights website 64 Tianwang, was sentenced to 12 years in prison on charges of “intentionally leaking state secrets.”²³⁴ In December 2019, labor activist Chen Weixiang was released after spending fifteen days in police detention in Guangdong Province for discussing the legal rights and problems of

sanitation workers in a WeChat group he ran.²³⁵ That same month, human rights lawyer Qin Yongpei was arrested for “inciting subversion of state power” as a result of criticism of the Chinese government he had posted on Twitter.²³⁶

Users sharing information from or with foreigners were also penalized. In June 2019, Liu Pengfei, the moderator of a popular WeChat account that posted news from outside China, was sentenced to two years in prison.²³⁷ Liu's arrest came after state media warned that WeChat group administrators could be held responsible for the content in their group under regulations in effect since 2017.²³⁸ Similarly, on July 7, 2020, Chen Zong from Guangzhou was reportedly sentenced to 15 months in prison on charges of “picking quarrels” after he set up WeChat groups to share information he had collected from blocked overseas websites.²³⁹ Chen had been detained in August 2019.

In a reflection of the flexibility and reach of Chinese legal interpretations, in July 2019, a Chinese international student was arrested by authorities in Wuhan and detained for six months due to comments critical of the Chinese government he had posted on Twitter while studying at the University of Minnesota.²⁴⁰ In September 2019, a Taiwanese businessman was detained in Shenzhen on national security grounds for using Line to share pictures of the Hong Kong protest movement with his friends.²⁴¹

Authorities selectively enforce the ban on unapproved VPNs, often prosecuting activists who provide access to them—some who do so as a form of anticensorship activism. Prison sentences and other penalties were handed down during the coverage period in several cases for the use or sale of VPN services as part of a broader crackdown on circumvention tools (see B1). In December 2019, a graduate student in Jiangsu Province was arrested for providing a VPN service to at least 28,000 customers.²⁴² That same month, police in Shenzhen arrested another man for selling VPNs.²⁴³ In May 2020, a man was fined by local police in the city of Ankang, Shaanxi Province, for using a VPN to access content blocked by Chinese censors.²⁴⁴ In addition to those sharing VPNs, in April 2020, Beijing police detained three netizens who had archived and shared through the code-sharing site GitHub censored articles and other material related to the coronavirus outbreak, later charging them with “picking quarrels and provoking trouble.”²⁴⁵

Members of persecuted religious and ethnic minority groups face particularly harsh treatment for their online activities. Since early 2017, a systematic Chinese government campaign has been underway to repress Xinjiang’s roughly 13 million Muslims through mass arbitrary detentions, intrusive surveillance, and torture.²⁴⁶ An estimated one million people are being held in political reeducation camps or forced labor facilities,²⁴⁷ some of whom were targeted for their online activities, including communication with relatives living abroad via WeChat.²⁴⁸ During the coverage period, reports emerged of prison sentences being imposed on some of these detainees. A leaked Chinese government document with details of dozens of Uighurs and other Muslims jailed or taken away for reeducation in Xinjiang that was made public in February 2020 included in its list someone who was friends on WeChat with a Uighur in Turkey, an individual who accidentally clicked on an overseas website on their phone, and a woman sentenced in August 2017 to 15 years in prison for making contact online with Uighurs outside the country.²⁴⁹ There are also reports that ethnic Hui Muslims inside and outside Xinjiang have come under greater state surveillance and experience periodic detention.²⁵⁰ In January 2020, Cui Haoxin, a Hui Muslim poet, was detained by police in the city of Jinan, Shandong Province, for tweeting about repression in Xinjiang and charged with “picking quarrels and provoking trouble.”²⁵¹ That same month the *Washington Post* reported on the case of a Hui woman who was held at a reeducation camp for five months after she used a VPN to submit homework to the University of Washington when visiting her father in Xinjiang.²⁵²

Tibetan Buddhists, including those living outside the Tibetan Autonomous Region, have also been targeted, particularly for views and information shared via WeChat. In August 2019, authorities in Qinghai Province issued a notice calling for intensified monitoring of messaging apps like WeChat and warning that sharing of banned information, including related to politics, Hong Kong, or “unverified news reports” would result in prison terms of between one and eight years.²⁵³ In July 2019, a Tibetan man living in Sichuan Province was held in police custody for ten days after sharing a photograph of the Dalai Lama on WeChat,²⁵⁴ while in September 2019 a 22-year-old Tibetan monk was arrested for complaining about the negative impact of Chinese state policy on the Tibetan language on WeChat.²⁵⁵

Members of other religious minorities are also prosecuted for their online and digital activities. Many Falun Gong practitioners have been jailed in recent years for posting messages about the spiritual group or human rights abuses on social media, accessing banned websites, and possessing or sharing prohibited VPN technology,²⁵⁶ a trend that reportedly intensified during the pandemic.²⁵⁷ In August 2019, police in Liaoning province detained 29-year-old Zhai Zihui after she sent a WeChat message to a friend about Falun Gong and shared a USB drive with information related to the practice with an acquaintance.²⁵⁸ As of September 2020, she was awaiting trial and could face several years in prison, based on the outcome of past such cases.²⁵⁹

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption? 0 / 4

Under data-privacy legislation in effect since 2012 and additional rules that were implemented in 2017,²⁶⁰ web service companies are required to register users under their real names and national ID numbers, compromising anonymity and placing communications at risk of direct government surveillance.²⁶¹ Chinese authorities also introduced new guidelines for online gamers in November 2019, requiring all players to register using their name and phone number.²⁶²

Mobile phone registration requirements also greatly infringe on user anonymity, especially given that the majority of internet services require registration with a mobile phone number.²⁶³ The authorities justify real-name registration as a means to prevent cybercrime, but uploaded identity documents are vulnerable to theft or misuse.²⁶⁴ In December 2019, new regulations took effect that require mobile phone users (which make up the vast majority of internet users in China) to have their face scanned when registering for mobile phone services.²⁶⁵

The government’s tightening restrictions on VPN use and controls over available services has further reduced the options for user anonymity, while raising concerns that government approved VPN services would share user data with authorities.

Authorities in some areas have instructed public Wi-Fi providers to comply with user registration requirements.²⁶⁶ Cybercafés check photo identification, record user activities, and at times require facial scans, sometimes in cooperation with law enforcement. However, cybercafés are no longer as popular as they once were due to expanding broadband and mobile phone internet access, and are used mostly by gamers.

Users’ ability to use encryption communication is also undermined. The 2015 antiterrorism law requires companies to offer technical support to decrypt information at the request of law enforcement agencies, among other provisions.²⁶⁷ 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.²⁶⁸ In January 2020, a new Encryption Law took effect which requires critical information-infrastructure providers to apply for a review by the CAC if their use of encryption technologies is viewed as potentially impacting national security.²⁶⁹

As with censorship, measures that erode privacy disproportionately target groups that are perceived as threats to the regime. In Xinjiang, Uighurs have been required since 2015 to register with their real names when purchasing electronic devices with storage, communication, and broadcast features. Stores selling such equipment are also required to install software that provides police with real-time electronic records on transactions.²⁷⁰

C5 0-6 pts

Does state surveillance of internet activities infringe on users’ right to privacy? 0 / 6

Direct surveillance of internet and mobile phone communications is pervasive and highly sophisticated, and privacy protections under Chinese law are minimal. In recent years, the Chinese government has increasingly moved towards big-data integration with the help of private companies, essentially consolidating in various databases a wide array of information on individuals, including their internet and mobile phone activities.

When conducting investigations, the authorities have unfettered access to user communications and data on certain popular platforms, as indicated by reports of users being punished for their presumably private conversations, particularly on WeChat. In April 2018, for example, a leaked directive from an internet policing department in Zhejiang Province revealed instructions to investigate an individual who had criticized Xi Jinping in a WeChat group with only eight members. Though the individual used a pseudonym, the instructions identified him with his real name, address, and phone number.²⁷¹

Residents of Xinjiang are subject to severely invasive surveillance tactics. In February 2019, security researcher Victor Gevers discovered and exposed a large database containing the personal information of 2.6 million people in Xinjiang, including official identification numbers, addresses, employers, and a list of each individual’s physical locations over the past 24 hours.²⁷² Some of this collected data may come from the surveillance software that individuals in the region were required to install on their mobile phones beginning in 2017. The spyware, known as Jingwang (“Web Cleansing” or “Clean Net”), scans for files that match blacklisted content.²⁷³ Researchers at the Open Technology Fund confirmed the application’s intrusive capabilities and discovered inherent vulnerabilities in the channels used to relay collected data to government servers.²⁷⁴ Earlier, in 2017, Chinese authorities identified more than 40,000 Uighurs for internment by monitoring their use of the video and audio-sharing app Zappya.²⁷⁵

Surveillance technologies and policies deployed in one part of China are often later expanded to other parts of the country, with Xinjiang emerging as a particularly important testing ground.²⁷⁶ Chinese border police are reported to have installed surveillance apps on the phones of tourists traveling in Xinjiang, which grant authorities the ability to extract user data and identify politically and culturally sensitive material stored on the person’s phone.²⁷⁷ In August 2019, reports emerged that Chinese border officers were beginning to check the photographs, messages, and apps on the phones of anyone arriving in China from Hong Kong for evidence of support for the prodemocracy protest movement in the city.²⁷⁸

Existing, albeit geographically disparate, data sets assembled through surveillance efforts could feed into “social credit” systems that create an assessment of individuals’ online activities and other personal data; a few municipalities are currently testing such systems,²⁷⁹ which have been subject to criticism within and outside China due to privacy and other concerns. Although a 2014 document referred to the full implementation of a vaguely defined “social credit” system by 2020,²⁸⁰ a fully integrated national social credit system does not yet exist and questions have been raised about how widespread and effective local pilot efforts have been.²⁸¹ Nevertheless, being listed as problematic by municipal or provincial authorities under such systems can result in restrictions on movement, education, and financial transactions. By contrast, those highly rated in Alibaba’s Sesame Credit scoring system or in municipal ratings of local governments like Xiamen and Fuzhou can win privileged access to private services, deposit waivers, free library book borrowing, or shorter lines at airport security.²⁸²

C6 0-6 pts

Are service providers and other technology companies required to aid the government in monitoring 0 / the communications of their users? 6

Internet companies are required under numerous laws and regulations to assist the government in monitoring users’ online activities. Recent regulations include a September 2018 rule that provides security authorities with broad powers to enter the premises of all internet service companies to inspect and copy any information deemed important to cybersecurity.²⁸³ That rule formed part of the Provisions on Internet Security Supervision and Inspection by Public Security Organs, published by the Ministry of Public Security, which allows officials to supervise and inspect the “network security” of ISPs. The new regulatory package complemented the 2017 cybersecurity law’s requirement that network operators assist police and security agencies with criminal investigations or national security operations.²⁸⁴ Inspections under the new rules began immediately.²⁸⁵

While a 2012 law requires businesses to obtain users’ consent to collect their personal electronic data and outline the “use, method, and scope” of the collection, there are no limits placed on law enforcement requests for personal records. The scope of industries and companies collecting and sharing information on users has expanded in recent years. In October 2019, for example, China’s Ministry of Culture and Tourism released 42 regulations requiring online travel providers to store the information of users posting on their sites, document any illegal content posted, and report violations to the authorities.²⁸⁶

Other surveillance laws include a 2013 amendment to the criminal procedure code that lays out a vague review process for allowing police monitoring of suspects’ electronic communications, which the Ministry of Public Security permits in many types of criminal investigations.²⁸⁷ The State Secrets Law obliges telecommunications companies to cooperate with authorities investigating leaked state secrets, or risk losing their licenses.²⁸⁸

Individuals or entities that refuse to comply with government requests for surveillance assistance risk detention or criminal punishment. A National Intelligence Law adopted in 2017 states that those deemed to be obstructing national intelligence work can be subject to 15 days of administrative detention or further criminal charges.²⁸⁹

Various regulations outline requirements for companies to retain user data, which they must make available to officials.²⁹⁰ CAC rules issued in 2016 oblige Chinese app providers to register users and keep user activity logs for 60 days.²⁹¹ Other ISPs are required to retain user information for 60 days and submit it to the authorities upon request, without judicial oversight or transparency.²⁹²

Tencent—the parent company of WeChat and QQ, two of the world’s most widely used social media platforms—directly assists the Chinese government with surveillance. Security researcher Victor Gevers found in March 2019 that millions of conversations and user identities on Tencent platforms were being sent from Chinese cybercafés to police stations across the country.²⁹³ Research by the University of Toronto’s Citizen Lab found in early 2020 that WeChat was also monitoring messages and images sent by users registered outside of China, scanning them for politically sensitive key words and retaining the relevant conversations in order to train the platform’s censorship system.²⁹⁴

The e-commerce giant Alibaba also helps the government with surveillance. In October 2019, research published by the Open Technology Fund revealed evidence that the government’s Study the Great Nation app, which was designed by Alibaba to promote the CCP’s ideology and encourage the study of “Xi Jinping thought” in particular, was built with a back door that could grant the authorities access to users’ internet browsing histories, text messages, photos, and other personal information.²⁹⁵

Such private-government partnerships and apparent backdoors in effectively mandatory apps continued after the coronavirus struck, as regional officials partnered with major Chinese tech firms Alibaba and Tencent to develop “health code” apps. The prevailing software assigns individuals a QR code and low (green), medium (amber), or high (red) risk ratings depending on factors such as their location history and self-reported symptoms, although neither authorities nor the companies provide further information on how the risk levels are calculated. A green code is required to access certain public spaces and office buildings. Although there are variations among the dozens of apps used in each province or municipality, an analysis by the law firm Norton Rose Fulbright found that the privacy policy of Beijing’s app does not incorporate strong privacy-by-design principles or state any time limit on the retention of data.²⁹⁶ A *New York Times* investigation showed that the Alipay Health Code app automatically shared data with the police.²⁹⁷ As the initial outbreak was brought under control in China, certain health code apps were rolled back in cities like Shanghai. Conversely, in May, health officials in Hangzhou proposed to expand the city’s app system from simple color codes into personal “health scores” that would reflect people’s sleep patterns, alcohol consumption, smoking habits, and exercise levels. The proposal led to uproar among users and even earned a rare rebuke from state-run media.

The 2017 cybersecurity law mandates that internet companies store the data of Chinese residents on servers based in the country, a practice that makes it easier for the government to access user information. Apple quickly complied with the requirement.²⁹⁸ In February 2018, Apple’s iCloud began storing the data of its Chinese users in partnership with Guizhou-Cloud Big Data, a state-run company,²⁹⁹ while Chinese state media reported plans to open a second data center in Inner Mongolia in 2020.³⁰⁰ Apple has also complied with other obligations that facilitate government surveillance: in September 2018, it changed the hardware specifications of new iPhones for the Chinese market to comply with real-name registration rules and improve authorities’ ability to track user identities.³⁰¹

Dozens of private companies in China have developed “key individual” databases for security agencies across the country. At least 13 tenders for such projects were issued by Public Security Bureaus in seven provinces or centrally administered cities between October 2015 and May 2019,³⁰² according to information available online.³⁰³ Of 40 companies building surveillance database systems, at least 10 provide accompanying handheld devices, like Sensingtech, while 13 mention mapping or geolocation features, like Netposa.³⁰⁴ In addition to basic biographical data—including name, date of birth, gender—as well as biometric data, many databases collect information on targeted individuals’ social media accounts. Key individuals are broadly defined by 2007 guidelines created by the Ministry of Public Security as those “suspected of threatening national security or public order.”³⁰⁵ An examination of more than 70 local government notices issued in 26 of China’s 34 provinces and administrative regions between 2011 and 2019 found frequent mentions of petitioners, Falun Gong practitioners, people with mental illnesses, and those involved in “stability maintenance” or “terrorist” activities—two terms that are often applied to rights activists, protesters, and members of ethnic minority groups like Xinjiang’s Uighurs.³⁰⁶ Some databases also referred to migrants, foreigners, and clergy from state-sanctioned religious groups as “key individuals.”

C7 0-5 pts

Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities? 0 / 5

Cases of extralegal intimidation and violence involving internet users are widespread. During the coverage period, instances including intimidation, aggressive interrogation, beatings, disappearances, and deaths from abuse in custody were reported.

Law enforcement officials frequently summon individuals for questioning in relation to online activity, an intimidation tactic referred to euphemistically as being “invited to tea.”³⁰⁷ This includes activists who expressed opposition to the Chinese government’s attempts to exercise greater political control over Hong Kong.³⁰⁸ Chinese users of Twitter and Line also encountered harassment and intimidation during the coverage period.

Activists have also been forced to travel within the country during sensitive political events, effectively keeping them away from their normal online activities.³⁰⁹ Others have gone into hiding to avoid arrest, including a Falun Gong practitioner from Hunan who was sought by police after putting up posters in April 2020 with a QR code that enabled others to access blocked websites with information about the pandemic.³¹⁰ Beginning in August 2018, a young Uighur man, Miradil Hesen, was in hiding after authorities noticed he had downloaded the blocked app Instagram to his cell phone. In September 2020, police in Jiangsu Province detained him after he also posted YouTube videos relaying the harassment, detention, and forced sterilization of his family members.³¹¹

According to Human Rights Watch, detainees in ordinary criminal cases face “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 February 2020, Chinese Human Rights Defenders reported that “torture and cruel, inhuman and degrading treatment remained rampant in China in 2019.”³¹² Political and religious prisoners often experience even worse treatment.³¹³ Many—like online activist Huang Qi—are denied medication and medical parole despite serious illnesses, raising the possibility that they might die in custody.³¹⁴

Members of religious and ethnic minority groups are among the internet users most vulnerable to extralegal detention, torture, and killing. In Xinjiang, some of the estimated one million Uighurs and other Muslim minorities were taken to reeducation camps as a result of their online activities, such as downloading WhatsApp, possessing the contact information of prominent Uighur scholars, or simply clicking on links on their mobile phones.³¹⁵ Those detained or imprisoned typically suffer harsh conditions and often torture,³¹⁶ resulting in long-term health problems and sometimes death. In April 2020, a Tibetan monk passed away from complications resulting from severe beatings he suffered in custody in 2017, when he was detained for sharing via WeChat a recognition letter from the Dalai Lama about the reincarnation of another prominent Tibetan religious figure.³¹⁷

Online commentators expressing views critical of the Chinese government or deemed to harm China’s international reputation have in recent years faced increased bullying, harassment, and real-world repercussions from nationalistic online users. For example, in April 2020, just two months after her online diary—which detailed the Wuhan lockdown and the hardships of city residents, and at times was critical of authorities—garnered much sympathetic attention within China, Wuhan-based author Fang Fang was attacked by nationalist online mobs after news emerged that the diary would be translated into English and published abroad.³¹⁸ And on April 26, Hubei University announced that it was investigating Liang Yanping, a professor, after she used her social media account to express support for Fang Fang.³¹⁹

C8 0-3 pts

Are websites, governmental and private entities, service providers, or individual users subject to 0 / widespread hacking and other forms of cyberattack? 3

Hackers employ various methods to interrupt or intercept online content with political implications. China remains a top source of global cyberattacks,³²⁰ though those with commercial targets have declined or become harder to trace.³²¹ Attacks known to have originated in China can rarely be linked directly to the state, and much of the activity appears decentralized and uncoordinated. However, many attacks employ sophisticated technology, and experts believe that Chinese military and intelligence agencies either sponsor or condone technical attacks on political targets both within and outside China.

In April 2019, the human rights group Charter 08 reported that the contents of its online forum had been deleted and its Google blog removed. The organization also noted that its Twitter account had been hacked several times in recent months.³²² Many Chinese Twitter users were hacked during the coverage period, apparently as part of the government’s crackdown on the platform (see B2 and C7). One activist, Wang Aizhong, had 3,000 tweets deleted from his account in December 2018, which he attributed to state-sponsored hacking.³²³

Websites associated with the persecuted Uighur minority group have faced frequent cyberattacks in recent years, while China-based hackers have deployed various phishing campaigns to infiltrate these communities in exile and collect intelligence. In April 2019, researchers reported that 11 websites commonly visited by members of the Uighur community had been compromised with malicious software that infected visitors’ mobile devices and intercepted user data such as unique identification numbers, phone numbers, and location information.³²⁴ These attacks continued through December 2019 to March 2020, with hackers planting malware on the iPhones of people who visited the mobile version of popular Uighur websites.³²⁵

Footnotes

- ¹CNNIC, “The 45th China Statistical Report on Internet Development,” CNNIC, April, 2020, <https://www.cnnic.net.cn/hlwfzyj/hlwzbg/hlwjbg/202004/P02020042859659...>
- ²Cable.co.uk, “Worldwide broadband speed league 2020,” The ranking is based largely on the amount of time taken to download a 5GB HD movie, September 2, 2020, <https://www.cable.co.uk/broadband/speed/worldwide-speed-league/>
- ³CNNIC, “The 45th China Statistical Report on Internet Development,” CNNIC, April, 2020, <https://www.cnnic.net.cn/hlwfzyj/hlwzbg/hlwjbg/202004/P02020042859659...>
- ⁴Charlotte Gao, “China’s Great Firewall: A Serious Pain in the Neck for European and US Companies,” Diplomat, June 21, 2018, <https://thediplomat.com/2018/06/chinas-great-firewall-a-serious-pain-in-...>
- ⁵China Law Translate, “Cybersecurity Law,” China Law Translate, July 4, 2016, <http://www.chinalawtranslate.com/cybersecurity2/?lang=en>
- ⁶China Power Team, “How web-connected is China?,” China Power, April 18, 2019, <https://chinapower.csis.org/web-connectedness/>
- ⁷China Law Translate, “Cybersecurity Law,” China Law Translate, July 4, 2016, <http://www.chinalawtranslate.com/cybersecurity2/?lang=en>
- ⁸CGTN, “China to build 600,000 5G bases in 2020 despite COVID-19 impact,” CGTN, June 7, 2020, <https://news.cgtn.com/news/2020-06-06/China-to-build-600-000-5G-base-st-...>
- ⁹Takashi Kawakami, Nikkei staff writer, “China closes in on 70% of world’s 5G subscribers,” Nikkei Asia, May 12, 2020, <https://asia.nikkei.com/Spotlight/5G-networks/China-closes-in-on-70-of-...>
- ¹⁰People’s Daily Overseas Edition, “7月1日取消“漫游”费 提速降费又见“大礼包” [The national data roaming charges have been cancelled since July 1],” 中国政府网 www.gov.cn, July 4 2018, http://www.gov.cn/xinwen/2018-07/04/content_5303336.htm
- ¹¹CGTN, “Premier Li’s speech at the third session of the 13th NPC,” CGTN, May 22, 2020, <https://news.cgtn.com/news/2020-05-22/Full-text-Premier-Li-s-speech-at-...>
- ¹²Southern Metropolis Daily, “政府工作报告明确今年宽带资费降15% 将惠及4.3亿宽带用户 [The government work report clarifies that a 15% reduction in broadband tariffs this year will benefit 430 million broadband users],” Southern Metropolis Daily, May 22, 2020, <http://finance.eastmoney.com/a/202005221495033950.html>
- ¹³CNNIC, “The 45th China Statistical Report on Internet Development,” CNNIC, April, 2020, <https://www.cnnic.net.cn/hlwfzyj/hlwzbg/hlwjbg/202004/P02020042859659...>
- ¹⁴CNNIC, “The 45th China Statistical Report on Internet Development,” CNNIC, April, 2020, <https://www.cnnic.net.cn/hlwfzyj/hlwzbg/hlwjbg/202004/P02020042859659...>
- ¹⁵CNNIC, “The 45th China Statistical Report on Internet Development,” CNNIC, April, 2020, <https://www.cnnic.net.cn/hlwfzyj/hlwzbg/hlwjbg/202004/P02020042859659...>
- ¹⁶Qin Chem, “Inkstone Explains: How China engineers an alternative internet for its people,” Inkstone news, Jun 11, 2020, <https://www.inkstonenews.com/tech/inkstone-explains-how-china-engineers-...>
- ¹⁷Ouyang Shijia and Ma Si, “Cybersecurity rule to take effect June 1,” China Daily, April 28, 2020 <https://global.chinadaily.com.cn/a/202004/28/WS5ea78912a310a8b241152323...>
- ¹⁸CAC, “网络安全审查办法[Cyber Security Review Measures],” CAC, April 27, 2020, http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm
- ¹⁹China Law Translate, “Cybersecurity Review Measures,” China Law Translate, May 7, 2020, <https://www.chinalawtranslate.com/en/cyber-security-review/>
- ²⁰Alexa Olesen, “Welcome to the Uighur Web,” Foreign Policy, April 21, 2014, <http://atfp.co/1jmJCYH>
- ²¹Olivia Li, “China Tested Internet Shutdown Ahead of 30th Anniversary of Tiananmen Massacre,” Epoch Times, June 5, 2019, <https://www.theepochtimes.com/china-tests-internet-shutdown-ahead-of-30-...>

- [22](#)China Digital Times, “【立此存照】切断全县互联网上网服务营业场所的网络信号接入服务”[[Save the photo here] Cut off the network signal access service of the county's Internet service business premises] January 29, 2020, <https://perma.cc/7BFR-A256>; Beijing News, “湖北阳新县回应为防疫断网：仅关停经营场所[Hubei Yangxin County respond disconnecting the network for epidemic prevention: only shut down business premises],” January 31, 2020, <http://www.bjnews.com.cn/wevideo/2020/01/31/682049.html>.
- [23](#)明報專訊 MingPao, “六四臨近 當局逼丁子霖離京限通訊 [Authorities Force Ding Zilin to Leave Beijing on June 4],” 明報MingPao, May 21, 2019, <https://perma.cc/XZD7-TNJC>; 美国之音Voice of America, “六四敏感日近 天安门母亲丁子霖等人被监控 [Tiananmen mother Ding Zilin and others are under surveillance on June 4th],” 美国之音Voice of America, May 20, 2019, <https://www.voachinese.com/a/Founder-Of-Tiananmen-Mothers-Taken-Out-Of-...>.
- [24](#)Drew Foerster, “China’s Legislature Gears Up to Pass a Sweepingly Vague Cybersecurity Law,” American Bar Association, May 2, 2016, http://www.americanbar.org/publications/blt/2016/05/02_foerster.html; China Law Translate, “Counter-Terrorism Law (2015),” China Law Translate, December 27, 2015, <https://www.chinalawtranslate.com/en/counter-terrorism-law-2015/>.
- [25](#)Alan Weissberger, “China’s big 3 mobile operators have 9 Million 5G subscribers in advance of the service; Barron’s: China to lead in 5G deployments,” Techblog, October 7, 2019, <https://techblog.comsoc.org/2019/10/07/chinas-big-3-mobile-operators-ha...>.
- [26](#)Lan Xinzhen, “Full-Pricing Autonomy,” Beijing Review, May 26, 2014, http://www.bjreview.com.cn/business/txt/2014-05/26/content_621017.htm; Paul Mozur and Lorraine Luk, “China to Liberalize Telecommunications Pricing,” Wall Street Journal, May 9, 2014, <http://on.wsj.com/1NFam3s>; 毛启盈, “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],” 搜狐Sohu, December 30, 2015, <http://it.sohu.com/20151230/n432995626.shtml>.
- [27](#)Global Services, BT, “First global telco to receive domestic telecoms licences in China,” January 24, 2019, <https://www.globalservices.bt.com/en/aboutus/news-press/bt-first-global...>.
- [28](#)Phoebe Zhang and Sidney Leng, “China plans to allow foreign investment in VPN services as part of Beijing trial in latest opening up move,” South China Morning Post, August 16, 2019, <https://www.scmp.com/economy/china-economy/article/3023081/china-plans-...>.
- [29](#)These include the Public Security Bureau and the State Administration for Industry and Commerce. “一看就明白全程图解网吧牌照申请流程图” [A look at an illustration of the whole course of the cybercafe license application process],” Detail.Zol.com, http://detail.zol.com.cn/picture_index_100/index997401.shtml.
- [30](#)Qianzhan, “2018年中国网吧服务行业市场分析：网吧数量及客流双双下滑 中型网吧更具市场优势 [Market analysis of China's Internet cafe service industry in 2018: both the number of Internet cafes and passenger flow have declined. Medium-sized Internet cafes have more market advantages],” Qianzhan, October 27, 2019, <https://bg.qianzhan.com/report/detail/300/191025-577e9421.html>.
- [31](#)Karen Chiu, “Life hasn’t returned to normal for China’s internet cafes,” South China Morning Post, April 16, 2020, [https://www.scmp.com/tech/apps-social/article/3080130/life-hasnt-return...](https://www.scmp.com/tech/apps-social/article/3080130/life-hasnt-return-...).
- [32](#)Central Cyberspace Affairs Commission website, <http://www.cac.gov.cn/>.
- [33](#)David Feng, “Chinese Cyber Administration Office Goes Online,” Tech Blog 86, December 31, 2014, <https://web.archive.org/web/20150112152942/http://www.techblog86.com/20...>; National Law Review, “More Officials Appointed to Lead Film and Media Authorities in China,” National Law Review, July 31, 2018, [https://www.natlawreview.com/article/more-officials-appointed-to-lead-f...](https://www.natlawreview.com/article/more-officials-appointed-to-lead-f-...).
- [34](#)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.
- [35](#)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, [https://thediplomat.com/2014/02/xi-jinping-leads-chinas-new-internet-se...](https://thediplomat.com/2014/02/xi-jinping-leads-chinas-new-internet-se-...).
- [36](#)Kathleen Wilson, “Revoking Trust in one CNNIC Intermediate Certificate,” Mozilla Security Blog, March 23, 2015, [https://blog.mozilla.org/security/2015/03/23/revoking-trust-in-one-cnni...](https://blog.mozilla.org/security/2015/03/23/revoking-trust-in-one-cnni-...).
- [37](#)Timothy P. Stratford, Jason Goldberg and Christopher Adams, “More Officials Appointed to Lead Film and Media Authorities in China,” Global Policy Watch, July 31 2018, [https://www.globalpolicywatch.com/2018/07/more-officials-appointed-to-l...](https://www.globalpolicywatch.com/2018/07/more-officials-appointed-to-l-...).
- [38](#)Xinhua, “Senior CPC official stresses united front work in Internet sector,” Xinhua Net, November 28, 2019, http://www.xinhuanet.com/english/2019-11/28/c_138590257.htm.
- [39](#)“Censorship of Alexa Top 1000 Domains in China,” GreatFireChina, <https://en.greatfire.org/search/alexa-top-1000-domains>.
- [40](#)“BBC websites blocked in China after security change,” BBC, August 7, 2018, <https://www.bbc.com/news/technology-45098190>.
- [41](#)“Censorship of Alexa Top 1000 Domains in China,” GreatFireChina, <https://en.greatfire.org/search/alexa-top-1000-domains>; Sherisse Pham, “China adds Pinterest to list of banned sites,” CNN, March 17, 2017, <http://money.cnn.com/2017/03/17/technology/pinterest-banned-china/>.

- ⁴²Chauncey Jung, “Reddit Blocked In China,” Supchina, August 12, 2018, <https://supchina.com/2018/08/12/reddit-blocked-in-china/>
- ⁴³“Wikipedia blocked in China in all languages,” BBC, May 14, 2019; <https://www.bbc.com/news/technology-48269608>
- ⁴⁴Hillary Leung, “Wikipedia Is Now Banned in China in All Languages,” Time, May 15, 2019, <https://time.com/5589439/china-wikipedia-online-censorship/>
- ⁴⁵Michael Kan, “Google blocked in China by censors, unclear how long it will last,” Info World, November 9, 2012, <https://www.infoworld.com/article/2615782/google-blocked-in-china-by-ce...>
- ⁴⁶Rachel Mok, “Yahoo search is now blocked in China,” Startup Living China, August 31, 2018, <https://startuplivingchina.com/yahoo-search-now-blocked-china/>
- ⁴⁷“China blocks Microsoft’s Bing search engine for one day,” Guardian, January 24, 2019, <https://www.theguardian.com/world/2019/jan/24/china-blocks-microsofts-b...>
- ⁴⁸StateCounter, “Search Engine Market Share China,” <https://gs.statcounter.com/search-engine-market-share/all/china>
- ⁴⁹“Businesses, consumers uncertain ahead of China VPN ban,” Reuters, March 30, 2018, <https://www.reuters.com/article/us-china-vpns/businesses-consumers-unce...>
- ⁵⁰Jingjing Ma, “New regulations set rules for Internet access services sector: experts,” Global Times, January 22, 2017, <http://www.globaltimes.cn/content/1030188.shtml>
- ⁵¹Wong Siu-san and Sing Man, “China Mobilizes The ‘Masses’ to Join Nationwide Security Ops Ahead of Oct. 1,” RFA, September 25, 2019, <https://www.rfa.org/english/news/china/anniversary-surveillance-0925201...>
- ⁵²Grady McGregor, “China deploys a favorite weapon in the coronavirus crisis: A crackdown on VPNs,” Fortune, February 25, 2020, <https://fortune.com/2020/02/25/coronavirus-china-vpn/>
- ⁵³Sophia Yan, “China blocks internet searches abroad as Xi under pressure ahead of major speech,” The Telegraph, March 5, 2019, <https://www.telegraph.co.uk/news/2019/03/05/china-blocks-internet-searc...>
- ⁵⁴Jane Li & Matthew De Silva, “This is the blacklist Apple uses to censor the internet in China,” Quartz, October 31, 2019, <https://qz.com/1737232/apple-and-tencent-use-this-blacklist-to-censor-s...>
- ⁵⁵Sam Biddle, “Shutterstock Employees Fight Company’s New Chinese Search Blacklist,” The Intercept, November 6, 2019, <https://theintercept.com/2019/11/06/shutterstock-china-censorship-tech/>
- ⁵⁶Steve Stecklow, “Refinitiv created filter to block Reuters stories amid Hong Kong protests,” Reuters, December 12, 2019, <https://www.reuters.com/article/us-hongkong-protests-media-specialrepor...>
- ⁵⁷China Law Translate, “Cybersecurity Law,” China Law Translate, July 4, 2016, <http://www.chinalawtranslate.com/cybersecurity2/?lang=en>
- ⁵⁸Secrss, “网信办：2019年全国网信行政执法成效显著[Office of the Cyberspace Administration of China: Significant achievements in national cybersecurity and informatization administrative law enforcement in 2019],” Secrss, February 18, 2020, <https://www.secrss.com/articles/17195>
- ⁵⁹CAC, “国家网信办启动专项整治行动 严厉打击网络恶意营销账号 [The State Cyberspace Administration of China launched a special rectification action to crack down on malicious online marketing accounts],” CAC, April 24, 2020, http://www.cac.gov.cn/2020-04/24/c_1589274589221739.htm
- ⁶⁰Xinhua, “Chinese Internet watchdog launches crackdown on illicit online accounts,” Xinhua, April 26, 2020, http://www.xinhuanet.com/english/2020-04/26/c_139008678.htm
- ⁶¹China News, “百度发布2019年信息安全治理年报 处理有害信息531.5亿余条 [Baidu releases 2019 annual report on information security governance, handling more than 53.15 billion pieces of harmful information],” China News, February 14, 2020, <http://www.chinanews.com/business/2020/02-14/9091543.shtml>
- ⁶²Jill Shen, “Amid intensified scrutiny, Baidu removes 50 billion pieces of ‘harmful’ content,” Tech Node, January 7, 2019, <https://technode.com/2019/01/07/baidu-content-removal-50-billion/>
- ⁶³赫海威, “中国‘标题党女王’的倒下：咪蒙为何被封杀 [Why China Silenced a Clickbait Queen in Its Battle for Information Control],” New York Times Chinese, March 19, 2019, <https://cn.nytimes.com/china/20190319/china-bloggers-internet/dual/>
- ⁶⁴Dave Yin, “Chinese Image Providers Shut Down for ‘Illegal’ Work With Foreign News,” Caixin Global, December 11, 2019, <https://www.caixinglobal.com/2019-12-11/chinese-authorities-shut-down-i...>
- ⁶⁵Xie Yu, “China’s internet censor shuts financial news aggregator wallstreetcn.com amid worsening US relations over trade and tech,” South China Morning Post, June 10, 2019, <https://www.scmp.com/business/companies/article/3013925/china-shuts-dow...>
- ⁶⁶Dave Yin, “Chinese Image Providers Shut Down for ‘Illegal’ Work With Foreign News,” Caixin Global, December 11, 2019, <https://www.caixinglobal.com/2019-12-11/chinese-authorities-shut-down-i...>
- ⁶⁷David Bandurski, “Internet Giants Warned Amid Coronavirus Crackdown,” China Media Project, February 6, 2020, <https://chinamediaproject.org/2020/02/06/internet-giants-warned-amid-co...>

- ⁶⁸Reuters, “China’s online censors tighten grip after brief coronavirus respite,” Reuters, February 11, 2020, <https://www.reuters.com/article/us-china-health-censorship/chinas-onlin...>
- ⁶⁹Wendy Huang, “When Weibo Stopped Updating Its Trending Topics List...,” Whats on Weibo, June 17, 2020, <https://www.whatsonweibo.com/when-weibo-stopped-updating-its-trending-t...>
- ⁷⁰Tony Xu, “Internet regulator cracks down on music and audio-based social platforms,” Tech Node, July 1, 2019, <https://technode.com/2019/07/01/internet-regulator-cracks-down-on-music...>
- ⁷¹He Wei, “Jinri Toutiao looks to BRICS nations,” China Daily, September 6, 2017, http://www.chinadaily.com.cn/bizchina/2017-09/06/content_31619329.htm
- ⁷²Tony Xu, “Regulator censures Bytedance’s search engine for smearing national hero,” Tech Node, November 12, 2019, <https://technode.com/2019/11/12/regulator-censures-bytedances-search-en...>
- ⁷³Reporting Center of the Cyberspace Administration of China, “百度APP部分频道因严重违规今日起暂停更新 国家网信办指导北京市网信办约谈百度公司负责人[Some channels of Baidu APP suspended update today due to serious violation of regulations. The State Cyberspace Administration of China instructed Beijing Cyberspace Administration to interview the person in charge of Baidu Company],” Weixin, April 8, 2020, <https://mp.weixin.qq.com/s/9U0Fiqvix8ycmOMNRzQpA>; China.org, “Baidu app suspends updating certain columns due to regulation violations,” April 8, 2020, [http://www.china.org.cn/china/Off the Wire/2020-04/08/content_75907866...](http://www.china.org.cn/china/Off%20the%20Wire/2020-04/08/content_75907866...)
- ⁷⁴Nick Statt, “Apple removes Quartz news app from the Chinese App Store over Hong Kong coverage,” The Verge, October 9, 2019, <https://www.theverge.com/2019/10/9/20907228/apple-quartz-app-store-chin...>
- ⁷⁵Tim Bradshaw, “Apple drops hundreds of VPN apps at Beijing’s request,” Financial Times, November 21, 2017, <https://www.ft.com/content/ad42e536-cf36-11e7-b781-794ce08b24dc>
- ⁷⁶Hassan Maishera, “China’s Internet Censorship Effort Continues as Authorities Blacklist Hundreds of VPN Servers,” Blokt, May 6, 2019, <https://blokt.com/news/chinas-internet-censorship-effort-continues-as-a...>; “How does your VPN speed measure against other VPNs in China,” Circumvention Central, accessed October 12, 2020, <https://cc.greatfire.org/en>.
- ⁷⁷Great Fire, “3636 apps are unavailable in the China (mainland) App Store,” Apple Censoship, <https://applecensorship.com/na/CN?l=en>
- ⁷⁸Elliott Zaagman, “Cat videos meet Big Brother,” The Interpreter, September 11, 2019, <https://www.lowyinstitute.org/the-interpreter/cat-videos-meet-big-broth...>
- ⁷⁹“Under Pressure From Cyberspace Administration, China’s Top News App Will Hire 2,000 More Content Reviewers,” Global Voices, January 5, 2018, <https://globalvoices.org/2018/01/05/under-pressure-from-cyberspace-admi...>
- ⁸⁰Emma Lee, “Kuaishou is hiring more people to filter content after crackdown on “vulgar” content,” Tech Node, April 8, 2018, <https://technode.com/2018/04/08/kuaishou-content-patrols/>
- ⁸¹Yuan Li, “Learning China’s Forbidden History, So They Can Censor It,” New York Times, January 2, 2019, <https://www.nytimes.com/2019/01/02/business/china-internet-censor.html>
- ⁸²<https://beyondsoft.com/interview-with-beyondsoft-ceo/> Matt Field, “Censorship 101: China’s young censors first have to learn about forbidden topics,” Bulletin of the Atomic Scientists, January 3, 2019, <https://thebulletin.org/2019/01/censorship-101-chinas-young-censors-fir...>
- ⁸³Jeffrey Knockel, Lotus Ruan, Masashi Crete-Nishihata, and Ron Deibert, “(Can’t) Picture This,” The Citizen Lab, August 14, 2018, <https://citizenlab.ca/2018/08/cant-picture-this-an-analysis-of-image-fi...>
- ⁸⁴Lusha Zhang and Ryan Woo, “Censorship pays: China’s state newspaper expands lucrative online scrubbing business,” Reuters, March 28, 2019, <https://www.reuters.com/article/us-china-censorship/censorship-pays-chi...>
- ⁸⁵Shan Li, “Made-in-China Censorship for Sale,” Wall Street Journal, March 6, 2020, <https://www.wsj.com/articles/made-in-china-censorship-for-sale-11583448...>
- ⁸⁶Shan Li, “Made-in-China Censorship for Sale,” Wall Street Journal, March 6, 2020, <https://www.wsj.com/articles/made-in-china-censorship-for-sale-11583448...>
- ⁸⁷Paul Mozur, “Twitter Users in China Face Detention and Threats in New Beijing Crackdown,” New York Times, January 10, 2019, <https://www.nytimes.com/2019/01/10/business/china-twitter-censorship-on...>; Yaxue Cao, “China Steps up Nationwide Crackdown to Silence Twitter Users – the Unmediated Story,” China Change, December 5, 2018, <https://chinachange.org/2018/12/05/china-steps-up-nationwide-crackdown-...>
- ⁸⁸Sarah Cook, “The News China Didn’t Want Reported in 2017,” Diplomat, January 27, 2018, <https://thediplomat.com/2018/01/the-news-china-didnt-want-reported-in-2...>
- ⁸⁹“Directives from the Ministry of Truth,” China Digital Times, accessed October 8, 2020, <https://chinadigitaltimes.net/china/directives-from-the-ministry-of-tru...>
- ⁹⁰Reuters, “China’s online censors tighten grip after brief coronavirus respite,” Reuters, February 11, 2020, <https://www.reuters.com/article/us-china-health-censorship/chinas-onlin...>

- ⁹¹Emily Feng and Amy Cheng, “Critics Say China Has Suppressed And Censored Information In Coronavirus Outbreak,” NPR, February 8, 2020, <https://www.npr.org/sections/goatsandsoda/2020/02/08/803766743/critics-...>
- ⁹²David Bandurski, “Wrestling Back the Agenda,” China Media Project, February 5, 2020, <https://chinamediaproject.org/2020/02/05/wrestling-back-the-agenda/>
- ⁹³Samuel Wade, “Control Temperature on Death of Coronavirus Whistleblower,” China Digital Times, February 6, 2020, <https://chinadigitaltimes.net/2020/02/minitru-control-temperature-on-d...>
- ⁹⁴Josh Rudolph, “Delete Article on Economic Impact of Who Declaring Coronavirus an “Emergency”,” China Digital Times, January 29, 2020, <https://chinadigitaltimes.net/2020/01/minitru-delete-article-on-econom...>
- ⁹⁵Sophie Beach, “Do not Transmit Video and Images of Law Enforcements Actions Around COVID-19 Prevention,” China Digital Times, March 13, 2020, <https://chinadigitaltimes.net/2020/03/minitru-do-not-transmit-video-an...>
- ⁹⁶Masashi Crete-Nishihata, Jakub Dalek, Jeffrey Knockel, Nicola Lawford, Caroline Wesley, and Mari Zhou, “A Timeline of Information Control on Chinese Social Media During COVID-19,” Cltizen Lab, August 25, 2020, <https://citizenlab.ca/2020/08/censored-contagion-ii-a-timeline-of-infor...>
- ⁹⁷Lotus Ruan, Jeffrey Knockel, and Masashi Crete-Nishihata, “How Information on the Coronavirus is Managed on Chinese Social Media,” Cltizen Lab, March 3, 2020, <https://citizenlab.ca/2020/03/censored-contagion-how-information-on-the-...>; Liz Carter, Jessica Stahl, FangFang Zhang, and Jessica Beinecke, “The Largest Social Network You’ve Never Heard Of,” VOA, August 20, 2012, <https://blogs.voanews.com/digital-frontiers/2012/08/20/the-largest-soci...>
- ⁹⁸Coco Liu and Nikki Sun and nikkei staff writers, “China’s online classes are minefield for censorship amid coronavirus,” Nikkei Asia, February 27, 2020, <http://archive.vn/mHTGa>
- ⁹⁹Paul Mozur, “Zoom Blocks Activist in U.S. After China Objects to Tiananmen Vigil,” New York Times, June 11, 2020, <https://www.nytimes.com/2020/06/11/technology/zoom-china-tiananmen-squa...>
- ¹⁰⁰Mimi Lau, “Why Chinese activists are fighting to keep Tiananmen Square memories alive, 31 years on from crackdown,” South China Morning Post, June 3, 2020, <https://www.scmp.com/news/china/politics/article/3087226/why-chinese-ac...>
- ¹⁰¹Josh Rudolph, “Delete Beijing Youth Daily Front Page on Li Peng,” China Digital Times, July 26, 2019, <https://chinadigitaltimes.net/2019/07/minitru-delete-beijing-youth-dai...>; Josh Rudolph, “Delete Article on Suicide of Bank President,” China Digital Times, July 26, 2019, <https://chinadigitaltimes.net/2019/07/minitru-delete-article-on-suicid...>; Samuel Wade, “Fury at Censorship of Tycoon’s Arrest,” China Digital Times, July 5, 2019, <https://chinadigitaltimes.net/2019/07/minitru-backlash-over-censorship...>; Josh Rudolph, “Delete Corruption Report on “Broker Xu Sheng”,” China Digital Times, June 23, 2020, <https://chinadigitaltimes.net/2020/06/minitru-delete-corruption-report...>
- ¹⁰²BC, “Hong Kong protest: What is mainland China hearing?,” BBC, August 16, 2019, <https://www.bbc.com/news/blogs-china-blog-49354507>; Josh Rudolph, “Do Not Report on Withdrawal of HK Extraditional Bill,” China Digital Times, September 5, 2019, <https://chinadigitaltimes.net/2019/09/minitru-do-not-report-on-withdra...>; Sophie Beach, “Delete Content Related to HK Protests,” China Digital Times, June 16, 2019, <https://chinadigitaltimes.net/2019/06/minitru-delete-content-related-t...>
- ¹⁰³Eva Dou and Philip Wen, “Uighurs Use Videos to Draw Attention to Missing Family Members,” Wall Street Journal, August 22, 2019, <https://www.wsj.com/articles/uighurs-use-videos-to-draw-attention-to-mi...>
- ¹⁰⁴Javier C. Hernández, “China Deploys Propaganda Machine to Defend Move Against Hong Kong,” New York Times, May 23, 2020, <https://www.nytimes.com/2020/05/23/world/asia/china-hong-kong-propagand...>
- ¹⁰⁵Xueyang Xu, Z. Morely Mao, and J. Alex Halderman, “Internet Censorship in China: Where Does the Filtering Occur?,” Passive and Active Measurement, (2011): 133–142, <https://web.eecs.umich.edu/~zmao/Papers/china-censorship-pam11.pdf>
- ¹⁰⁶Gary King, Jennifer Pan, and Margaret E. Roberts, “How Censorship in China Allows Government Criticism But Silences Collective Expression,” American Political Science Review 107, no. 2, May 2013, 1–18, <http://j.mp/2nxNUhk>
- ¹⁰⁷Linda Lew, “Kuniao web browser peeks over China’s Great Firewall but it’s no VPN, expert says,” South China Morning Post, November 15, 2019, <https://www.scmp.com/news/china/society/article/3037985/kuniao-web-brow...>
- ¹⁰⁸萧雨, “自称中国首款“合法”翻墙神器, 酷鸟两天后一命呜呼[Claiming to be China’s first “legal” artifact, Kuniao died two days later],” VOA, November 16, 2019, <https://www.voachinese.com/a/mysterious-censorship-evading-web-browser-...>
- ¹⁰⁹Drew Foerster, “China’s Legislature Gears Up to Pass a Sweepingly Vague Cybersecurity Law,” American Bar Association, May 2, 2016, http://www.americanbar.org/publications/blt/2016/05/02_foerster.html; China Law Translate,

- “Counter-Terrorism Law (2015),” China Law Translate, December 27, 2015, <https://www.chinalawtranslate.com/en/counter-terrorism-law-2015/>
- ¹¹⁰Sina, “网络造谣者将被列入失信主体黑名单 明确了四类情形[Internet rumors will be included in the blacklist of untrustworthy subjects, four types of situations are clarified],” Sina, July 29, 2019, <https://tech.sina.com.cn/i/2019-07-29/doc-ihytterm6966396.shtml>; “国家互联网信息办公室关于《互联网信息服务严重失信主体信用信息管理办法（征求意见稿）》公开征求意见的通知 [Notice of the State Internet Information Office on the Public Comment on the ‘Administrative Measures for the Credit Information of Internet Information Services Deemed Seriously Untrustworthy Entities (Draft for Comment.)’]” Cyberspace Administration of China, July 22, 2019, http://www.cac.gov.cn/2019-07/22/c_1124782573.htm
 - ¹¹¹Josh Rudolph, “NEW RULES CRACK DOWN ON SHORT VIDEOS,” China Digital Times, January 18, 2019 <https://chinadigitaltimes.net/2019/01/new-rules-crack-down-on-short-vid...>
 - ¹¹²China Law Translate, “Norms for the Administration of Online Short Video Platforms and Detailed Implementation Rules for Online Short Video Content Review Standards,” China Law Translate, January 9, 2019, <https://www.chinalawtranslate.com/en/网络短视频平台管理规范/>
 - ¹¹³David Bandurski, “A Censor for Every 1,000 Videos Please,” China Media Project, January 13, 2019, <http://chinamediaproject.org/2019/01/13/a-censor-for-every-1000-videos-...>
 - ¹¹⁴Viola Zhou, “Locked out of an online life,” Ink Stone, July 26, 2018, <https://www.inkstonenews.com/tech/chinas-wechat-increasing-censorship-i...>
 - ¹¹⁵Arjun Kharpal, “Everything you need to know about WeChat — China’s billion-user messaging app,” CNBC, February 3, 2019, <https://www.cnbc.com/2019/02/04/what-is-wechat-china-biggest-messaging-...>
 - ¹¹⁶“Censored on WeChat: A year of conte,” Global Voice, February 11, 2019, <https://globalvoices.org/2019/02/11/censored-on-wechat-a-year-of-conten...>
 - ¹¹⁷Alexandra Ma, “Relatives of China’s oppressed Muslim minority are getting blocked online by their own family members, who are terrified to even tell them how bad their lives are,” Business Insiders, February 16, 2019, <https://www.businessinsider.com/family-of-ughurs-in-china-say-are-bloc...>
 - ¹¹⁸Jane Li, “‘He refused’: China sees online tributes to an official who freed Muslims in Xinjiang,” Quartz, November 18, 2019, <https://qz.com/1750441/china-sees-online-tributes-to-official-who-freed...>
 - ¹¹⁹Muyi Xiao, “It’s 5 am in China right now, but many people did not sleep tonight — hashtag ‘I want freedom of speech’ started to trend on Weibo from 1 am and now has nearly 2 million views.” photo, February 6, 2020, <https://twitter.com/muvixiao/status/1225526482497343489?s=20>
 - ¹²⁰BBC, “Fang Fang: The Wuhan writer whose virus diary angered China,” BBC, May 18, 2020, <https://www.bbc.com/news/world-asia-china-52712358>
 - ¹²¹Sarah Cook, “China Media Bulletin: 2017 YEAR IN REVIEW (Issue No. 125),” Freedom House, January 2018, <https://freedomhouse.org/china-media/china-media-bulletin-2017-year-in-...>
 - ¹²²Bill Bostock, “China enacted a sweeping new law that bars people from posting negative content online, and it could be used to suppress coronavirus news,” Business Insider, March 2, 2020, <https://www.businessinsider.com/china-internet-ban-criticism-could-supp...>; CAC, “网络信息内容生态治理规定[Regulations on the ecological governance of network information content],” CAC, December 20, 2019, http://www.cac.gov.cn/2019-12/20/c_1578375159509309.htm
 - ¹²³China Law Translate, “Governing the E-cosystem 2,” China Law Translate, March 1, 2020, <https://www.chinalawtranslate.com/en/governing-the-e-cosystem-2/>
 - ¹²⁴Rebecca Davis, “China’s New Internet Censorship Rules Outline Direction For Content,” Variety, January 3, 2020, <https://variety.com/2020/digital/news/china-censorship-law-bytedance-12...>
 - ¹²⁵Nectar Gan, “China’s internet regulator orders online AI algorithms to promote ‘mainstream values’,” South Chins Morning Post, September 11, 2019, <https://www.scmp.com/news/china/politics/article/3026784/chinas-interne...>
 - ¹²⁶Athiyah Azeem, “China’s Provinces at Forefront of Online Censorship Enforcement,” Voice of America, May 1, 2020, <https://www.voanews.com/east-asia-pacific/chinas-provinces-forefront-on...>
 - ¹²⁷Special Report, “China has the world’s most centralised internet system,” Economist, June 28, 2018, <https://www.economist.com/special-report/2018/06/28/china-has-the-world...>
 - ¹²⁸These propaganda workers are colloquially known as the 50 Cent Party due to the amount they are reportedly paid per post, though other reports have 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, <https://www.nybooks.com/daily/2013/07/10/censoring-news-before-happens-...>; 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>
 - ¹²⁹Murong Xuecun, “Beijing’s Rising Smear Power,” New York Times, September 21, 2014, <http://nyti.ms/1OvsWuZ>; 克里斯蒂安·谢泼德, “中国官媒Twitter账号被疑‘僵尸粉’过多[Chinese

- official media Twitter account suspected of too many “zombie follower”], FT中文网, November 23, 2015, <http://m.ftchinese.com/story/001064972>
- ¹³⁰Gary King, Jennifer Pan, and Margaret E. Roberts, “How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument,” *American Political Science Review* 111, no. 3 (2017): 484-501, <http://j.mp/2pGQ843>
 - ¹³¹Sarah Cook, “Welcome to the New Era of Chinese Government Disinformation,” *Diplomat*, May 11, 2020, <https://thediplomat.com/2020/05/welcome-to-the-new-era-of-chinese-gover...>; Bolsover, Gillian, and Philip Howard. “Chinese Computational Propaganda: Automation, Algorithms and the Manipulation of Information about Chinese Politics on Twitter and Weibo.” *Information, Communication & Society*, 2018, pp. 1–18., doi:10.1080/1369118x.2018.1476576.
 - ¹³²Samantha Bradshaw and Philip N. Howard, “The Global Disinformation Order: 2019 Global Inventory of Organized Social Media Manipulation,” Oxford Internet Institute, Computational Propaganda Research Project, September 4, 2019 <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberT...>
 - ¹³³“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-inter...>
 - ¹³⁴Oiwan 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-inter...>
 - ¹³⁵Sandra Fu, “Central Committee of Communist Youth League Issues an Announcement,” *China Digital Times*, January 19, 2015, <https://perma.cc/HM8P-PT9J>; Xu Yangjingjing and Simon Denyer, “Wanted: Ten million Chinese students to ‘civilize’ the Internet,” *Washington Post*, April 10, 2015, <http://wapo.st/1NbD9tb>
 - ¹³⁶Qiao Long, “留学生从‘自干五’升团中央宣传部掌控新媒体[International students promote new media from Central Propaganda Department],” *Radio Free Asia*, November 2, 2016, <http://www.rfa.org/mandarin/vataibaodao/meiti/ql2-11022016100942.html>
 - ¹³⁷Zhou Tian, “团中央新媒体：他们认同了‘团团’，就会更加认同党[Central Youth League New Media: When they identify with ‘Tuantuan’, they will identify with the Party more],” *China News Week*, February 23, 2017, https://mp.weixin.qq.com/s?_biz=MjM5MDU1Mzg3Mw==&mid=2651195974&idx=1&...
 - ¹³⁸Jack Hu and Oiwan Lam, “HKFP VOICES POLITICS & PROTEST SCIENCE & TECHNOLOGY: In quest for ‘ideological security’, China pushes to extend Communist Party influence inside tech firms,” *HKFP*, September 19, 2017, <https://www.hongkongfp.com/2017/09/10/quest-ideological-security-china-...>
 - ¹³⁹Sina, “知乎成立党支部 CEO周源称值得载入公司历史[Knowing the establishment of the party branch CEO Zhou Yuan said that it is worthy to be included in the company's history],” August 23, 2017, <http://tech.sina.com.cn/i/2017-08-23/doc-ifykiurx1211850.shtml>
 - ¹⁴⁰Chen Qingqing, “Concerns over Alibaba founder’s Party membership reflect lack of knowledge of CPC grass-roots functions: experts,” *Global Times*, November 27, 2018, <https://www.globaltimes.cn/content/1129283.shtml>.
 - ¹⁴¹Raymond Zhong and Paul Mozur, “Tech Giants Feel the Squeeze as Xi Jinping Tighten His Grip,” *New York Times*, May 2, 2018, <https://www.nytimes.com/2018/05/02/technology/china-xi-jinping-technolo...>
 - ¹⁴²CAC, “庄荣文赴新浪微博宣讲党的十九届四中全会精神[Zhuang Rongwen went to Sina Weibo to preach the spirit of the Fourth Plenary Session of the 19th Central Committee of the Party],” CAC, November 12, 2019, http://www.cac.gov.cn/2019-11/22/c_1575956636881388.htm
 - ¹⁴³Danielle Cave, Fergus Ryan & Vicky Xiuzhong Xu, “Mapping more of China's tech giants: AI and surveillance,” *Australian Strategic Policy Institute*, November 28, 2019, <https://www.aspi.org.au/report/mapping-more-chinas-tech-giants>
 - ¹⁴⁴Shan Li, “Tech Giant Tencent Caught in Chinese Regulatory Trap,” *Wall Street Journal*, August 15, 2018, <https://www.wsj.com/articles/tencent-disappoints-on-earnings-as-its-gam...>
 - ¹⁴⁵“国家网信办公布《互联网新闻信息服务管理规定》[National Network Office Announce ‘Regulations on the Administration of Internet News Information Services’],” *Sina*, May 4, 2017, <http://finance.sina.com.cn/roll/2017-05-04/doc-ifyexxhw2298844.shtml>; China Copyrights and Media, “Internet News Information Service Management Regulations”, May 2, 2017, <https://chinacopyrightandmedia.wordpress.com/2017/05/02/internet-news-i-...>
 - ¹⁴⁶“网信办颁新令 矛头指向谁[Internet Information Office issues a new order],” *DW*, May 2, 2017, <http://www.dw.com/zh/%E7%BD%91%E4%BF%A1%E5%8A%9E%E9%A2%81%E6%96%B0%E4%B...>; “Implementing Rules for the Management of Internet News Information Service,” trans. Rogier Creemers, *China Copyright and Media*, May 22, 2017, <https://chinacopyrightandmedia.wordpress.com/2017/05/22/implementing-ru...>, noting: “Specifically, those applying for an Internet news information gathering and dissemination license shall be news work units (including work units share-controlled by news work units) or work units controlled by news and propaganda departments. News work units refers to newspaper or periodical publishers, radio stations, television stations, news agencies and news film studios established lawfully and with permission of relevant state departments. Share-controlled means a proportion of over 50% of the capital contribution value, or the proportion of stock held in the total value of corporate capital, or the total share value, or, where even though the proportion in

capital contribution value or held stock is less than 50%, the capital contribution value or held stock is sufficient to engender major influence on corporate decision-making. News and propaganda departments include all levels’ propaganda departments, cybersecurity and informatization departments, radio and television departments, etc.”

- [147](#)Hogan Lovells, “Are Foreigners Banned from Publishing on the Internet in China?,” May 2016, http://f.datasrvr.com/fr/1716/75489/Final_Publishing_on_Intranet.pdf
- [148](#)Wen Yunchao, a blogger and activist in New York, says new rules for social media make it impossible for self-media to sustain themselves. “A few newspeople in China tried to use social media to report breaking news, but the CAC’s latest regulations constrain this possibility,” he told Freedom House. “That is to say, Chinese media professionals can’t earn enough from publishing on social media (like WeChat public accounts) to continue their work.” China Media Bulletin no. 125, <https://freedomhouse.org/china-media/china-media-bulletin-2017-year-in-...>. See also: “Forbidden Feeds: Government Controls on Social Media,” PEN America, March 13, 2018, <https://pen.org/wp-content/uploads/2018/06/PEN-America-Forbidden-Feeds-...>
- [149](#)Zhang Shuai, “Caixin becomes the first Chinese media outlet to erect paywalls for its products,” China Plus, October 20, 2017, <http://chinaplus.cri.cn/news/business/12/20171020/42045.html>
- [150](#)Johanna M. Costigan and Xu Xin, “China’s Digital Cultural Revolution,” Diplomat, April 29, 2020, <https://thediplomat.com/2020/04/chinas-digital-cultural-revolution/>
- [151](#)A recent example of a crackdown would be the closure of Beijing’s Unirule Institute, which founded to promote economic liberalization and democracy. It was shut down after a quarter-century amid government pressure. Chun Han Wong, “China Finally Snuffs Out a Beacon of Liberal Thought and Democracy,” Wall Street Journal, August 27, 2019, <https://www.wsj.com/articles/china-finally-snuffs-out-a-beacon-of-liber-...>
- [152](#)Viola Zhou, “Mainland Chinese evade censors to support Hong Kong protests,” Inkstone, June 13, 2019, <https://www.inkstonenews.com/politics/chinese-internet-users-evade-cens-...>
- [153](#)Darren Byler, “For China’s Muslim minority, the internet was a safe haven—until it wasn’t,” Fast Company, September 23, 2019, <https://www.fastcompany.com/90405715/for-chinas-muslim-minority-the-int-...>; China File, “Islamophobia in China,” China File, May 14, 2019, <http://www.chinafile.com/conversation/islamophobia-china>; Frankie Huang, “China’s Most Popular App Is Full of Hate,” Foreign Policy, November 27, 2018, <https://foreignpolicy.com/2018/11/27/chinas-most-popular-app-is-full-of-...>
- [154](#)Huizhong Wu, “Students in Inner Mongolia protest Chinese language policy,” AP News, September 3, 2020, <https://apnews.com/fbec428448572f4789f9b3f711d7e2f8>; Heather Chen, “The Only Mongolian-Language Social Media Site Was Shut Down in China,” Vice, August 31, 2020, https://www.vice.com/en_uk/article/xg8p7n/the-only-mongolian-language-s-...
- [155](#)Li Changshan, “For Mobile Users in China, One ‘Wrong’ Word Means Punishment,” Bitter Winter, October 6, 2020, <https://bitterwinter.org/for-mobile-users-in-china-one-wrong-word-means-...>
- [156](#)Wan Zixin, “Religious Activities Online Banned or Censored During Pandemic,” Bitter Winter, October 7, 2020, <https://bitterwinter.org/religious-activities-online-banned-or-censored-...>
- [157](#)Manish Singh, “Douyin, TikTok app in China, hits 400 million daily active users,” Tech Crunch, January 7, 2020, <https://techcrunch.com/2020/01/06/douyin-tiktok-app-in-china-hits-400-m-...>
- [158](#)David Paulk, “THREAD about how Douyin, the Chinese version of #TikTok, is banning livestreamers for speaking Cantonese instead of Mandarin,” Thread Reader, April 1, 2020, <https://threadreaderapp.com/thread/1245299840944201729.html>
- [159](#)Rik Glauert, “EXCLUSIVE: China throws out court challenge against gay online content ban,” Gay Star News, October 26, 2018, <https://www.gaystarnews.com/article/exclusive-china-throws-out-court-ch-...>
- [160](#)Rik Glauert, “Court challenge of China’s LGBTI content ban loses appeal,” Gay Star News, April 15, 2019, <https://www.gaystarnews.com/article/court-challenge-of-chinas-lgbti-con-...>
- [161](#)Aja Romano, “China has censored the Archive of Our Own, one of the internet’s largest fanfiction websites,” VOX, March 1, 2020, <https://www.vox.com/2020/3/1/21159275/china-ao3-archive-of-our-own-bann-...>
- [162](#)Ivacy, “Do You Know Which Country Has The Highest Percentage Of VPN Users?,” Ivacy, September 26, 2019, <https://www.ivacy.com/blog/do-you-know-which-country-have-the-highest-v-...>
- [163](#)Global Web Index, “VPN Users Around the World,” Global Web Index, 2018, https://www.globalwebindex.com/hubfs/Downloads/VPN_Usage_Around_The_Wor...
- [164](#)Tim Bradshaw, “Apple drops hundreds of VPN apps at Beijing’s request,” Financial Times, November 21, 2017, <https://www.ft.com/content/ad42e536-cf36-11e7-b781-794ce08b24dc>
- [165](#)Hassan Maishera, “China’s Internet Censorship Effort Continues as Authorities Blacklist Hundreds of VPN Servers,” Blokt, May 6, 2019, <https://blokt.com/news/chinas-internet-censorship-effort-continues-as-a-...>; “How does your VPN speed measure against other VPNs in China,” Circumvention Central, accessed October 12, 2020, <https://cc.greatfire.org/en>

- ¹⁶⁶Yuan Yang, “China’s ‘MeToo’ movement evades censors with #RiceBunny,” August 8, 2018, <https://www.ft.com/content/61903744-9540-11e8-b67b-b8205561c3fe>
- ¹⁶⁷Benjamin Haas, “China bans Winnie the Pooh film after comparisons to President Xi,” Guardian, August 6, 2018, <https://www.theguardian.com/world/2018/aug/07/china-bans-winnie-the-poo...>
- ¹⁶⁸“Pho noodles and pandas: How China’s social media users created a new language to beat government censorship on COVID-19,” Amnesty International, March 6, 2020, <https://www.amnesty.org/en/latest/news/2020/03/china-social-media-langu...>
- ¹⁶⁹Echo Huang, “People in China are using song lyrics as code to voice support for Hong Kong,” Quartz, June 14, 2019, <https://qz.com/1643804/chinese-internet-users-turn-to-songs-to-discuss-...>
- ¹⁷⁰Javier C. Hernandez, “China’s investigative journalists warn they are ‘almost extinct’ under Xi Jinping’s strict censorship regime,” Independent, July 14, 2019, <https://www.independent.co.uk/news/world/asia/china-investigative-journ...>
- ¹⁷¹Joey Qi, “Editor’s Pick: 2019’s Best Investigative Stories from China,” Global Investigative Journalism Network, December 16, 2019, <https://gijn.org/2019/12/16/editors-pick-2019s-best-investigative-stori...>
- ¹⁷²Sarah Cook, “China Media Bulletin: Coronavirus-era repression, propaganda, censorship, surveillance and more,” Freedom House, March 2020, <https://freedomhouse.org/report/china-media-bulletin/2020/china-media-b...>; Adam Taylor, “China’s investigative journalists offer a fraught glimpse behind Beijing’s coronavirus propaganda,” Washington Post, April 9, 2020, <https://www.washingtonpost.com/world/2020/04/08/chinas-investigative-jo...>
- ¹⁷³Sarah Cook, “Coronavirus cover-ups, disinformation, netizen pushback,” Freedom House, April 2020, <https://freedomhouse.org/report/china-media-bulletin/2020/coronavirus-c...>
- ¹⁷⁴Sarah Cook, “China Media Bulletin: Coronavirus-era repression, propaganda, censorship, surveillance and more,” Freedom House, March 2020, <https://freedomhouse.org/report/china-media-bulletin/2020/china-media-b...>
- ¹⁷⁵王廷瑜, “中國立法嚴格管控 部落客噤聲接受再教育 [Chinese legislation strictly controls bloggers clamor for reeducation],” Storm Media, July 14, 2015, <http://www.storm.mg/article/57176>
- ¹⁷⁶David Bandurski, “PREVENTING CYBER SHOCK,” China Media Project, November 17, 2018, <http://chinamediaproject.org/2018/11/17/preventing-cyber-shock/>
- ¹⁷⁷Cate Cadell, “Chinese regulator orders detailed user data to fight online mobilization,” Reuters, November 14, 2018, <https://www.reuters.com/article/china-censorship/chinese-regulator-orde...>
- ¹⁷⁸“China: Detention of activist shows unrelenting assault on freedom of expression,” Amnesty International, February 17, 2020, <https://www.amnesty.org/en/latest/news/2020/02/china-detention-of-activ...>; Shamil Shams, “China arrests pro-democracy activists in year-end crackdown,” DW, February 1, 2020, <https://www.dw.com/en/china-arrests-pro-democracy-activists-in-year-end-...>; Yibing Feng and Hai Yan, “Sentencing, Arrest of Activists Are Signs of China’s Unrelenting Crackdown,” VOA, May 6, 2020, <https://www.voanews.com/east-asia-pacific/sentencing-arrest-activists-a...>
- ¹⁷⁹Cao Yin, “Civil code defines, bans sexual harassment,” China Daily, June 1, 2020, http://www.chinadaily.com.cn/a/202006/01/WS5ed45843a310a8b241159c5e_6.h...
- ¹⁸⁰Guo Rui, “Two years on, woman who set off #MeToo in China still looking for ‘breakthrough’,” South China Morning Post, December 28, 2019, <https://www.scmp.com/news/china/politics/article/3043702/two-years-woma...>
- ¹⁸¹Sarah Cook, “China Media Bulletin: ‘Key individual’ police databases, Tiktok censorship, NBA backlash,” Freedom House, October, 2019, <https://freedomhouse.org/report/china-media-bulletin/2019/china-media-b...>
- ¹⁸²Jane Li, “Chinese citizens are racing against censors to preserve coronavirus memories on GitHub,” Quartz, March 3, 2020, <https://qz.com/1811018/chinese-citizens-use-github-to-save-coronavirus-...>
- ¹⁸³Li Yuan, “In Coronavirus Fight, China Sidelines an Ally: Its Own People,” New York Times, February 18, 2020, <https://www.nytimes.com/2020/02/18/business/china-coronavirus-charity-s...>
- ¹⁸⁴Xiao Hui, Wang Su, Zhao Ning and Denise Jia, “In Depth: Civil Society Fills in the Gaps as Virus Overwhelms Hubei,” Caixin, February 29, 2020, <https://www.caixinglobal.com/2020-02-29/in-depth-civil-society-fills-in-...>
- ¹⁸⁵Shannon Liao, “2018 was the year Chinese internet users evaded censorship — briefly,” The Verge, December 20, 2018, <https://www.theverge.com/2018/12/20/18129020/china-internet-great-firew...>
- ¹⁸⁶Roger Huang, “Chinese Netizens Use Ethereum To Avoid China’s COVID-19 Censorship,” Forbes, March 31, 2020, <https://www.forbes.com/sites/rogerhuang/2020/03/31/chinese-netizens-use...>
- ¹⁸⁷Stanley Lubman, “Arrested, Detained: A Guide to Navigating China’s Police Powers,” Wall Street Journal, August 12, 2014, <https://blogs.wsj.com/chinarealtime/2014/08/12/arrested-detained-a-guid...>
- ¹⁸⁸Xinhua, “Victims of Re-education Through Labor System Deserve Justice,” Global Times, January 28, 2013, <http://www.globaltimes.cn/content/758696.shtml>

- ¹⁸⁹Economist, “China’s strong-arm approach to drug addiction does not work,” Economist, March 21, 2020, <https://www.economist.com/china/2019/03/21/chinas-strong-arm-approach-t...>
- ¹⁹⁰Benedict Rogers, “China’s ‘Residential Surveillance at a Designated Location’ – a licence to disappear, hold and torture dissenters,” Hog Kong Free Press, February 4, 2018, <https://hongkongfp.com/2018/02/04/chinas-residential-surveillance-design...>
- ¹⁹¹Per an amendment to the criminal procedure law enacted by the National People’s Congress in 2012, which 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://cpi.org/x/49d9>
- ¹⁹²Jennifer Creery, “‘Ink girl’ who defaced Xi Jinping poster released from Chinese psychiatric facility,” Hog Kong Free Press, January 7, 2020, <https://hongkongfp.com/2020/01/07/ink-girl-defaced-xi-jinping-poster-re...>
- ¹⁹³Rogier Creemers, Paul Triolo, and Graham Webster, “Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017),” New America, June 29, 2018, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/tran...>; Jack Wagner, “China’s Cybersecurity Law: What You Need to Know,” Diplomat, June 1, 2017, <https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-...>
- ¹⁹⁴King & Wood Mallesons, “The 1st Year Implementation of the Cybersecurity Law,” China Law Insight, January 10, 2018, <https://www.chinalawinsight.com/2018/01/articles/antitrust-internationa...>
- ¹⁹⁵According to the Supreme People’s Court and the Supreme People’s Procuratorate, the top prosecutorial body, which provided a formal definition in 2013. The definition was given in 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.” Human Rights Watch, “China: Draconian Legal Interpretation Threatens Online Freedom,” September 13, 2013, <https://www.hrw.org/news/2013/09/13/china-draconian-legal-interpretatio...>; Megha Rajagopalan and Adam Rose, “China Crackdown on Online Rumors Seen as Ploy to Nail Critics,” Reuters, September 18, 2013, <https://www.reuters.com/article/net-us-china-internet/china-crackdown-o-...>
- ¹⁹⁶Freedom House, “The Politburo’s Predicament,” 2015, <https://freedomhouse.org/report/special-report/2015/politburos-predicam...>
- ¹⁹⁷“China: Draconian Legal Interpretation Threatens Online Freedom,” Human Rights Watch, September 13, 2013, <https://www.hrw.org/news/2013/09/13/china-draconian-legal-interpretatio...>
- ¹⁹⁸For example, Ilham Tohti was found guilty of “separatism” and sentenced to life in prison in September 2014. He was known for his advocacy, both online and off, for China’s Uighur minority. See Edward Wong, “China Sentences Uighur Scholar to Life,” New York Times, September 23, 2014, <https://www.nytimes.com/2014/09/24/world/asia/china-court-sentences-uig...>; Andrew Jacobs, “Uighur Intellectual Who Won’t Back Down in China,” New York Times, August 20, 2010, <https://www.nytimes.com/2010/08/21/world/asia/21china.html?module=inline>
- ¹⁹⁹“The Battle for China’s Spirit,” Freedom House, February 2017, page 115, https://freedomhouse.org/sites/default/files/FH_ChinasSprit2016_FULL_FL...
- ²⁰⁰China Law Translate, “People’s Republic of China Criminal Law Amendment (9),” September 1, 2015, <http://chinalawtranslate.com/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85...>
- ²⁰¹Xinhua, “刑法修正案下月起正式实施 微信、微博造谣最高获刑七年 [Criminal law amendments formally implemented on WeChat starting next month, up to seven years in prison for making rumors on Weibo],” Xinhuanet, October 28, 2015, http://news.xinhuanet.com/legal/2015-10/28/c_1116970714.htm
- ²⁰²Shi Jiangtao, “Chinese authorities say coronavirus control at heart of clampdown on 10 broad categories of crime,” South China Morning Post, February 12, 2020, <https://www.scmp.com/news/china/society/article/3050294/chinese-authori...>
- ²⁰³“关于依法惩治妨害新型冠状病毒感染肺炎疫情防控违法犯罪的意见[Opinions on Punishment of Crimes Obstructing the Prevention and Control of the Novel Coronavirus Infection Pneumonia Epidemic According to Law],” People.cn, February 10, 2020, <http://legal.people.com.cn/n1/2020/0210/c42510-31580349.html>
- ²⁰⁴“China: Police ‘Big Data’ Systems Violate Privacy, Target Dissent,” Human Rights Watch, November 19, 2017, <https://www.hrw.org/news/2017/11/19/china-police-big-data-systems-viola...>
- ²⁰⁵Stephanie Hegarty, “The Chinese doctor who tried to warn others about coronavirus,” BBC, February 6, 2020, <https://www.bbc.com/news/world-asia-china-51364382>
- ²⁰⁶Verna Yu, “Hero who told the truth’: Chinese rage over coronavirus death of whistleblower doctor,” Guardian, February 7, 2020, <https://www.theguardian.com/global-development/2020/feb/07/coronavirus-...>; Sarah Cook, “Coronavirus cover-ups, disinformation, netizen pushback,” Freedom House, April, 2019, <https://freedomhouse.org/report/china-media-bulletin/2020/coronavirus-c...>
- ²⁰⁷Chinese Human Rights Defenders, “China: Protect Human Rights While Combatting Coronavirus Outbreak,” Chinese Human Rights Defenders, January 31, 2020, <https://www.nchrd.org/2020/01/china-protect-human-rights-while-combatti...>

- [208](#)Weiguanwan, “遭拘留15天后山东邹城民主人士任自元（网名韩铮）今获释[Shandong Zoucheng democracy activist Ren Ziyuan (net name Han Zheng) was released today after being detained for 15 days],” Weiguanwan, February 27, 2020, <http://wqw2010.blogspot.com/2020/02/15.html>
- [209](#)Weiguanwan, “大陆疫情肆虐全国 中共当局维稳封口依旧 四川人权捍卫者谭作人遭传唤、微信冻结[China's epidemic rages across the country, the Chinese Communist Party maintains stability and seals, Sichuan human rights defender Tan Zuoren is summoned and WeChat is frozen],” Weiguanwan, February 4, 2020, http://wqw2010.blogspot.com/2020/02/blog-post_25.html
- [210](#)Yaqiu Wang, “Chinese Social Justice Activist ‘Disappeared’,” Human Rights Watch, March 11, 2020, [https://www.hrw.org/news/2020/03/11/chinese-social-justice-activist-dis-...](https://www.hrw.org/news/2020/03/11/chinese-social-justice-activist-dis-)
- [211](#)William Zheng, “Chinese scholar Zhang Xuezhong returns home after questioning over call for political reform,” South China Morning Post, May 12, 2020, [https://www.scmp.com/news/china/politics/article/3083962/chinese-schola-...](https://www.scmp.com/news/china/politics/article/3083962/chinese-schola-)
- [212](#)Committee to Protect Journalists, “Journalist Zhang Zhan arrested for covering COVID-19 in Wuhan,” Committee to Protect Journalists, May 18, 2020, [https://cpj.org/2020/05/journalist-zhang-zhan-arrested-for-covering-cov-...](https://cpj.org/2020/05/journalist-zhang-zhan-arrested-for-covering-cov-)
- [213](#)Mimi Lau, “Chinese citizen journalist arrested after reporting on coronavirus from Wuhan,” South China Morning Post, June 23, 2020, [https://www.scmp.com/news/china/politics/article/3090308/chinese-citize-...](https://www.scmp.com/news/china/politics/article/3090308/chinese-citize-); Guo Rui, “Chinese citizen journalist detained after live-streaming on coronavirus from Wuhan,” South China Morning Post, May 18, 2020, [https://www.scmp.com/news/china/politics/article/3084882/chinese-citize-...](https://www.scmp.com/news/china/politics/article/3084882/chinese-citize-)
- [214](#)Weiguanwan, “原南京师范大学副教授、南京著名人权捍卫者郭泉因揭露新冠病毒内幕、及持续为疫区人民发声遭中共当局刑事拘留后 又被以涉嫌‘煽动颠覆国家政权’正式批捕[Guo Quan, former associate professor of Nanjing Normal University and a famous human rights defender in Nanjing, was detained by the Chinese Communist Party for exposing the inside story of the new crown virus and continuing to speak out for the people in the affected area. He was officially arrested on suspicion of “inciting subversion of state power.”],” Weiguanwan, February 26, 2020, https://wqw2010.blogspot.com/2020/02/blog-post_16.html
- [215](#)Committee to Protect Journalists, “China, Turkey, Saudi Arabia, Egypt are world’s worst jailers of journalists,” Committee to Protect Journalists, December 11, 2019, [https://cpj.org/reports/2019/12/journalists-jailed-china-turkey-saudi-a-...](https://cpj.org/reports/2019/12/journalists-jailed-china-turkey-saudi-a-)
- [216](#)Chinese Human Rights Defenders, “China: Release Journalist Chen Jieren Imprisoned for 15 Years for Criticising CCP,” Chinese Human Rights Defenders, April 30, 2020, [https://www.nchrd.org/2020/04/china-release-journalist-chen-jieren-impr-...](https://www.nchrd.org/2020/04/china-release-journalist-chen-jieren-impr-)
- [217](#)Matt Ho, “Missing Chinese citizen journalist Li Zehua back online after ‘quarantine’ in coronavirus epicentre,” South China Morning Post, April 23, 2020, [https://www.scmp.com/news/china/politics/article/3081298/missing-chines-...](https://www.scmp.com/news/china/politics/article/3081298/missing-chines-)
- [218](#)BBC, “Li Zehua: Journalist who ‘disappeared’ after Wuhan chase reappears,” BBC, April 23, 2020, <https://www.bbc.com/news/world-asia-china-52392762>; Guo Rui, “Missing Chinese citizen journalist Chen Qiushi with parents under close watch,” South China Morning Post, September 24, 2020, [https://www.scmp.com/news/china/politics/article/3102757/missing-chines-...](https://www.scmp.com/news/china/politics/article/3102757/missing-chines-)
- [219](#)Emily Feng, “Rights Activist Xu Zhiyong Arrested In China Amid Crackdown On Dissent,” NPR, February 17, 2020, [https://www.npr.org/2020/02/17/806584471/rights-activist-xu-zhiyong-arr-...](https://www.npr.org/2020/02/17/806584471/rights-activist-xu-zhiyong-arr-)
- [220](#)Xu Zhiyong, Translated and Annotated by Geremie R. Barmé, “Dear Chairman Xi, It’s Time for You to Go,” China File, February 26, 2020, <https://www.chinafile.com/reporting-opinion/viewpoint/dear-chairman-xi-...>
- [221](#)许志永, “劝退书[Dismissal letter],” CMCN, February 4, 2020, <https://cmcn.blog/2020/02/04/%e5%8a%9d%e9%80%80%e4%b9%a6/>
- [222](#)Steven Jiang, Nectar Gan and Ben Westcott, “Chinese billionaire who criticized Xi Jinping over coronavirus under investigation,” CNN, April 8, 2020, <https://www.cnn.com/2020/04/08/asia/china-ren-zhiqiang-xi-jinping-coron-...>; Javier C. Hernández, “A Chinese Tycoon Denounced Xi Jinping. Now He Faces Prosecution,” New York Times, July 24, 2020, <https://www.nytimes.com/2020/07/24/world/asia/china-communist-party-ren-...>; “China Jails Xi Jinping Critic Ren Zhiqiang For 18 Years,” Radio Free Asia, September 23, 2020, <https://www.rfa.org/english/news/china/tycoon-sentence-09232020075841.h-...>
- [223](#)高峰, “发视频促习近平下台 山东诗人鲁扬遭正式逮捕[Sending video to urge Xi Jinping to step down, Shandong poet Lu Yang was formally arrested],” Radio Free Asia, June 22, 2020, <https://www.rfa.org/mandarin/yataibaodao/renquanfazhi/gf-06222020072027-...>; Taiwan News, “Chinese poet arrested for demanding Xi’s resignation in online video,” Taiwan News, June 23, 2020, <https://www.taiwannews.com.tw/en/news/3951952>
- [224](#)Asia News, “Beijing using ‘subversion’ charges to suppress democratic voices,” Asia News, June 25, 2020, <http://www.asianews.it/news-en/Beijing-using-‘subversion’-charges-to-su-...>
- [225](#)Chinese Human Rights Defenders, “Chen Jiahong 陈家鸿,” Chinese Human Rights Defenders, April 14, 2020, <https://www.nchrd.org/2020/04/chen-jiahong/>

- [226](#)Yibing Feng, Hai Yan, “Sentencing, Arrest of Activists Are Signs of China’s Unrelenting Crackdown,” VOA, May 6, 2020, <https://www.voanews.com/east-asia-pacific/sentencing-arrest-activists-a...>
- [227](#)小山, “因“煽動顛覆國家政權罪”指控 中國維權律師余文生今被秘密判刑4年[Chinese rights lawyer Yu Wensheng was secretly sentenced to 4 years in prison for “inciting subversion of state power”],” Rfi, June 17, 2020, <https://perma.cc/676X-N7HY>.
- [228](#)Guo Rui, “Chinese human rights lawyer Yu Wensheng sentenced to four years in prison,” South China Morning Post, June 17, 2020, <https://www.scmp.com/news/china/politics/article/3089441/chinese-human-...>
- [229](#)Chinese Human Rights Defenders, “Defending Human Rights in the Era of Dystopia: The Situation of Defenders in China (2019),” Chinese Human Rights Defenders, February 12, 2020, <https://www.nchrd.org/2020/02/defending-human-rights-in-the-era-of-dyst...>; Frances Eve, “#StandWithHongKong is Essentially a Crime in Mainland China,” China Human Rights Defenders, September 23, 2019, <https://www.nchrd.org/2019/09/standwithhongkong-is-essentially-a-crime-...>
- [230](#)Gao Feng, “Activist Held in China’s Chongqing Over Social Media Comment About Hong Kong,” RFA, August 6, 2019, <https://www.rfa.org/english/news/comment-08062019130629.html>
- [231](#)Lily Kuo, “‘We can’t do anything’: China accused of muffling voices of Hong Kong supporters,” Guardian, September 10, 2020, <https://www.theguardian.com/world/2019/sep/11/we-cant-do-anything-china...>
- [232](#)Mimi Lau, “Police detain Chinese #MeToo activist Sophia Huang Xueqin on public order charge,” South China Morning Post, October 24, 2019, <https://www.scmp.com/news/china/politics/article/3034389/police-detain-...>
- [233](#)Laurie Chen, “Chinese #MeToo activist Sophia Huang Xueqin freed from detention, lawyers and sources say,” South China Morning Post, January 18, 2020, <https://www.scmp.com/news/china/politics/article/3046643/chinese-metoo-...>
- [234](#)Lily Kuo and agencies, “China’s first ‘cyber-dissident’ jailed for 12 years,” Guardian, July 29, 2019, <https://www.theguardian.com/world/2019/jul/29/china-first-cyber-disside...>
- [235](#)China Labour Bulletin, “Labour activist Chen Weixiang released from detention,” China Labour Bulletin, January 3, 2020, <https://clb.org.hk/content/labour-activist-chen-weixiang-released-deten...>
- [236](#)Agence France-Presse, “Former Chinese rights lawyer arrested for ‘inciting subversion’,” South China Morning Post, December 7, 2019, <https://www.scmp.com/news/china/politics/article/3041101/former-chinese-...>
- [237](#)Radio Free China, “Court in China’s Chongqing Jails WeChat Foreign News Service Moderator,” Radio Free China, June 27, 2016, <https://www.rfa.org/english/news/china/wechat-surveillance-062720191502...>
- [238](#)Gabi Verberg, “Chinese Media Warn WeChat Group Admins: ‘You Can Be Arrested for What Happens in Your Group Chat,’” What’s on Weibo, May 1, 2019, <https://www.whatsonweibo.com/chinese-media-warn-wechat-group-admins-you...>
- [239](#)Weiquan, “广州公民陈宗因组建微信群而获罪 被判刑1年3个月[Guangzhou citizen Chen Zong convicted of forming a WeChat group and sentenced to 1 year and 3 months in prison],” Weiquan, July 7, 2020, <https://wqw2010.blogspot.com/2020/07/13.html>; CHRД人权捍卫者, “Chen Zong, a Guangzhou-based citizen, sentenced to 15 months’ imprisonment (‘picking quarrels & provoking trouble’) just for setting up WeChat groups (冰火岛), using a VPN to access overseas websites & sharing information from those sites to the groups <https://wqw2010.blogspot.com/2020/07/13.html>,” Twitter, July 6, 2020, <https://twitter.com/CHRDnet/status/1280194508433403904>
- [240](#)Bethany Allen-Ebrahimian, “University of Minnesota student jailed in China over tweets,” Axios, January 23, 2020, <https://www.axios.com/china-arrests-university-minnesota-twitter-e495cf...>
- [241](#)Chun Han Wong and Joyu Wang, “China Detains Taiwanese Businessman,” Wall Street Journal, September 11, 2019, <https://www.wsj.com/articles/china-detains-taiwanese-businessman-115682...>
- [242](#)Callum Tennent, “Man Arrested in China for Selling VPN Software,” Top 10 VPN, January 6, 2020, <https://www.top10vpn.com/research/opinion/man-arrested-in-china-for-sel...>; Catalin Cimpanu, “Chinese man arrested after making \$1.6 million from selling VPN services,” ZD Net, January 16, 2020, <https://www.zdnet.com/article/chinese-man-arrested-after-making-1-6-mil...>
- [243](#)Masha Borak, “Man arrested for selling VPN to hop the Great Firewall,” South China Morning Post, January 3, 2020, <https://www.scmp.com/abacus/tech/article/3044407/man-arrested-selling-v...>
- [244](#)Gao Feng, “Fine For VPN Use Sparks Rare Backlash on Chinese Internet,” RFA, May 21, 2020, <https://www.rfa.org/english/news/china/vpn-punishments-05212020103537.h...>
- [245](#)Phoebe Zhang, “Chinese activists detained after sharing censored coronavirus material on crowdsourcing site Github,” South China Morning Post, April 25, 2020, <https://www.scmp.com/news/china/politics/article/3081569/chinese-activi...>; Guo Rui, “Coronavirus: Chinese activists held for posting censored articles to face trial on criminal charges,” South China Morning Post, June 14, 2020, <https://www.scmp.com/news/china/society/article/3089002/coronavirus-chi...>
- [246](#)“China: Massive Crackdown in Muslim Region,” Human Rights Watch, September 9, 2018, <https://www.hrw.org/news/2018/09/09/china-massive-crackdown-muslim-regi...>

- [247](#)Adrian Zanz, “New Evidence for China’s Political Re-Education Campaign in Xinjiang,” The Jamestown Foundation, May 15, 2018, <https://jamestown.org/program/evidence-for-chinas-political-re-educatio...>
- [248](#)“China has turned Xinjiang into a police state like no other,” Economist, May 31, 2018, <https://www.economist.com/briefing/2018/05/31/china-has-turned-xinjiang...>
- [249](#)Uyghur Human Rights Project, “‘Ideological Transformation’: Records of Mass Detention from Qaraqash, Hotan,” February, 2020, https://docs.uhrp.org/pdf/UHRP_QaraqashDocument.pdf
- [250](#)Gene A. Bunin, “Xinjiang’s Hui Muslims Were Swept Into Camps Alongside Uighurs,” FP, February 10, 2020, <http://archive.vn/GLu1h>; Emily Feng, “‘Afraid We Will Become The Next Xinjiang’: China’s Hui Muslims Face Crackdown,” NPR, September 26, 2019, <https://www.npr.org/2019/09/26/763356996/afraid-we-will-become-the-next...>
- [251](#)Ng Yik-tung and Sing Man, “China Detains Hui Muslim Poet Who Spoke Out Against Xinjiang Camps,” RFA, January 27, 2020, <https://www.rfa.org/english/news/china/poet-01272020163336.html>; Pen America, “Pen America Concerned Over Detained Chinese Poet’s Safety,” Pen America, March 5, 2020, <https://pen.org/press-release/pen-concerned-poet-safety/>
- [252](#)Josh Rogin, “China’s camps now have survivors, and their ordeals aren’t over,” Washington Post, January 23, 2020, <https://www.washingtonpost.com/opinions/global-opinions/chinas-camps-no...>
- [253](#)Tibetan Centre for Human Rights and Democracy, “Tibetan man sentenced to prison for sharing books on WeChat,” Tibetan Centre for Human Rights and Democracy, <https://tchrd.org/tibetan-man-sentenced-to-prison-for-sharing-books-on-...>
- [254](#)Lobe Socktsang, “Tibetan Man Detained For Sharing Dalai Lama Photo on WeChat,” RFA, August 26, 2019, <https://www.rfa.org/english/news/tibet/photo-08262019142526.html>
- [255](#)“Monk from Tibet’s Amdo Ngaba arrested over social media posts on Tibetan Language,” Central Tibetan Administration, October 5, 2019, <https://tibet.net/monk-from-tibets-amdo-ngaba-arrested-over-social-medi...>
- [256](#)Sarah Cook, “The Battle for China’s Spirit: Religious Revival, Repression, and Resistance under Xi Jinping,” New York: Freedom House, 2017, <https://freedomhouse.org/report/china-religious-freedom>
- [257](#)Josh Rogin, “China’s camps now have survivors, and their ordeals aren’t over,” Washington Post, January 23, 2020, <https://faluninfo.net/during-pandemic-police-in-china-detain-those-trvi...>
- [258](#)Falun Info, “WeChat, Facial Recognition in China’s Police State Targets Falun Gong,” Falun Info, September 24, 2020, <https://faluninfo.net/wechat-facial-recognition-in-chinas-police-state-...>
- [259](#)Falun Info, “WeChat, Facial Recognition in China’s Police State Targets Falun Gong,” Falun Info, September 24, 2020, <https://faluninfo.net/wechat-facial-recognition-in-chinas-police-state-...>
- [260](#)Catherine Shu, “China doubles down on real-name registration laws, forbidding anonymous online posts,” Tech Crunch, August 28, 2017, <https://techcrunch.com/2017/08/27/china-doubles-down-on-real-name-regis...> Samm Sacks and Paul Triolo, “Shrinking Anonymity in Chinese Cyberspace,” Lawfare (blog), September 25, 2017, <https://www.lawfareblog.com/shrinking-anonymity-chinese-cyberspace>
- [261](#)Tim Stratford et al., “China Enacts New Data Privacy Legislation,” Covington & Burling LLP, January 11, 2013, <https://www.cov.com/en/news-and-insights/insights/2013/01/china-enacts-...>
- [262](#)Huo Jingnan, “China Introduces Restrictions On Video Games For Minors,” NPR, November 6, 2019, <https://www.npr.org/2019/11/06/776840260/china-introduces-restrictions-...>
- [263](#)C. Custer, “China to start seriously enforcing real-name mobile registration, government claims,” Tech In Asia, May 31, 2016, <https://www.techinasia.com/china-start-enforcing-realname-mobile-regist...>
- [264](#)Danny O’Brien, “China’s name registration will only aid cybercriminals,” Committee to Protect Journalists blog, December 28, 2012, <https://cpj.org/x/5177>
- [265](#)BBC, “China due to introduce face scans for mobile users,” BBC, December 1, 2019, <https://www.bbc.com/news/world-asia-china-50587098>
- [266](#)Radio Free Asia, “Chinese Police Order Businesses to Monitor Use of Public Wi-fi,” Radio Free Asia, April 6, 2017, <http://www.rfa.org/english/news/china/monitor-04062017121748.html>
- [267](#)Chris Buckley, “China Passes Antiterrorism Law That Critics Fear May Overreach,” New York Times, December 28, 2015, <http://www.nytimes.com/2015/12/28/world/asia/china-passes-antiterrorism...>
- [268](#)Adan Segal, “The Cyber Trade War,” Foreign Policy, October 25, 2014, <http://atfp.co/1Oq5LzN>
- [269](#)Yan Luo, Eric Carlson and Zhijing Yu, “China Enacts Encryption Law,” Inside Privacy, October 31, 2019, <https://www.insideprivacy.com/data-security/china-enacts-encryption-law/>
- [270](#)Bai Tiantian, “Xinjiang asks real-name registration for cellphones, PCs,” Global Times, January 29, 2015, <http://www.globaltimes.cn/content/904898.shtml>
- [271](#)Josh Rudolph, “Clean up harmful information, report wall-scaling tool,” China Digital Times, April 12, 2018, <https://chinadigitaltimes.net/2018/04/notice-clean-up-harmful-informati...>

- [272](#)AFP, “‘They have no clue about network security’: China data leak exposes mass surveillance across Muslim Xinjiang,” Hong Kong Free Press, February 20, 2019, <https://www.hongkongfp.com/2019/02/20/no-clue-network-security-china-da...>
- [273](#)Phil Muncaster, “Xinjiang Users Arrested over State Spyware Usage,” Infosecurity Magazine, July 24, 2017, <https://www.infosecurity-magazine.com/news/xinjiang-arrested-state-spyw...>
- [274](#)Adam Lynn, “APP TARGETING UYGHUR POPULATION CENSORS CONTENT, LACKS BASIC SECURITY,” Open Technology Fund, August 31, 2018, <https://www.opentech.fund/news/app-targeting-uyghur-population-censors-...>
- [275](#)Alexandra Ma, “China used a file-sharing app to round up 40,000 Uighur Muslims for prison camps, a startling insight into how it oppresses people via technology,” Business Insider, November 25, 2019, <https://www.businessinsider.com/china-uyghurs-prison-camps-round-up-zap...>
- [276](#)Josh Chin and Clément Bürge, “Twelve Days in Xinjiang: How China’s Surveillance State Overwhelms Daily Life,” Wall Street Journal, December 19, 2017, <https://www.wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveil...>
- [277](#)Hilary Osborne and Sam Cutler, “Chinese border guards put secret surveillance app on tourists’ phones,” Guardian, July 2, 2019, <https://www.theguardian.com/world/2019/jul/02/chinese-border-guards-sur...>
- [278](#)Raymond Zhong, “Going From Hong Kong to Mainland China? Your Phone Is Subject to Search,” New York Times, August 15, 2019, <https://www.nytimes.com/2019/08/15/world/asia/hong-kong-protest-phone-c...>
- [279](#)Samuel Wade, “China’s social credit system: Black Mirror or red herring?,” China Digital Times, February 16, 2017, <http://chinadigitaltimes.net/2017/02/qa-shazeda-ahmed-on-chinas-social-...>
- [280](#)China Law Translate, “Establishment of a Social Credit System,” China Law Translate, April 27, 2015, <http://archive.vn/Z0H0W>
- [281](#)Louise Matsakis, “How the West Got China’s Social Credit System Wrong,” Wired, July 29, 2019, <https://www.wired.com/story/china-social-credit-score-system/>; Bloomberg, “China’s trial program to rate citizens on public behavior is a bureaucratic mess,” LA Times, June 21, 2019, <https://www.latimes.com/business/la-fi-china-big-brother-social-credit-...>
- [282](#)Dev Lewis, “All Carrots and No Sticks: A Case Study on Social Credit Scores in Xiamen and Fuzhou,” Digital Asia Hub, October 11, 2019, <https://www.digitalasiahub.org/2019/10/11/all-carrots-and-no-sticks-a-c...>
- [283](#)Samuel Wade, “China’s social credit system: Black Mirror or red herring?,” China Digital Times, February 16, 2017, <https://www.scmp.com/news/china/politics/article/2167240/chinese-police-...>
- [284](#)Laney Zhang, “Global Legal Monitor,” Library of Congress, November 13, 2018, <https://www.loc.gov/law/foreign-news/article/china-new-regulation-on-po...>; 中共中央网络安全和信息化委员会办公室 (CAC), “具有舆论属性或社会动员能力的互联网信息服务安全评估规定[Regulation on Internet Information Service Security Assessment with Paradoxical Attributes or Social Mobilization Capabilities],” November 15, 2018, http://www.cac.gov.cn/2018-11/15/c_1123716072.htm
- [285](#)武陵公安, “运营商也需履行网络安全责任, 否则依法处罚[Network operators also need to fulfill their network security responsibilities, otherwise they will be punished according to law],” January 8, 2019, <https://mp.weixin.qq.com/s?biz=MzI4OTYzNTc4NQ==&mid=2247485693&idx=1&...>
- [286](#)Celia Chen, “China’s regulatory oversight of booming online travel platforms will include censorship of ‘illegal’ content,” South China Morning Post, October 16, 2019, <https://www.scmp.com/tech/apps-social/article/3033025/chinas-regulatory-...>
- [287](#)Luo Jieqi, “Cleaning Up China’s Secret Police Sleuthing,” Caixin, January 24, 2013, <https://www.caixinglobal.com/2013-01-24/cleaning-up-chinas-secret-polic-...>
- [288](#)Per 2010 amendments. See Central People’s Government of the People’s Republic of China, “Presidential order of the People’s Republic of China, No. 28” [中华人民共和国主席令], April 29, 2010, http://www.gov.cn/fbg/2010-04/30/content_1596420.htm; Jonathan Ansfield, “China Passes Tighter Information Law,” New York Times, April 29, 2010, <http://nyti.ms/1LMMx9j>
- [289](#)NPC, “中华人民共和国国家情报法[National Intelligence Law of the People’s Republic of China],” NPC, June 27, 2017, http://www.npc.gov.cn/zgrdw/npc/xinwen/2017-06/27/content_2024529.htm
- [290](#)Economist, “China’s new cyber-security law is worryingly vague,” Economist, June 1, 2017, <https://www.economist.com/news/business/21722873-its-rules-are-broad-am...>
- [291](#)He Huifeng and Nectar Gan, “All mainland app providers ordered to keep user logs for months to curb spread of ‘illegal information,’” SCMP, June 28, 2016, <http://www.scmp.com/news/china/policies-politics/article/1982756/all-ma...>
- [292](#)OpenNet Initiative, “China,” August 9, 2012, <http://opennet.net/research/profiles/china-including-hong-kong>
- [293](#)Victor Gever, @0xDUDE, “One of the multiple intelligence feeds showing the distribution of triggered events routed to the police stations identified by numbers,” March 3, 2019, <https://twitter.com/0xDUDE/status/1102303971765641216/photo/1>

- [294](#)Jeffrey Knockel, Christopher Parsons, Lotus Ruan, Ruohan Xiong, Jedidiah Crandall, and Ron Deibert, “How International Users Unwittingly Build up WeChat’s Chinese Censorship Apparatus,” The Citizen, May 7, 2020, <https://citizenlab.ca/2020/05/we-chat-they-watch/>
- [295](#)Open Technology Fund, “Studying ‘Study the Great Nation,’” Open Technology Fund, October 12, 2019, <https://www.opentech.fund/news/studying-study-the-great-nation/>
- [296](#)Norton Rose Fulbright, “Contact tracing apps in China,” Norton Rose Fulbright, May 11, 2020, <https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/contact-tr...>
- [297](#)Paul Mozur, Raymond Zhong and Aaron Krolik, “In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags,” New York Times, August 7, 2020, <https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveilla...>
- [298](#)Paul Mozur, Daisuke Wakabayashi and Nick Wingfield, “Apple Opening Data Center in China to Comply With Cybersecurity Law,” New York Times, July 12m 2017, <https://www.nytimes.com/2017/07/12/business/apple-china-data-center-cyb...>
- [299](#)Shannon Liao, “Apple officially moves its Chinese iCloud operations and encryption keys to China,” The Verge, February 28, 2018, <https://www.theverge.com/2018/2/28/17055088/apple-chinese-icloud-accoun...>
- [300](#)Reuters, “Apple to build a second data center in China: Xinhua,” February 6, 2018, <https://www.reuters.com/article/us-apple-datacenter/apple-to-build-a-se...>
- [301](#)Yoko Kubota and Tripp Mickle, “Apple’s Challenge: Win Over China With Pricey New iPhones,” Wall Street Journal, September 13, 2018, <https://www.wsj.com/articles/apple-faces-uphill-battle-to-win-over-chin...>
- [302](#)China Bidding, “陆丰市公安局陆丰市涉毒重点人员数据库系统及移动警务APP系统建设项目竞争性谈判采购公告[Lufeng City Public Security Bureau Lufeng City Key Drug-related Personnel Database System and Mobile Police APP System Construction Project Competitive Negotiation Procurement Announcement],” China Bidding, May 6, 2019, <http://www.chinabidding.com/bidDetail/239174831.html>
- [303](#)China Bidding, “天津市公安局第六处涉恐涉稳重点人管控子系统项目（项目编号：TGPC-2015-D-0624）成交公告[Announcement on the Transaction of the Management and Control Subsystem Project of Key Persons Involving Terrorism and Stability of the Sixth Division of Tianjin Public Security Bureau (Project Number: TGPC-2015-D-0624)],” China Bidding, October 14, 2015, <http://www.chinabidding.com/bidDetail/226484108-BidResult.html>
- [304](#)Emile Dirks, Sarah Cook, “China’s Surveillance State Has Tens of Millions of New Targets,” Foreign Policy, October 21, 2019, <https://foreignpolicy.com/2019/10/21/china-xinjiang-surveillance-state-...>
- [305](#)Gao Feng and Wong Lok-to, “Chinese Police Target Activists Who Supported Hong Kong Protests,” RFA, June 1, 2020, <https://www.rfa.org/english/news/china/target-06012020144022.html>.
- [306](#)Emile Dirks and Sarah Cook, “China’s Surveillance State Has Tens of Millions of New Targets,” Foreign Policy, October 21, 2019, <https://foreignpolicy.com/2019/10/21/china-xinjiang-surveillance-state-...>
- [307](#)China Blog Staff, “Sorry, no comment - we might get invited to tea,” China Blog, BBC, December 9, 2013, <http://bbc.in/1LKxO0k>
- [308](#)“Chinese Police Target Activists Who Supported Hong Kong Protests,” Radio Free Asia, June 1, 2020, <https://www.rfa.org/english/news/china/target-06012020144022.html>.
- [309](#)Kris Cheng, “Liu Xia, widow of Nobel laureate Liu Xiaobo, ‘forced to travel’ ahead of China’s key Congress meeting, says NGO,” Hong Kong Free Press, October 16, 2017, <https://www.hongkongfp.com/2017/10/16/liu-xia-widow-nobel-laureate-liu-...>
- [310](#)Minghui.org, “40 Falun Gong Practitioners Persecuted to Death, 5,313 Targeted in First Half of 2020,” Falun Info, August 12, 2020, <https://faluninfo.net/40-falun-gong-practitioners-persecuted-to-death-5...>
- [311](#)Shohret Hoshur, “Uyghur Youth Held After Posting Rare Videos Criticizing Government From Inside China,” RFA, September 18, 2020, <https://www.rfa.org/english/news/uyghur/videos-09182020174137.html?sear...>
- [312](#)“Defending Human Rights in the Era of Dystopia: The Situation of Defenders in China (2019),” Chinese Human Rights Defenders, February 12, 2020, <https://www.nchrd.org/2020/02/defending-human-rights-in-the-era-of-dyst...>
- [313](#)“Tiger Chairs and Cell Bosses: Political Torture of Criminal Suspects in China,” Human Rights Watch, May 13, 2015, <https://www.hrw.org/report/2015/05/13/tiger-chairs-and-cell-bosses/poli...>
- [314](#)Agence France-Presse, “Chinese activist Huang Qi will die in custody if denied medical treatment – rights groups,” South China Morning Post, November 5, 2018, <https://www.scmp.com/news/china/society/article/2171746/chinese-activis...>
- [315](#)Isobel Cockerell, “Inside China’s Massive Surveillance Operation,” Weird, May 9, 2019, <https://www.wired.com/story/inside-chinas-massive-surveillance-operatio...>
- [316](#)Willem Marx and Olivia Sumrie, “Uighurs accuse China of mass detention, torture in landmark complaint,” NBS NEWS, September 9, 2020, <https://www.nbcnews.com/news/world/uighurs-accuse-china-mass-detention-...>

- [317](#)Pema Ngodup, "Tibetan Monk Dies After Living Two Years With Torture Injuries Sustained in Custody," RFA, April 24, 2020, <https://www.rfa.org/english/news/tibet/gendun-sherab-04242020150923.html>
- [318](#)BBC News, "Fang Fang: The Wuhan writer whose virus diary angered China," BBC News, May 18, 2020, <https://www.bbc.com/news/world-asia-china-52712358>
- [319](#)"艾米, "发文挺方方的湖北大学教授梁艳萍遭"校方调查" [Hubei University professor Liang Yanping who published an article supporting Fang Fang was "investigated by the school"]," rfi, April 27, 2020, <https://perma.cc/5C3Z-EPTS>.
- [320](#)Akamai, "State of the internet/security Q4 2017 report," <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet...>
- [321](#)Mara Hvistendahl, "The Decline in Chinese Cyberattacks: The Story Behind the Numbers," MIT Technology Review, October 25, 2016, <https://www.technologyreview.com/s/602705/the-decline-in-chinese-cybera...>
- [322](#)08宪章论坛, "零八宪章论坛所有内容于4月24日突然被人为删除, 由零八宪章签署人义务服务近10年的博客已经"被不存在"! 近期除了博客, 此推特账号亦多次受到攻击。[All contents of Charter 08 Forum were suddenly deleted artificially on April 24, and the blog that has been volunteered by Charter 08 signatories for nearly 10 years has been "non-existent"! In addition to blogs recently, this Twitter account has also been attacked many times.]," Twitter, April 24, 2019, <https://twitter.com/08charterbbs/status/1121247488017457152>
- [323](#)Paul Mozur, "Twitter Users in China Face Detention and Threats in New Beijing Crackdown," New York Times, January 10, 2019, <https://www.nytimes.com/2019/01/10/business/china-twitter-censorship-on...>
- [324](#)Andrew Case, Matthew Meltzer and Steven Adair, "Digital Crackdown: Large-Scale Surveillance and Exploitation of Uyghurs," Volatility, September 2, 2019, <https://www.volatility.com/blog/2019/09/02/digital-crackdown-large-scale-...>
- [325](#)Andy Greenberg, "Amid Its Covid-19 Crisis, China Was Still Hacking Uighurs' iPhones," Wired, April 22, 2020, <https://www.wired.com/story/amid-covid-19-crisis-china-hacking-ughur-i...>

ecoi.net summary:

Report on digital media and
internet freedom (reporting period
June 2019 - May 2020)

Country:

China

Source:

[Freedom House](#)

Original link:

<https://freedomhouse.org/country/china/freedom-net/2020>

Document type:

Periodical Report

Language:

English

Published:

14 October 2020

Document ID:

2039060

Austrian Red Cross Austrian Centre for Country of Origin and Asylum Research and Documentation (ACCORD)	Wiedner Hauptstraße 32, 1041 Wien T (Telefon) +43 1 589 00 583 F (Fax) +43 1 589 00 589 info@ecoi.net	Contact Imprint & Disclaimer F.A.Q. Data Protection Notice
--	---	---

ecoi.net is run by the Austrian Red Cross (department ACCORD) in cooperation with Informationsverbund Asyl & Migration. ecoi.net is funded by the Asylum, Migration and Integration Fund, the Austrian Ministry of the Interior and Caritas Austria. ecoi.net is supported by ECRE & UNHCR.

