China's Cyber Superpower Strategy: Implementation, Internet Freedom Implications, and U.S. Responses

Written Testimony by Sarah Cook
Senior Research Analyst for East Asia and China Media Bulletin Director

House Committee on Oversight and Government Reform, Subcommittee on Information Technology

Countering China: Ensuring America Remains the World Leader in Advanced Technologies and Innovation

September 26, 2018

Chairman Hurd, Ranking Member Kelly, and members of the subcommittee, it is an honor to testify before you today. I have divided my comments into four parts:

I. A brief overview of the Chinese Communist Party's strategy for becoming a "Cyber Superpower"
II. Examples of how this is being implemented, often with the assistance of Chinese and foreign technology companies
III. Analysis of the costs these dynamics impose on human rights, internet freedom, and tech companies themselves
IV. Recommendations for steps the U.S. government can take in response to these trends
V. Concluding thoughts based on Freedom House experience

China's "cyber superpower" strategy

Last fall, the Chinese Communist Party (CCP) declared its aspirations for China to become a "cyber superpower," the desired outcome of developing improved capabilities and influence in areas ranging from domestic censorship to high-tech innovation to global internet governance.

During his October 2017 speech to the 19th Party Congress, Chinese president and CCP head Xi Jinping emphasized the importance of innovation as China emerges as a world power.[1] The speech was preceded by a detailed article published in the vanguard Party journal *Qiushi*

[1] Freedom House, China Media Bulletin, No. 126, November 4, 2017, https://freedomhouse.org/china-media/china-media-bulletin-party-congress-media-vision-surveillance-updates-africa-impact-issue-no-123

the month before outlining the full details of Xi and the CCP's vision for achieving "cyber superpower" 网络强国 (*wǎngluò qiángguó)* status.[2] The piece—authored by officials at the Cyberadministration of China (CAC), the country's top internet regulator—is at times surprisingly candid about the Party's ambitions and motives in several areas relevant to today's discussion:

- **Increasing domestic Chinese internet controls to ensure authoritarian longevity**: The authors note that the goal of strengthening "positive energy" online and making innovations in propaganda and content controls is "so that the Party's ideas always become the strongest voice in cyberspace." The article acknowledges that controlling the internet is key to the party's own political survival, stating that "If our party cannot traverse the hurdle represented by the Internet, it cannot traverse the hurdle of remaining in power for the long term." A central element of strengthening party leadership in the cybersecurity and information technology field includes safeguarding "Comrade Xi Jinping as the core of Party Central Committee authority."

- **Using the technology sector as a foundation to secure China's economic health at a time of reduced GDP growth rates**: A central part of the strategy laid out is to "accelerate indigenous innovation of core technologies in the information field," "obtain breakthroughs,' and "narrow the gap with developed countries" in areas like artificial intelligence, cloud computing, and 5G mobile networks. Other aspects of the CCP's strategy in this regard include developing the digital economy and continuing to enhance the "global influence of internet companies like Alibaba, Tencent, Baidu, [and] Huawei," as well as supporting the international adoption of Beidou satellite navigation as an example of military-civilian integration.

- **Expanding information controls beyond China's borders:** The article's authors note that online propaganda should also target international audiences with the goal of "expanding online international communication to 200 countries … and more than 1 billion overseas users." They also state that the purpose of strengthening international exchanges and cooperation in the field of information technology and cybersecurity—including with the United States—is "to push China's proposition of Internet governance toward becoming an international consensus."

Prioritization and effective implementation of such CCP strategies related to cyberspace has emerged as a hallmark of Xi Jinping's leadership of the Communist Party since 2012. Compared to his predecessor Hu Jintao, Xi is more sophisticated in his understanding of how the internet and social media applications function, as well as how free expression in the

[2] Elsa Kania, Samm Sacks, Paul Triolo, and Graham Webster, "China's Strategic Thinking on Building Power in Cyberspace," *New America*, September 25, 2017, https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/

online sphere could pose an existential political threat to the CCP. He has also proved himself to be adept at closing previously existing loopholes in internet controls that enabled tens of millions of Chinese netizens to share breaking news, expose corruption and rights abuses, debate government policies, and have an occasional laugh at the expense of CCP leaders. This track record of Xi's within China—as well as the full scale and impact of the domestic internet control apparatus—are worth keeping in mind when considering the CCP's commitment to implementing the dimensions of his vision with international implications. Even before the above article's publication outlining this strategy, China's authoritarian regime had begun taking steps to achieve its stated goals, adopting and implementing a new Cybersecurity Law and declaring its Made in China 2025 policy. But over the past year, China has taken new strides in technological advancement and international expansion.

Technological innovation in China, for better or for worse

Some aspects of the Chinese government's innovation drive have clear public benefits. The number of internet users in China has grown exponentially over the past 15 years, reaching an estimated 802 million people as of June, more than double the entire population of the United States. The vast majority of these Chinese users access the internet via their mobile phones.[3] That access is set to get a new boost. In August, state-owned China Unicom successfully launched and tested its first 5G experimental network in Beijing, the next generation of high-speed mobile web access, which it plans to have rolled out across the city by next summer.[4]

But other advances are more problematic. Although widespread mobile web connectivity engenders many benefits, it also personalizes censorship and surveillance practices to an unprecedented degree. This is especially the case when, alongside increased access to internet services, China's ruling Communist Party has developed the world's most multi-layered and sophisticated internet control apparatus. For the past three years, China has been the worst abuser of internet freedom among 65 countries assessed in Freedom House's annual *Freedom on the Net* report.[5]

Yet even with that robust baseline, the past year has seen new waves of tightening in areas of free expression or dissemination channels that were previously tolerated. Since a new Cybersecurity Law came into effect in June 2017, online censorship and surveillance have expanded dramatically alongside increasing arrests of Chinese citizens, particularly for content shared on the popular instant messaging platform WeChat.

---

[3] China Internet Network Information Center. (2018). *Statistical Report on Internet Development in China*. Retrieved from https://cnnic.com.cn/IDR/ReportDownloads/201807/P020180711391069195909.pdf
[4] Sina, "Beijing enters 5G network era with China Unicom's experimental sites," August 14, 2018, http://english.sina.com/buz/b/2018-08-14/detail-ihhtfwqq8823911.shtml
[5] Freedom House, *Freedom on the Net 2017,* November 2017, https://freedomhouse.org/report/freedom-net/freedom-net-2017.

Technical and regulatory innovation and experimentation is constantly underway. Additions to the censorship and surveillance toolbox from the past year include: large-scale shuttering of social media accounts rather than just deleting posts and particularly influential accounts, forcing the removal of hundreds of mobile phone apps that enable users to reach blocked websites, and the mass purchasing by security agencies of devices for extracting and scanning the contents of smartphones.[6]

Chinese technology firms at the forefront

Chinese technology companies have been central to censorship advancements. For example, some firms are developing the ability to automatically scan images for subversive text rather than relying solely on human censors. An August 14 report by the Toronto-based Citizen Lab revealed two forms of image censorship being deployed by Tencent's mobile application WeChat[7]: One tool filters images containing sensitive text, and the other snags those that are visually similar to images already on a blacklist. Social media users have long posted images to circumvent censorship of simple text, and these new capabilities could close that loophole. Tencent has taken a number of other steps since May to meet the government's censorship demands. It has barred users from linking to external videos in chat groups,[8] deleted large numbers of audio and video clips (including those deemed to "distort history"),[9] and banned users from making changes to their profile pictures or user names—a common form of commentary—during the June summit of the Shanghai Cooperation Organization, the regional security bloc led by China.[10]

In the realm of surveillance, the western region of Xinjiang has become a laboratory for testing big-data, facial-recognition, and smartphone-scanner technologies that can eventually be deployed across China and beyond. Several firms have emerged at the cutting edge of this effort, including CloudWalk, Hikvision, Dahua, SenseTime, and Yitu.[11] Although

---

[6] Freedom House, *China Media Bulletin,* No. 121, September 11, 2017, https://freedomhouse.org/china-media/china-media-bulletin-party-congress-censorship-vpn-crackdown-surveillance-upgrades-no-121; Freedom House, *China Media Bulletin,* No. 127, March 23, 2018, https://freedomhouse.org/china-media/china-media-bulletin-risks-of-xis-power-grab-npc-censorship-xinjiang-reprisals-issue-no-127. Cate Cadell, "From laboratory in far west, China's surveillance state spreads quietly," *Reuters*, August 14, 2018, https://www.reuters.com/article/us-china-monitoring-insight/from-laboratory-in-far-west-chinas-surveillance-state-spreads-quietly-idUSKBN1KZ0R3

[7] Jeffrey 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-filtering-on-wechat-moments/

[8] https://www.rfa.org/mandarin/yataibaodao/meiti/ql2-05212018101620.html

[9] Xinhua, "Chinese video websites delete 1.5 mln illegal clips," May 10, 2018, http://www.xinhuanet.com/english/2018-05/10/c_137170187.htm

[10] China Digital Times, "Minitrue: WeChat Group Controls for Qingdao Summit," June 5, 2018, https://chinadigitaltimes.net/2018/06/minitrue-wechat-group-controls-for-qingdao-sco-summit/

[11] Charles Rollet, "In China's Far West, Companies Cashin on Surveillance Program that Targets Muslims," *Foreign Policy*, June 13, 2018, https://foreignpolicy.com/2018/06/13/in-chinas-far-west-companies-cash-in-on-surveillance-program-that-targets-muslims/

the work entails complicity in the oppression of Xinjiang's Uighur Muslim population, it could give the companies a competitive edge on the international market, partly because access to large amounts of data can help train artificial-intelligence algorithms. For example, data and images of ethnic Chinese, Turkic Uighurs, and—under a new deal with Zimbabwe's government—sub-Saharan Africans could collectively enable developers to correct common race-related errors in facial-recognition software and gain market share in other parts of the world.[12] Chinese firms are already expected to control 44 percent of the global market for such technology by 2023.[13]

Chinese firms seek to expand in a wide range of other areas. A report published by Hong Kong–based *Abacus* in July shows how Baidu, Alibaba, and Tencent have been investing in or acquiring dozens of companies within China and abroad, from e-commerce and ride-sharing apps to blockchain developers and makers of self-driving cars.[14] These tech giants are private enterprises, and they may have their own reasons for making such investments, but they also remain beholden to the government and its strategic goals. As the report notes: "Success or failure in China's internet landscape is contingent upon government authority." Evidence of this reality has been abundant in recent months. In May, after a brief suspension by regulators, Toutiao overhauled the content and messaging of its popular personalized news app, altering its mission statement to include spreading "correct public opinion orientation."[15] Also that month, industry leaders joined in the creation of a new China Federation of Internet Societies (CFIS), directed by the Cyberspace Administration of China (CAC).[16] Individuals like Tencent chairman Pony Ma, Alibaba founder Jack Ma, and Baidu chairman Robin Li were appointed as vice presidents. One of the CFIS's inaugural commitments was to "conscientiously study and implement the spirit of Xi Jinping's Strategic Thought on Building a Cyber Superpower."

Foreign tech firms in China

Chinese tech firms are not the only ones eager to please the leadership in Beijing. Many of the world's top technology and social media companies are banned or extremely constrained in their ability to provide services to Chinese internet users. Notably, the websites of

[12] Lynsey Chutel, "China is exporting facial recognition software to Africa, expanding its vast database," *Quartz Africa*, May 25, 2018, https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/
[13] Eudora Wang, "China To Take Nearly Half Of Global Face Recognition Device Market By 2023," *China Money Network*, August 23, 2018, https://www.chinamoneynetwork.com/2018/08/23/china-to-take-nearly-half-of-global-face-recognition-device-market-by-2023
[14] Abacus News. (2018). *China Internet Report 2018 [Short Version]*. Retrieved from https://www.slideshare.net/EdithYeung/china-internet-report-2018-short-version
[15] Yimian Wu, "China's Toutiao Has A New Mission: To Shape Correct Public Opinion," *China Money Network*, May 17, 2018, https://www.chinamoneynetwork.com/2018/05/17/chinas-toutiao-has-a-new-mission-to-shape-correct-public-opinion
[16] David Bandurski, "Building the Party's Internet," *China Media Project*, May 11, 2018, http://chinamediaproject.org/2018/05/11/building-the-partys-internet/

Facebook and Twitter are blocked, while restrictions on Google have expanded from its search engine to its email client, translation services and more. Such restrictions place real costs on these companies and U.S. businesses operating in China generally. A 2016 survey by the American Chamber of Commerce found that 79 percent of U.S. companies reported that Chinese government internet restrictions hurt their business.[17]

The Chinese government is adept at using the combination of its ability to block online services from reaching potential customers and the lure of its enormous domestic market to extract concessions from foreign firms, including assistance with its censorship and surveillance system. The recent controversy surrounding Google's plans to develop a censored search engine for the Chinese market is only the latest among many examples of such cooperation. LinkedIn restricts users in China from accessing profiles or posts by people based outside the country that are deemed to contain politically sensitive information.[18] Earlier this year, Apple removed more than 600 applications from its mobile store that facilitated Chinese users' ability to access blocked websites.[19]

Foreign companies operating in China also increasingly risk accusations of complicity in politicized arrests or violations of user privacy. Last year's Cybersecurity Law stipulates that foreign companies must store Chinese users' cloud data on servers located in China. To meet this requirement, Apple announced in January that iCloud data would be transferred to servers run by Guizhou on the Cloud Big Data (GCBD), which is owned by the provincial government.[20] Apple and GCBD now both have access to iCloud data, including photos and other content. In February, the U.S.-based note-taking app company Evernote similarly announced that Chinese users' data would be transferred to Tencent Cloud by mid-2018 to comply with data localization rules in the Cybersecurity Law.[21] Airbnb alerted its hosts that starting on March 30, "Airbnb China may disclose your information to Chinese government agencies without further notice to you."[22] And one of the biggest investors in the artificial

[17] Erik Crouch, "79% of American companies say China's internet restrictions are hurting them," *Tech in Asia*, January 20, 2016, https://www.techinasia.com/china-amcham-restrictions-internet-survey
[18] Paul Mozur and Vindu Goel, "To Reach China, LinkedIn Plays by Local Rules,' *New York Times,* October 5, 2014, https://www.nytimes.com/2014/10/06/technology/to-reach-china-linkedin-plays-by-local-rules.html.
[19] Letter from Cynthia C. Hogan, Apple Vice President for Public Policy in the Americas to Senators Patrick Leahy and Ted Cruz, November 21, 2017, https://www.leahy.senate.gov/imo/media/doc/Apple%2011212017.pdf.
[20] BBC, "Apple: Chinese firm to operate China iCloud accounts," January 10, 2018, http://www.bbc.com/news/business-42631386.
[21] Freedom House, *China Media Bulletin,* No. 126, February 27, 2018, https://freedomhouse.org/china-media/china-media-bulletin-resisting-beijings-influence-new-year-gala-metoo-in-china-issue-no-126#a4.
[22] Twitter post by Bill Bishop with screenshot of AirBnb notice, March 28, 2018, https://twitter.com/niubi/status/978945772971614209.

intelligence (AI) firm SenseTime, which provides facial recognition technologies to some local police and at least one prison in China, is U.S. chipmaker Qualcomm.[23]

But in a new and disturbing development, the Chinese government has used market leverage—and in some cases arbitrary blocking and other regulatory actions—to spur censorship of information available to people outside China. In a spate of incidents over the spring and summer, hotel, airline, and automobile companies changed their presentation of content on topics like Tibet or Taiwan to fit Beijing's political positions. A piece of code in Apple's iPhone operating system that was meant to prevent Chinese users from displaying the Taiwan flag emoji recently caused phones with China location settings to crash, even if the device was being used in San Francisco.[24] Apple is now weighing the inclusion of China's Beidou navigation system on the next generation of iPhones; one can already imagine how its maps will handle Beijing's territorial claims.[25]

The costs of compliance

As Chinese and foreign companies take more steps to appease the regime, the human toll will continue to mount. The space for ordinary Chinese to obtain and share information on a wide range of both political and apolitical topics has noticeably shrunk in recent years, while the risks of punishment for even facetious comments deemed unacceptable to the authorities have risen. These shifts have affected hundreds of millions of users in China. Although not all may be aware of the full set of changes, many have been forced to alter their online habits due to increasing censorship and real-name registration requirements.

For target populations like activists, religious believers, or members of ethnic minorities, the consequences have been dire. Censorship and surveillance on sensitive topics like Taiwan, Tibet, Xinjiang, Falun Gong, and the 1989 Tiananmen massacre either whitewash or exacerbate large-scale human rights violations—including mass detentions, torture, and extrajudicial killings.

Beyond that, on a daily basis, vital information is kept from the Chinese public. Annual Freedom House analysis of leaked censorship directives has repeatedly shown that a broad range of breaking news topics are targeted for control, including critical information about public health and safety.[26] Meanwhile, Chinese people's ability to discuss the current and

[23] Reuters, "Qualcomm invests in Chinese AI facial recognition startup SenseTime," November 14, 2017, https://www.reuters.com/article/us-sensetime-fundraising-qualcomm/qualcomm-invests-in-chinese-ai-facial-recognition-startup-sensetime-idUSKBN1DF0HE.
[24] Andy Greenberg, "Apple's China-friendly Censorship Caused An IPhone-crashing Bug," *Wired*, July 10, 2018, https://www.wired.com/story/apple-china-censorship-bug-iphone-crash-emoji/
[25] Asia Times, "Apple may build China's BeiDou navigation into future iPhones," August 22, 2018, http://www.atimes.com/article/apple-may-build-chinas-beidou-navigation-into-future-iphones/
[26] Freedom House, *China Media Bulletin*, No. 125, January 27, 2018, https://freedomhouse.org/china-media/china-media-bulletin-2017-year-in-review-issue-no-125

future direction of their country has been severely constrained. This was especially evident in the run-up to the 19th Party Congress last October and constitutional changes earlier this year. As the country underwent some of the most significant political events in its recent history, deletion of social media posts and accounts spiked. The vast majority of Chinese citizens were not only shut out of the conversation, but also risked severe punishment should they even try to take part from afar.

But ironically, the complicit companies themselves are also important victims of the government's repressive measures, enduring a number direct and indirect costs as a result of state abuses.

First, the arbitrary nature of Chinese regulatory decisions can wreak havoc on the best-laid business plans and nascent successes. In July, it seemed briefly that Facebook had gained government approval to open a subsidiary and innovation hub in Zhejiang Province, no doubt after long and arduous negotiations.[27] But within hours, the registration announcement disappeared and was censored in Chinese media, apparently because the CAC vetoed the local government's decision. The same arbitrariness affects the Chinese tech sector as well. In April, several extremely popular applications providing news or enabling the sharing of humorous content to tens of millions of users were abruptly suspended or shut down for failing to "rectify" their content sufficiently.

Second, the Chinese government's ever-increasing censorship and surveillance demands reduce profit margins. Actions like moving data service centers from overseas to China and partnering with local companies—as required under the new Cybersecurity Law and implemented by companies like Apple and Evernote—are not inexpensive endeavors. Neither is rapid expansion of censorship staff, as Toutiao announced following its suspension in April; the company increased the number of editorial monitors from 6,000 to 10,000 and established a special committee to manage a politicized content overhaul.[28]

Third, while close government ties are a necessity in China, they provoke scrutiny, distrust, and skepticism abroad. More foreign governments and civil society groups now object when Chinese firms seek to build critical infrastructure or provide important technology and services. Last month, Australia blocked Huawei and ZTE from building the country's 5G network, citing security risks.[29] The Fiscal Year 19 National Defense Authorization Act signed into law on August 13 banned federal agencies from purchasing equipment made by

---

[27] Paul Mozur, "China Said to Quickly Withdraw Approval for New Facebook Venture," *New York Times*, July 25, 2018, "https://www.nytimes.com/2018/07/25/business/facebook-china.html

[28] Yimian Wu, "Toutiao CEO Issues Apology As Chinese Media Regulator Shuts Joke App Permanently," China Money Network, April 11, 2018, https://www.chinamoneynetwork.com/2018/04/11/toutiao-ceo-issues-apology-as-chinese-media-regulator-shuts-joke-app-permanently.

[29] Hong Kong Free Press, "Australia blocks China's Huawei, ZTE from 5G network citing security risks," August 23, 2018, https://www.hongkongfp.com/2018/08/23/australia-blocks-chinas-huawei-zte-5g-network-citing-security-risks/

Hikvision, Dahua, Huawei, or ZTE.[30] And on September 18, broadcasters in Ghana raised concerns about the government's talks with a Chinese company on a contract to build the country's digital television infrastructure. [31] Meanwhile, Google's reputation has taken a hit from the revelations about its Chinese search engine project,[32] with some top employees resigning in protest.[33]

Recommendations

China and the CCP's cyberspace policies and strategies are complex and multi-layered. Some aspects have clear public benefits. Some are legitimate government actions to support Chinese companies in a competitive market or restrict circulation of content deemed problematic by international standards. But at least as many aspects of the Chinese regime's actions involve unfair practices, corporate espionage, and rights violating censorship and surveillance. This reality requires an equally sophisticated and multi-layered response, not only to uphold U.S. economic competitiveness, but also internet freedom for people within China, the United States, and elsewhere around the world.

The U.S. government and international community should be ready to respond to recent events and future trends. The following are a few select recommendations to the U.S. government

I. **The United States should be proactive in developing its own capabilities and upholding international free speech and privacy standards**. This can be done by:

- **Developing a comprehensive national strategy on artificial intelligence**. This should cover a five to ten year time frame and include outlining the state of current research and applications, threats and opportunities presented by artificial intelligence, current gaps, and how to move forward.

- **Dedicating diplomatic resources to upholding internet freedom at international forums and holding China to its World Trade Organization commitments**. This should include proactively tracking and countering

[30] United States. Cong. House. *John S. McCain National Defense Authorization Act for Fiscal Year 2019*. 115th Cong. H.R. 5515. https://www.congress.gov/bill/115th-congress/house-bill/5515/text
[31] Ghana Web, "Don't hand digital migration contract to StarTimes – GIBA warns government," September 18, 2018, https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Don-t-hand-digital-migration-contract-to-StarTimes-GIBA-warns-government-685952
[32] Ryan Gallagher, "Google China Prototype Links Searches to Phone Numbers," *The Intercept, September 14, 2018,* https://theintercept.com/2018/09/14/google-china-prototype-links-searches-to-phone-numbers/
[33] Ryan Gallagher, "Senior Google Scientist Resigns Over 'Forfeiture of Our Values' in China," *The Intercept*, September 13, 2018, https://theintercept.com/2018/09/13/google-china-search-engine-employee-resigns/

Chinese, Russian and other authoritarian countries' efforts to weaken international standards and protections for human rights online.

- **Exercising caution regarding Chinese investments in the United States.** In addition to investigating potential national security risks and economic impacts, reviews would do well to take into consideration whether there is evidence or reason to believe that Chinese companies have been involved in human rights abuses in China.

II. **The United States should be proactive in challenging the authoritarian foundations of the Communist Party's cyberspace strategy.** This can be done by:

- **Promoting internet freedom within China in bilateral engagement.** U.S. officials should consistently raise the issues of internet freedom in China publicly and in private meetings with Chinese counterparts, including at the highest levels. They should urge the release of imprisoned journalists and free expression activists (see here for sample list) and highlight the harm done to Chinese citizens when reporting on topics of public concern—like health, safety, and corruption—is constrained. Additional recommendations on how to support and advance free expression in China are available on Freedom House's website as part of the resource section of our *China Media Bulletin* project. But, restrictions on the internet in China don't just hurt Chinese, citizens, they hurt U.S. businesses, as well.

- **Funding counter censorship efforts specific to China.** Studies and anecdotal evidence have shown that some of the first websites that Chinese internet users visit after "jumping" the so-called Great Firewall are internet services provided by top U.S. technology companies such as Google's search engine, Facebook, YouTube, and Twitter. Supporting Chinese internet users' ability to access these websites enhances both U.S. economic competitiveness and internet freedom. Actions to be taken might include:

    - Review how much U.S. funding to date for internet freedom has assisted users from China, including by seeking information from the BBG and State Department, and whether this appropriately matches demand.
    - Support groups that develop and disseminate tools to enable Chinese users on a large scale to access blocked websites and expand funding for applications that enhance access to uncensored information and digital security on mobile phone devices.
    - Create an emergency fund that can be activated quickly during moments of crisis or political turmoil to rapidly enhance the server

capacity of circumvention tools facing increased demand from China as periodically happens when the number of Chinese people seeking uncensored information spikes. The Senate Fiscal Year 19 State and Foreign Operations Appropriations bill contains an additional $2.5 million in internet freedom funding for this purpose, and we would urge its inclusion in final legislation that is worked out in December.

- Support efforts to monitor, preserve, and recirculate censored content within China, including news articles and social media posts that have been deleted by censors. This should also include support for developing new tools to create images more likely to evade artificial-intelligence driven censorship on applications like WeChat.

- **Support projects that raise awareness of internet controls**: Support research and outreach initiatives that inform Chinese audiences about the censorship and surveillance apparatus, imprisoned journalists and online activists, the regime's human rights record overall, and how democratic institutions function. Existing studies and surveys have shown that netizen awareness of censorship often yields a greater desire to access uncensored information, assist a jailed activist, or take steps to protect personal communications.

III. **The United States government should encourage the business community to take a principled stance vis-à-vis Chinese government internet controls**. This could be done by:

- **Pressing companies doing business in China to do no harm,** whether it be turning private citizen data over to the Chinese government or providing surveillance or law enforcement equipment used by Chinese authorities to violate user rights.

- **Reintroducing and passing the Global Online Freedom Act:** The Global Online Freedom Act, introduced in every Congress from 2006-2014, contains provisions that are relevant to today's challenges. Congress should reintroduce and pass these provisions, including directing the Secretary of State to designate internet-restricting countries; prohibiting the export to those countries of any items that could be used to carry out censorship, surveillance, or internet freedom restrictions; and requiring internet communication service companies operating in internet-restricting countries to disclose as part of their annual reporting what they are doing to protect human rights and freedom of information.

Conclusion

American and international firms are caught between a rock and a hard place. As they compete for profits and market share, they must navigate between the legal regimes and political demands emanating from Beijing on the one hand and democratic societies on the other. The Chinese Communist Party has laid out its own plans and ambitions, and it shows every sign of implementing them to the fullest. The question is whether the United States, other democracies, tech entrepreneurs, and investors will assert their own principles—including freedom of expression, free enterprise, and the rule of law—with equal determination.

At times, it can appear that internet freedom may be at odds with innovation or robust competition with China, but a race to the lowest common denominator of internet repression is precisely what Beijing would be happy to see take place. Some measures that would uphold principles of internet freedom and fair competition in the long term might seem to impose a cost on U.S. businesses in the short term, but as outlined above, currying favor with the Chinese government's repressive demands carries its own costs. Developing more resilient business models will benefit companies in the long run and garner support of many people in China as well.

As part of the *China Media Bulletin* project, Freedom House has been working with partners who run circumvention tools like GreatFire's FreeBrowser or overseas Chinese outlets who gain traffic via tools like FreeGate and Ultrasurf. These channels garner millions of impressions each month and bring tens of thousands of readers from inside China to the bulletin, many of whom stay on the page for long periods to read the content or subscribe to the newsletter directly. This is just one example of the eagerness with which a notable contingent of Chinese people are actively seeking out uncensored, credible information about their country and the media controls in place.

Earlier this year, we conducted a survey among Chinese readers of the bulletin. The impact on their own behavior of gaining a better understanding of censorship and surveillance in China was palpable. Significantly, 55 percent of Chinese respondents reported being more careful when using Chinese social media applications after reading the bulletin and over 45 percent reported making a greater effort to seek out uncensored information. In addition, 18 percent of Chinese readers reported deciding to take some action to support free expression or an individual activist.

As they learn about the reality of Chinese technology companies collaboration with the Chinese government, individuals like these are likely to seek out more secure international—and often American—alternatives, so long as those companies are not also compromising their services by conceding to Chinese government demands.

I would like to conclude with a quotation from one of those readers as a testament to the importance of international support for free expression and access to information in China.

> *I am a lower class worker in Chinese society and I don't speak English. An independent Chinese media like you, that does in-depth reports about the situation in China, gives me a better understanding of China's current situation and future development. And it also helped my personal life and work. On a macro scale, China is the largest authoritarian country in the world, the Chinese Communist Party oppresses its citizens, blocks information flows, and also threatens the existing world order. I think the flow of information and freedom of speech are very important to China's future development. Birds in cages long to fly, even if we can't fly out now, hearing the chirping of birds outside can still give us hope and faith!*

Sarah Cook

Senior Research Analyst for East Asia

Sarah Cook is a senior research analyst for East Asia at Freedom House. She directs the *China Media Bulletin*, a monthly digest in English and Chinese providing news and analysis on media freedom developments related to China. Cook is also the author of several Asian country reports for Freedom House's annual publications, as well as three special reports about China: *The Battle for China's Spirit* (2017), *The Politburo's Predicament* (2015), and *The Long Shadow of Chinese Censorship* (2013). Her comments and writings have appeared on CNN, *The Wall Street Journal*, *Foreign Policy*, and the U.S. Congressional-Executive Commission on China.
Before joining Freedom House, Ms. Cook co-edited the English translation of *A China More Just*, a memoir by prominent rights attorney Gao Zhisheng, and was twice a delegate to the United Nations Human Rights Commission meeting in Geneva for an NGO working on religious freedom in China. She received a B.A. in International Relations from Pomona College and as a Marshall Scholar, completed Master's degrees in Politics and International Law at the School of Oriental and African Studies in London.