Statement before the House Select Committee on the Chinese Communist Party

on the Great Firewall and the CCP's Export of its Techno-Authoritarian Surveillance State

Countering the Chinese Communist Party's Surveillance and Censorship

Zack Cooper
Senior Fellow

July 23, 2024

Chairman Moolenaar, Ranking Member Krishnamoorthi, and distinguished Members of the Committee, thank you for inviting me to testify about the Chinese Communist Party's Great Firewall and techno-authoritarianism.

The Communist Party's adoption of increasingly strict information controls does tremendous harm to the people of China. That alone is reason to care about the rise of techno-authoritarianism. But I want to focus my remarks on how this effects Americans directly and what we can do about it.

First, the Great Firewall is not only an obstacle for the Chinese people, but it is increasingly a roadblock for U.S.-China relations. As U.S. Ambassador to China Nicholas Burns recently warned, Chinese leaders "say they're in favor of reconnecting our two populations, but they're taking dramatic steps to make it impossible."[1] This raises the risk of crisis and conflict.

Second, techno-authoritarian tools developed by Beijing will not stay in China. They are already proliferating abroad and therefore pose a global threat in the years ahead. These tools and techniques will be adopted by autocrats from Russia to Iran to Venezuela and beyond.[2] This raises the risk of oppression and conflict abroad.

So all Americans have reason to worry about the rise of techno-authoritarianism. But we must move from words to action. The United States is home to the world's leading technology firms and innovators. I am honored to work with some of them in my role as chairman of the board of the Open Technology Fund. Now is the time for us as a nation to rise to meet this challenge.

Countering censorship and surveillance is vital to put the U.S.-China relationship on a better path and to ensure that other countries do not fall under the shadow of techno-authoritarianism. This is a critical issue that deserves greater attention and resources, so I thank the Committee for its bipartisan leadership on this topic.

Revolutionizing Censorship and Surveillance

As this Committee has highlighted, the Chinese Communist Party has developed and implemented the most sophisticated censorship and surveillance apparatus in the world. What has happened in the last few years, however, is not a simple evolution in the Party's tools and techniques. Rather, it is a whole new threat to internet freedom.

The first layer of tools, commonly known as the "Great Firewall," form the Communist Party's technical censorship apparatus. This enables the government to block thousands

of foreign websites, international media sources, and digital applications to isolate Chinese nationals from outside information. Unlike many other authoritarian regimes, the Communist Party has severely curtailed access to many virtual private networks and other anti-censorship tools.[3]

The Communist Party's censorship efforts are reinforced by its technologically-advanced surveillance apparatus. Authorities track both the online activity and physical whereabouts of Chinese citizens using a complex system of cell phone data, closed circuit television cameras with facial-recognition, and an array of other interconnected data collection and analysis tools.[4]

For example, Chinese censors can identify, intercept, and censor messages deemed sensitive while in transit, with no indication to the initial sender or recipient.[5] This system is used to identify and arrest real and would-be dissidents, and has shown a remarkable ability to anticipate perceived threats. The totality of China's digital and physical surveillance has perpetuated self-censorship, self-preservation, and communal distrust of political speech.

The final layer of the Communist Party's information control regime is the dissemination of its own messaging to provide an alternate version of history and current events.[6] For example, Chinese media continues to report that COVID originated from a U.S. lab;[7] that Russia's war in Ukraine was provoked by the United States;[8] and that protests in Hong Kong were organized by the Central Intelligence Agency.[9] These narratives include an estimates 500 million posts per year and follow classic authoritarian propaganda designed to project domestic unity while vilifying the Communist Party's opponents.[10]

The Communist Party's response to the "White Paper Protests" or "A4 Revolution" that began in opposition to China's "zero COVID" policy is illustrative. As members of this Committee know well, the Communist Party's censorship apparatus was quickly overwhelmed by the volume of content being shared about the demonstrations on Chinese social media. Protesters also used creative methods, like flipping videos on their side, using filters, or recording videos of videos, in order to trick the censors.[11]

The government's swift, punitive reaction was indicative of the extent to which information control is core to the Communist Party's governing philosophy. The government responded immediately by tracking protestors, confiscating phones and computers, detaining and arresting dozens of individuals, and wiping all related content from Chinese domestic social media within a matter of days. Today, it is as if these protests never occurred.[12]

At the same time that the Communist Party is gathering enormous amounts of data on the Chinese people, it is actively eliminating Chinese-language portions of the global internet. According to China's own internet regulator, there were over 5 million websites available to Chinese nationals in 2017. Since then, this number has fallen by more than 20 percent. Chinese language websites now account for just 1.3 percent of the global total, down from 4.3 percent in 2013.[13]

The result is that the Communist Party knows more about its people than ever before, but the Chinese people know less about the outside world, and even domestic realities. This information asymmetry is no accident. Indeed, the Communist Party spends billions (one estimate equates to $7.9-$15.6 billion in 2024 dollars) and employs tens of thousands of people to develop and refine this system of surveillance and control.[14]

Why does the Communist Party invest this much in controlling information? Because the free flow of information is a fundamental threat to the Party's control of the Chinese people. Xi Jinping often references Mao Zedong's exhortation to "seek truth from facts." But the Communist Party has become increasingly focused on reconstructing facts to hide the truth.

Impeding U.S.-China Relations

Although the primary impact of the Communist Party's censorship and surveillance regime is on the Chinese people, the effects go well beyond China's borders. Indeed, efforts to stabilize the U.S.-China relationship are now bedeviled by the Communist Party's own censorship and disinformation apparatus.

U.S. Ambassador Nicholas Burns recently called out "the very aggressive Chinese government…efforts to denigrate America, to tell a distorted story about American society, American history, American policy. It happens every day on all the networks available to the government here, and there's a high degree of anti-Americanism online."[15] He has noted that China's leaders say they want to stabilize the relationship, but they are taking actions that impede it in the information space.

The Communist Party's information controls are therefore a roadblock preventing better relations between China and the United States. Regardless of the strategy that the U.S. government pursues vis-à-vis China, the Communist Party's information controls pose a severe challenge. For those hoping for a more productive bilateral relationship, China's misinformation is an political and economic obstacle.[16] For those who envision a more moderate Chinese government emerging in the future, these controls make that less likely by hiding evidence of the Communist Party's misdeeds.

Moreover, if the Chinese economy continues to stumble as a result of the Communist Party's poor management, leadership in Beijing may choose to rely more on nationalism to bolster domestic support. If this occurs, the Communist Party might lean even more heavily into blaming the United States for China's woes. The recent stabbing attacks on American and Japanese citizens in China are a symptom of the Party's nationalist campaign.[17] Setting the record straight is important to guard against this strategy and the risks it poses, not just to the United States, but to its allies and partners as well.

In the long term, it is vital that citizens around the world—whether in the United States, China, or elsewhere—have the ability to accurately understand where each system is succeeding and failing. No government is flawless. Our system is designed around transparency and accountability. China is free, of course, to adopt a different approach, but we must acknowledge that the Communist Party's distortions of reality will pose a challenge to improved relations, in both the short- and long-term.[18]

Exporting Techno-Authoritarianism

In addition to exerting absolute control over the Chinese internet and Chinese people, the Communist Party is also attempting to extend its influence beyond China's borders. It is attempting to reshape long-held norms to reengineer the global internet. And other authoritarian countries will adopt these same tools and techniques if they appear successful in limiting dissent. The State Department has carefully detailed the "emerging community of digital authoritarians" promulgated by China's digital tools and norms.[19]

Over the last decade, the Chinese government has exported censorship and surveillance technologies to over 80 countries worldwide, with particular success amongst Belt and Road members. In Africa, Ethiopia, Uganda, and Nigeria have been adopters, along with Venezuela and Ecuador in Latin America, effectively embedding illiberalism abroad. These efforts expand the Communist Party's influence and insulate other autocratic regimes against the desires of their own people.[20] Equally concerning has been China's interference in democracies around the world using a variety of related strategies.[21]

These efforts are further reinforced by the Communist Party's determination to fundamentally reengineer the global internet and the norms on which it is based. Through multiple international technical and standard setting bodies, the Chinese government is attempting to reconfigure foundational elements of the internet to undermine its interoperability and security. This threatens to effectively redesign the very core of the global internet to enable control rather than connection.

By upending the international consensus around a free and open internet in this way, the Communist Party is enabling techno-authoritarianism globally. If the United States and its allies and partners do not act, we will wake up to a splintered internet or an internet backbone more tilted toward control and autocracy than freedom.[22]

Recommendations for the Committee's Consideration

In short, the Communist Party's information controls not only harm the Chinese people but also obstruct their ties with American counterparts and threaten to proliferate around the world. Having established the dangers associated with the Communist Party's surveillance and censorship, I want to focus on four suggestions designed to: 1) counter these dangers abroad, 2) bring them to light at home, 3) insulate American society against their effects, and 4) better predict their future evolution and spread.

First, the United States needs an ambitious moonshot to protect internet freedom. The Communist Party is putting billions into its censorship apparatus. If we do not act, then Beijing will be able to develop and deploy its surveillance and censorship tools around the world, damaging American interests for decades. Due to strong bipartisan congressional support, the Open Technology Fund is pursuing a deliberate strategy to reconceptualize both the challenge of and solutions to Communist Party censorship and surveillance. But this competition is too one sided. U.S. internet freedom efforts receive less than one percent of the resources that China likely devotes to information control. To counter this, we should support innovative research implemented by a variety of entities, including programs supported by the National Endowment for Democracy and others. We simply cannot compete on this scale without a major initiative cutting across U.S. departments, agencies, affiliated entities, and the private sector. The goal need not be to "tear down" the Great Firewall, but we must at least help vulnerable populations to circumvent it. The time to act is now, before these systems proliferate globally.

Second, we should ask American companies to do more to counter information controls. U.S. government investments depend on technology companies making independent content accessible, as well as the tools required to safely consume it in authoritarian countries. Yet, some major U.S. companies do just the opposite – for example, by restricting access to virtual private networks in China while allowing the Communist Party to replace these networks with ones that the Party can covertly monitor. Ideally this behavior would stop entirely. But the Congress should at least require that it be disclosed, given that enabling Communist Party censorship and surveillance harms not only the Chinese people, but the American people as well. Companies are required to disclose cybersecurity incidents to the U.S. government, they should have to do the same when they actively enable censorship and surveillance by autocratic regimes.

Thus, the Congress should insist that American companies at the very least disclose when they enable these activities by states that are designated as foreign adversaries.

Third, the United States should take steps to insulate itself against the spread of Chinese censorship and surveillance. While the Communist Party has long barred most American media and social media companies from operating in China, the United States has allowed tools like TikTok, which could be used for both surveillance and censorship. To protect against this fundamental asymmetry, U.S. media organizations and social media companies should be required to publicly disclose when they disseminate information or accept payments provided by entities affiliated with countries that have been designated as foreign adversaries. Today, this would include China, Cuba, Iran, North Korea, Russia, and Venezuela.[23] Few, if any, of these countries permit major U.S. media organizations to operate normally in their domestic environments, so it is only reasonable to insist on transparency, if not reciprocity, when they operate in the United States. The Congress should ensure that efforts by these governments to influence the American people via media organizations happen in broad daylight, if it happens at all.

Fourth, the Congress should support additional research on Chinese censorship and surveillance. Many non-profit institutions, such as Freedom House and Human Rights Watch, have done great work in this area, but we need a deeper understanding of the tools and techniques that the Communist Party is using if we are to understand the evolving nature of the threat it poses. Detailing the Communist Party's information control strategy is fundamental to building an effective U.S. government response. It is also critical to do this work not just in regard to China, but also other autocratically governed countries. To prevent the proliferation of these tools and techniques, U.S. government and non-government researchers need to have data on exactly how the internet landscape is changing. This research is vital to help the Congress target its funding to the places and populations that need U.S. assistance the most. Ideally, these efforts would be conducted in coordination with allies and partners who have a shared interest in protecting the open internet and the benefits it provides.

The information competition with China is not a minor aspect of the relationship, but a central pillar. Unfortunately, too few in the United States have treated it as such. The Communist Party is under no illusions about the importance of succeeding in this domain, which is why it devotes orders of magnitude more resources into this area. But the United States retains fundamental advantages in this area that just need to be employed energetically. Most fundamentally, freedom has an inherent advantage over censorship, surveillance, and control. Therefore, I thank the Committee for bringing these issues to light and I urge you to consider an ambitious agenda in this area.

[1] Jonathan Cheng, "In Rare Rebuke, U.S. Ambassador Accuses China of Undermining Diplomacy," *Wall Street Journal*, June 25, 2024, https://www.wsj.com/world/china/in-rare-rebuke-u-s-ambassador-accuses-china-of-undermining-diplomacy-f3e58d83.

[2] Maya Wang, "China's techno-authoritarianism has gone global," Human Rights Watch, November 10, 2021, https://www.hrw.org/news/2021/04/08/chinas-techno-authoritarianism-has-gone-global.

[3] Andrew Jacobs, "China further tightens grip on the internet," *New York Times*, January 29, 2015, https://www.nytimes.com/2015/01/30/world/asia/china-clamps-down-still-harder-on-internet-access.html.

[4] Isabelle Qian, Muyi Xiao, Paul Mozur, Alexander Cardia, "Four takeaways from a Times investigation into China's expanding Surveillance State," *New York Times*, June 21, 2022, https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html.

[5] Emily Feng, "China intercepts WeChat texts from U.S. and abroad, researchers say," *National Public Radio*, August 29, 2019, https://www.npr.org/2019/08/29/751116338/china-intercepts-wechat-texts-from-u-s-and-abroad-researcher-says.

[6] Sarah Cook, "The Long Shadow of Chinese censorship," Freedom House, October 22, 2013, https://freedomhouse.org/sites/default/files/2020-02/Special_Report_Long_Shadow_Chinese_Censorship_2013.pdf.

[7] Steven Lee Myers, "China spins tale that the U.S. Army started the coronavirus epidemic," *New York Times*, March 13, 2020, https://www.nytimes.com/2020/03/13/world/asia/coronavirus-china-conspiracy-theory.html.

[8] Joseph Bodnar, Bret Schafer, and Etienne Soula, "A year of disinformation: Russia and China's influence campaigns during the war in Ukraine," Alliance For Securing Democracy, May 4, 2023, https://securingdemocracy.gmfus.org/a-year-of-disinformation-russia-and-chinas-influence-campaigns-during-the-war-in-ukraine/.

[9] Steven Lee Myers, "In Hong Kong protests, China angrily connects dots back to U.S.," *New York Times*, September 5, 2019, https://www.nytimes.com/2019/09/05/world/asia/china-hong-kong-protests.html.

[10] Gary 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, 2017, https://www.cambridge.org/core/journals/american-political-science-review/article/how-the-chinese-government-fabricates-social-media-posts-for-strategic-distraction-not-engaged-argument/4662DB26E2685BAF1485F14369BD137C.

[11] Sarah Cook, "China's censors aim to contain dissent during harsh COVID-19 lockdowns," Freedom House, , S. May 19, 2022, https://freedomhouse.org/article/chinas-censors-aim-contain-dissent-during-harsh-covid-19-lockdowns-opinion-0.

[12] Nicole Hong and Zixu Wang, "China moves to erase the vestiges of 'zero covid' to deter dissent," *New York Times*, February 28, 2023, https://www.nytimes.com/2023/02/28/world/asia/china-covid-lab-leak.html.

[13] Li Yuan, "As China's internet disappears, 'we lose parts of our collective memory'," *New York Times*, June 4, 2024, https://www.nytimes.com/2024/06/04/business/china-internet-censorship.html.

[14] Ryan Fedasiuk, "Buying silence: The price of internet censorship in China," Jamestown Foundation,

January 12, 2021, https://jamestown.org/program/buying-silence-the-price-of-internet-censorship-in-china/; Sarah Cook, "The Politburo's predicament," Freedom House, January 2015, https://freedomhouse.org/report/special-report/2015/politburos-predicament.

[15] Cheng, "In Rare Rebuke."

[16] "Censorship-related measures in China cause significant annual revenue losses for certain U.S. industries, reports USITC," United States International Trade Commission, July 7, 2022, https://www.usitc.gov/press_room/news_release/2022/er0707ll1958.htm.

[17] "China takes a step to curb anti-Japanese rhetoric online," *The Economist*, July 4, 2024, https://www.economist.com/china/2024/07/04/china-takes-a-step-to-curb-anti-japanese-rhetoric-online.

[18] Yuyu Chen and David Y. Yang, "Does Bypassing Internet Censorship in China Change Individuals Beliefs, Attitudes, and Behaviors?," Stanford Center on China's Economy and Institutions, May 1, 2023, https://sccei.fsi.stanford.edu/china-briefs/does-bypassing-internet-censorship-china-change-individual-beliefs-attitudes-and.

[19] Global Engagement Center, "How the People's Republic of China Seeks to Reshape the Global Information Environment," U.S. Department of State, October 2023, https://www.state.gov/wp-content/uploads/2023/10/HOW-THE-PEOPLES-REPUBLIC-OF-CHINA-SEEKS-TO-RESHAPE-THE-GLOBAL-INFORMATION-ENVIRONMENT_508.pdf.

[20] Sheena Chestnut Greitens, "Dealing with demand for China's global surveillance exports," Brookings Institution, September 7, 2023, https://www.brookings.edu/articles/dealing-with-demand-for-chinas-global-surveillance-exports/.

[21] Matt Schrader, "Friends and Enemies: A Framework for Understanding Chinese Political Interference in Democratic Countries," Alliance for Securing Democracy, April 22, 2020, https://securingdemocracy.gmfus.org/friends-and-enemies-a-framework-for-understanding-chinese-political-interference-in-democratic-countries/.

[22] Julian Nocetti, "A splintered internet? internet fragmentation and the strategies of China, Russia, India and the European Union," French Institute of International Relations, February 27, 2024, https://www.ifri.org/en/publications/etudes-de-lifri/splintered-internet-internet-fragmentation-and-strategies-china-russia.

[23] "Determination of foreign adversaries," The Federal Register, 2024.