Digital Authoritarianism and Religious Repression in China

Testimony before the Congressional Executive Commission on China
Hearing on "Control of Religion in China through Digital Authoritarianism"

September 13, 2022

Chris Meserole
Brookings Institution

Chairman Merkley, Chairman McGovern, distinguished Members of the Commission, thank you for the opportunity to speak before you this morning on such a vital and important issue. Although there is a growing awareness of the threat posed by the Chinese Communist Party's model of digital authoritarianism, the extent to which its expansion has converged with the Xi regime's increasing restrictions on religious freedom is far less well known. I'm grateful for the chance to share my thoughts on how that convergence came to pass, the unprecedented challenges it poses for freedom of religion within China and around the globe, and how the United States should respond.

China's Surveillance State and Restrictions on Religion

Before delving into how the Xi regime's rising digital authoritarianism intersects with its growing religious repression, each trend needs to be understood separately.

After the arrival of the internet in China in the late 1980s, the Chinese Communist Party was quick to recognize both the danger digital networks posed to the Party and also their potential for surveillance and control. By 1994 the State Council of China had placed supervision of the internet under the control of the Ministry of Public Security, and by 1997 *Wired* was running a cover story on the "Great Firewall of China."[1] Over the next decade, Chinese authorities invested heavily in state censorship and surveillance technologies, including packet inspection and IP blocking, as part of the Golden Shield project.[2] At the same time, Internet firms were increasingly held liable for hosting and transmitted prohibited speech, leading the largest firms—including foreign firms operating in the country—to develop robust censorship and moderation capabilities themselves.[3] By the time Xi Jinping took power in 2012, Chinese authorities had established an online censorship and surveillance apparatus whose capabilities

---

[1] "Freedom of Expression and the Internet in China: A Human Rights Watch Backgrounder," *Human Rights Watch*, 2001; Geremie R. Barme and Sang Ye, "The Great Firewall of China," *Wired*, 1 June 1997.
[2] Elizabeth C Economy, "The Great Firewall of China: Xi Jinping's Internet Shutdown." *The Guardian*, 29 June 2018.
[3] "Race to the Bottom: Corporate Complicity in Chinese Internet Censorship." *Human Rights Watch*, 9 Aug. 2006.

were even then unprecedented in scope. Xi moved quickly to consolidate that apparatus under his control, primarily by establishing the Cyberspace Administration of China and tasking it with overseeing the country's censorship and cybersecurity policies.[4] As smartphone usage exploded over the past decade and hundreds of millions of Chinese have come online, the scale and reach of online censorship and surveillance under the Xi regime has expanded accordingly.

Yet the surveillance apparatus developed by Chinese authorities is not limited to the web alone. As prior testimony before this commission has shown, Beijing has also harnessed digital technology for off-line surveillance and monitoring too.[5] Most prominently, Chinese security services in Xinjiang and Tibet have leveraged cameras, drones, smartphones, and biometric technology to turn those regions into what are effectively open air prisons.[6] However, use of these surveillance technologies is by no means limited to Xinjiang and Tibet. Since 2005, when the Ministry of Public Safety and what is now the Ministry of Industry and Information Technology established the first "Skynet program," Chinese officials have launched and expanded a wide range of digital surveillance efforts throughout the country.[7] With prodding from Beijing, local authorities have invested heavily in the equipment, infrastructure, and training to build out Skynet as well as related surveillance efforts like Smart Cities, Sharp Eyes, and early pilots of the Social Credit System.[8] The most sophisticated of these systems—which have seen widespread use during the pandemic, thanks to China's Zero Covid policy—now also make it possible to track individuals in real time using facial recognition algorithms overlaid on drone cameras and CCTV feeds.[9] Since these systems often lack due process and public oversight, the Xi regime has effectively built out the world's most comprehensive architecture for digital repression.

Unfortunately, the Xi regime has in tandem built out a growing legal and bureaucratic architecture for religious repression. After banning religious activity outright during the Cultural Revolution, Chinese authorities had reversed course in the "Reform Era" that followed, most notably with the CCP Central Committee's issuance of Document 19 in 1982. The result was a remarkable resurgence of religious communities across China, with government estimates recognizing a nearly fourfold increase in Protestantism alone between 1997 and 2018.[10] Yet over the past decade, Beijing has once again sought to bring religion back under greater control. In part that effort has stemmed from Beijing's efforts to reign in what it views as "religious extremism" in Xinjiang and Tibet; the country's Counterterrorism-Terror Law of 2016, along with corresponding measures and regulations, granted local authorities in each region

[4] AJ Caughey and Shen Lu and "How the CAC Became Chinese Tech's Biggest Nightmare." *Protocol*, 11 Mar. 2022.
[5] Samantha Hoffman, "China's Tech-Enhanced Authoritarianism," CECC Hearing, November 17, 2021; Yaqui Wang, "Testimony of Yaqui Wang," CECC Hearing, November 17, 2021.
[6] Nithin Coca, "China's Digital Wall Around Tibet." *Coda Story*, 16 May 2019.
[7] Zhang Zihan, "Beijing's Guardian Angels?" *Global Times*. 10 Oct. 2012.
[8] Jessica Batke and Mareike Ohlberg, "Budgeting for Surveillance." *ChinaFile*, October 30, 2022.
[9] Rebecca Heilweil, "Coronavirus is the first big test for futuristic tech that can prevent pandemics." *Vox*, 27 Feb. 2020.
[10] "China's Policies and Practices on Protecting Freedom of Religious Belief," Information Office of the State Council, 3 Apr. 2018; "White Paper—Freedom of Religious Belief in China," Embassy of the People's Republic of China in the United States, Oct. 1997.

the power to detain individuals for otherwise conventional religious behavior, such as growing a long beard.[11]

However, the Xi regime's efforts to reign in religion extend well beyond its counter-terrorism policy. In 2016, Xi held a two-day conference of religion during in which he both outlined a more hardline vision for religious regulation and also called for greater Sinicization of religion, urging the CCP to "actively guide the adaptation of religions" and faith communities to "interpret religious doctrines in a way that is conducive to modern China's progress and in line with our excellent traditional culture."[12] The speech came amid a growing crackdown on Christian churches[13] and in advance of new regulations requiring all religious organizations to register with the government.[14] Soon after the regulations took effect in 2018, Xi then announced that the State Administration for Religious Affairs (SARA) would be dissolved and its oversight function shifted to a new bureau in the CCP's United Front Work Department, a move designed to bring the management of religion further under the Party's control.[15] In 2020, another set of regulations came into effect requiring religious organizations "to spread the principles and policies of the Chinese Communist Party" and to educate their adherents and leaders "to support the leadership of the Chinese Communist Party" and to follow "the path of socialism with Chinese characteristics."[16] In response to the regulations, a Chinese Catholic priest replied: "In practice, your religion no longer matters, if you are Buddhist, or Taoist, or Muslim or Christian: the only religion allowed is faith in the Chinese Communist Party."[17]

The Xi regime's effort to control religious life then converged with its growing attempts to regulate online activity in late 2021. Although Chinese officials had imposed some measures to regulate online religious activity before—most notably its decision to ban the sale of Bibles online,[18] and a handful of stipulations in the religious regulations that took effect in 2018 and 2020[19]—Xi himself brought the issue to the fore in another conference on religion at the end of last year. In addition to reiterating his earlier call for the Sinicization of religion, Xi's remarks at the conference pushed for greater regulation of digital religion and insisted that "China must

---

[11] "China detains Uighurs for growing beards or visiting foreign websites, leak reveals," *Guardian*, 17 Feb. 2020; "OHCHR Assessment of human rights concerns in the Xinjiang Uyghur Autonomous Region, People's Republic of China," *United Nations Office of the High Commissioner for Human Rights*, 31 Aug. 2022, page 8.

[12] "Xi Calls for Improved Religious Work." *Xinhua*, 24 Apr. 2016.

[13] Ian Johnson, "China Bans Online Bible Sales as It Tightens Religious Controls." *The New York Times*, 5 Apr. 2018

[14] Dominic J. Nardi, "The 2019 Regulation for Religious Groups in China," *USCIRF*, February 2020.

[15] Alex Joske, "Reorganizing the United Front Work Department: New Structures for a New Era of Diaspora and Religious Affairs Work." Jamestown, 9 May 2019. https://jamestown.org/program/reorganizing-the-united-front-work-department-new-structures-for-a-new-era-of-diaspora-and-religious-affairs-work/

[16] For background, see Eleanor Albert and Lindsay Maizland, "Religion in China," *Council on Foreign Relations*, 25 Sept. 2020; for translation, see Wang Zhicheng, "New Administrative Measures for Religious Groups," Asia News, 31 Dec. 2019.

[17] Ibid.

[18] Ian Johnson, "China Bans Online Bible Sales as It Tightens Religious Controls." *The New York Times*, 5 Apr. 2018.

[19] Article 48 of the 2020 regulations, for example, claimed that "internet religious information services" also had to comply with relevant laws and regulations concerning religious affairs.

strengthen the management of online religious affairs."[20] Chinese officials then released new regulations banning foreign organizations from publishing content online and requiring registered religious organizations to receive licenses for streaming religious services and ceremonies.[21] Shortly after the regulations came into effect in March 2022, provincial governments began training new staff to censor online religious activity and ensure compliance with the new regulations.[22]

The new regulations represent a significant new expansion of China's surveillance state. Provincial authorities will still play a leading role in regulating religion, as they have historically.[23] But with the key agencies responsible for China's surveillance apparatus also jointly issuing the new regulations—namely, the Ministry of Public Security, the Cyberspace Administration of China, the Ministry of Industry and Information Technology, and the Ministry for National Security—the oversight of religious activity now formally extends far beyond local administrators. If the impact of the new regulations can put be in Orwellian terms, what they mean is that "Big Brother" now has clear authority to extend its watchful eye over people of faith.

Local and Global Implications for Religious Freedom

As I've noted in previous testimony, digital technology has provided extraordinary new capabilities for religious repression.[24] From the Spanish Inquisition to Stalinist Russia, modern nation-states have long sought to persecute religious activity, often to devastating effect. Indeed, this happened within China itself during the Cultural Revolution. Yet in pre-digital eras states were largely only able to regulate *public* religion; religiosity has always been a mix of public and private beliefs, behaviors, and institutions, and in practice state regulation has generally been limited to the former. Regulating the offline exercise of private religion is simply too difficult and costly for a state to carry out at scale—which is partly why, for example, religious communities in Maoist China were able to endure and flourish anew once religious restrictions were lifted.

However, the digital surveillance that China has pioneered allows for restrictions on even the private exercise of religion. GPS sensors in smartphones and cars, plus facial recognition that

---

[20] Amber Wang, "China's latest crackdown on religion bans foreigners from spreading church and spiritual content online." *South China Morning Post,* 22 Dec. 2021.

[21] Tsukasa Hadano, "China Bans Online Religious Activity Ahead of Party Congress." *Nikkei Asia*, 6 Jan. 2022.

[22] John Zhang, "127 Persons Pass Internet Religious Information Service License Examination in Guangdong." China Christian Daily, 28 June 2022. http://chinachristiandaily.com/news/category/2022-06-28/127-persons-pass-internet-religious-information-service-license-examination-in-guangdong_11614

[23] Article 5 of the new regulations: "The religious affairs departments of people's governments at the provincial level and above, together with the network information departments, competent departments for telecommunications, public security organs, state security organs, and so forth, shall establish coordination mechanisms for the administration of Internet Religious Information Services." See here.

[24] Chris Meserole, "Technological Surveillance of Religion in China." USCIRF hearing, July 22, 2020.

can track citizens across a city, make it difficult for private and covert religious communities to form and operate undetected. Likewise, client- and server-side scanning have made it possible to detect private religious activity like downloading a picture of a religious leader or reading a sacred text, and smart televisions and cellphones make it possible to remotely watch and hear private prayers within a home. Most importantly, however, the knowledge that state authorities are able to monitor even private religious activity can create a chilling effect that ultimately seeks to deter individuals from engaging in private religious expression at all. By eroding faith that the private exercise of religion is possible, digital surveillance works to erode faith altogether.

Although China is still far from fully eradicating unlicensed religious activity, examples of their efforts still abound. The recent plight of Uighur Muslims in Western Xinjiang is most well known, with local authorities compiling massive DNA and facial recognition databases that can be used to track individual members of mosques and Islamic networks, as well as smartphone surveillance capable of blocking access to the Quran and censoring posts about Islam. Yet the state is not just interfering with the religious freedom of Turkic Muslims; Hui Muslims have also been jailed merely for creating WeChat groups to discuss the Quran.[25] Nor is the discrimination limited to Western China. Local authorities and security services across the rest of the China have implemented facial recognition technology—provided by firms like Huawei, Magvii, and Tiandy—to indiscriminately identify individuals who may be Muslim.[26]

Unfortunately, many of those technologies are readily applied to Buddhist and Christian communities too. In Tibet, merely storing an image of the Dalai Lama on a smartphone can warrant detention. And evading the authorities online and offline is increasingly difficult.[27] VPNs have been criminalized in the region, while an elaborate "digital wall" of cameras, drones, and remote sensing technologies has cut down the number of Tibetans successfully fleeing to Nepal by 97%.[28] Unregistered Christian Churches, which are viewed as a potential vector for foreign influence, have also been the subject of intense surveillance and censorship too. Pastors have been told to remove themselves from WeChat groups, while other clergy suspected of having ties to foreign churches have had their social media accounts and digital content banned.[29] Other underground or unregistered churches have been shut down entirely for refusing to comply with digital surveillance.[30]

---

[25] "China Jails Man for Teaching Islam Online," *CBS News*, 12 Sept. 2017.

[26] Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority." *The New York Times*, 14 Apr. 2019; Drew Harwell and Eva Dou, "Huawei Tested AI Software That Could Recognize Uighur Minorities and Alert Police, Report Says." *Washington Post*, 9 Sept. 2022; Tate Ryan-Mosley, "This Huge Chinese Company Is Selling Video Surveillance Systems to Iran." *MIT Technology Review*, December 15, 2021; Edward Wong and Ana Swanson, "U.S. Aims to Expand Export Bans on China Over Security and Human Rights." *The New York Times*, 5 July 2022.

[27] "Wave of Arrests Across Eastern Tibet After Digital Search Operations." *Free Tibet*, 22 July 2021.

[28] Nithin Coca, "China's Digital Wall Around Tibet." *Coda Story*, 16 May 2019.

[29] "Five members of the Sion Church in Taiyuan travelled abroad to attend an evangelical conference, and were arrested for 'the crime of stealing across the border'." *ChinaAid*, 27 July 2021.

[30] "China Outlaws Large Underground Protestant Church in Beijing." *Reuters*, 10 Sept. 2018.

The combination of the new religious regulations, along with China's ongoing "Zero Covid" policy, stand to exacerbate these trends. With Covid restrictions requiring the frequent closure of houses of worship (or serving as a pretext for their closure), online channels have offered a way for some religious organizations to remain in community. The new regulations thus threaten to remove a key option for exercising religion at a time when it is needed most.

Potential for Religion Repression Abroad

Although the Xi regime's combination of digital authoritarianism and religious repression most directly impacts religious organizations within China, it also poses an urgent challenge to faith communities abroad. There are three particular dangers in that regard.

First, China's efforts to digitally surveil and censor religious minorities extends well beyond its borders. As an illustration of how seriously Chinese authorities take the issue, in 2019 they expended a sophisticated "zero day" exploit for iOS devices on the Uighur diaspora. Chinese hackers had developed a way to gain root access to iPhone just by having the browser open a website, yet state authorities opted to exploit the vulnerability to monitor a small Uighur community abroad rather than a foreign political leader or high-value target.[31] In addition, the Chinese have also sought to leverage WeChat to monitor ties between Christian communities abroad and those in mainland China—to the point where domestic Chinese clergy have asked their members not to use WeChat with Christians in the United States.[32]

Second, China is increasingly exporting its surveillance technology to others. As part of its "Digital Silk Road," the Xi regime has sought to couple its Belt and Road development initiative with a concurrent push to boost foreign sales of Chinese telecommunications equipment and technology, including surveillance technology.[33] As a result, China has now successfully sold the surveillance technology it has pioneered to over 80 states globally,[34] many of whom also have extensive legal and bureaucratic structures for religious repression. For example, consider Iran. After widespread protests throughout the country in 2009, Tehran purchased a surveillance system from ZTE for Iran's telecommunications monopoly, enabling the regime to monitor landline and mobile communications and carry out deep packet inspection across nearly all internet traffic.[35] More recently, Tehran has entered into a 25-year trade agreement with China in which Iran will receive greater Chinese investment and technology, while earlier this year Iran's parliament pushed forward a new Internet "Protection Bill" that would place the country's internet infrastructure under control of its armed forces and security services and was

[31] Cooper Quintin and Mona Wang, "Watering Holes and Million Dollar Dissidents: The Changing Economics of Digital Surveillance." *Electronic Frontier Foundation*, 9 Sept. 2019.

[32] Wan Zixin, "China's Social Media Platforms—Tools of Religious Persecution." *Bitter Winter*, 19 May 2020.

[33] Jonathan E. Hillman, *The Digital Silk Road: China's Quest to Wire the World and Win the Future*. Washington, DC: CSIS, 2021.

[34] Dahlia Peterson, "How China Harnesses Data Fusion to Make Sense of Surveillance Data." *Brookings Techstream*, 23 Sept. 2021.

[35] "Special Report: Chinese Firm Helps Iran Spy on Citizens." *Reuters*, 22 Mar. 2012.

explicitly modeled in part on Beijing's approach to internet technology.[36] As one lawmaker put it, in reference to internet restrictions and surveillance, "the Chinese have unique and innovative experience in this field, which we can put to use."[37] Iran's security services have already made progress in that effort, with the purchase of video surveillance systems from the Chinese firm Tiandy—a company notorious for its supply of "smart interrogation desks" and facial recognition systems designed to target ethnic and religious minorities.[38] Left unchecked, the Iranian regime appears intent on replicating China's surveillance system within its borders using Chinese-made technology. Given Tehran's track record, this poses serious risks to religious freedom in the country.

Third, the Xi regime's use of digital surveillance for religiously-motivated repression has normalized the practice globally. Consider Saudi Arabia. As with China, the Saudi government has leveraged zero-day exploits to surveil and target dissident communities abroad.[39] It has also carried out mass surveillance of internet communications and social within the country, with one key advisor—who was also involved with the killing of Jamal Khashoggi—publicly crowdsourcing a list of dissidents to target using a Twitter hashtag.[40] Even though the Saudi regime has used Israeli rather than Chinese surveillance tech, and leveraged American rather than Saudi digital platforms, China's surveillance apparatus have helped to normalize its repression. Not surprisingly, Saudi officials have publicly acknowledged studying Beijing's technology development and deployment, claiming that "there is a lot to learn from China."[41]

How the United States Should Respond

As the international community has awoken to the threats posed by China's model of digital authoritarianism, the United States and its allies and partners have started to respond forcefully. The U.S. Entity List is now far more comprehensive, export controls have been expanded, and new sanctions have been put in place on officials and firms responsible for the worst human rights abuses within China.[42] Although the full effect of these and related efforts will take time to play out, the era in which Chinese firms were able to easily and openly develop and export repressive censorship and surveillance technology is drawing to a close—and rightfully so.

---

[36] "Iran: Human Rights Groups Sound Alarm Against Draconian Internet Bill." *Human Rights Watch*, 17 Mar. 2022.
[37] "Iran Plans to Work With China On Technology To Further Restrict Internet." *Iran International*, 3 Feb. 2022.
[38] Tate Ryan-Mosley, "This Huge Chinese Company Is Selling Video Surveillance Systems to Iran." *MIT Technology Review*, December 15, 2021.
[39] Bill Marczak, et al., "The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil." *Citizen Lab Research Report* No. 115, University of Toronto, 1 Oct. 2018.
[40] Katie Benner, et al., "Saudis' Image Makers: A Troll Army and a Twitter Insider." *The New York Times*, 20 Oct. 2018.
[41] Andrew England and Simeon Kerr, "'More of China, Less of America': How Superpower Fight Is Squeezing the Gulf." *Financial Times*, 20 Sept. 2021.
[42] Edward Wong and Ana Swanson, "U.S. Aims to Expand Export Bans on China Over Security and Human Rights." *The New York Times*, 5 July 2022.

However, where the application of China's surveillance and censorship technology to religious freedom specifically is concerned, there is still far more that can be done. In particular:

- **Establish a temporary, independent commission on digital authoritarianism**. Addressing the challenge that digital authoritarianism poses to freedom of religion will not be possible without a consensus understanding of the threat it poses to the United States and democratic societies more broadly. A new bipartisan commission could carry out a full review of the challenge posed by digital authoritarianism, especially to religious freedom, and offer a consensus set of recommendations for how the United States should respond.

- **Re-organize for the long-term**. With digital surveillance and high-tech competition set to be a defining challenge in the years and decades to come, the U.S. government has taken early steps to adapt its bureaucracy for the long-term nature of that challenge. Now that new bodies like the Bureau for Cyberspace and Digital Policy in the State Department have gotten off the ground, there should be an inter-agency review of how the offices set up to address digital policy and security liaise with and inform offices dedicated to religious freedom globally, and vice versa. This may result in more staff in the CDP or EAP bureaus having online religious freedom as part of their portfolio, and/or more staff in USCIRF and elsewhere with tech and digital policy as part of theirs. Regardless of the outcome, however, the Biden administration should mandate a review of how best to organize effectively against digital authoritarianism and religious repression.

- **Create an open-source monitoring function**. Crafting effective policy is difficult without reliable information and analysis, yet right now there is no consistent source of digital surveillance and censorship, much less its impact on religious repression, across the U.S. government. In light with the recommendation above, there should be an office dedicated to regularly providing the public with open-source information about how political regimes are deploying surveillance and censorship technology and what impact it is having on human rights, including the freedom of religion. By reliably producing this information, the United States will also be better positioned to build momentum for global efforts to counter digital authoritarianism in China, Iran, and elsewhere.

- **Link religious freedom with freedom of expression online**. In response to the growing calls for national internets like China's Great Firewall or Iran's "Halal web," the Biden administration rightly reiterated the need for an open and free internet earlier this year with its "Declaration for the Future of the Internet."[43] Yet religion was referenced only once in passing in the declaration, and is often downplayed in broader policy discussions around freedom of expression online—despite the role that religious repression often plays in motivating mass digital surveillance. As the United States advocates for greater

---

[43] "A Declaration for the Future of the Internet." White House, May 2022.

internet freedom around the world, its messaging should emphasize that freedom of speech and freedom of religion go hand-in-hand.

- **Leverage privacy-enhancing technologies**. As the scale of government and commercial surveillance has grown, privacy-enhancing technologies hold enormous promise for advancing and protecting democratic values and norms—yet they are often absent from discussions about how to push back on the high-tech surveillance of religion in China and elsewhere.[44] The U.S. should not only continue to invest more in privacy-enhancing technology, but they should also invest in efforts to educate religious minorities about how to use them. Virtual private networks (VPNs) are particularly valuable here, especially in states—like Saudi Arabia—that seek to emulate China's surveillance system but do not yet have the technical competence to do so effectively.[45] With many religious activities shifting online, the need for end-to-end encrypted group videoconference and streaming will be increasingly vital. Although early options like Jitsi and Signal exist, privacy-preserving group video platforms will require far more investment to become easily accessible and usable by religious communities.

---

[44] Andrew Imbrie, et al., "Privacy Is Power." *Foreign Affairs*, 16 Feb. 2022.
[45] "A Seven-Nation Survey." Northwestern University in Qatar, 2018.