Testimony Before the House Select Committee on Strategic Competition Between the United States and the Chinese Communist Party

Full Committee Hearing: "The Great Firewall and the CCP's Export of its Techno-Authoritarian Surveillance State."

XIAO Qiang,

Founder and Editor-in-Chief, China Digital Times

Research Scientist, School of Information, University of California at Berkeley

(Tuesday July 23, 2024)

Honorable Chairman Moolenaar and respectable members of the Committee,

My name is XIAO Qiang. I am the Founder and Editor-in-Chief of China Digital Times. I am also a research scientist at the School of Information of University of California at Berkeley.

The Rise of Chinese Digital Authoritarianism

A 2019 report by the Brookings Institution defines digital authoritarianism as “the use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations.” Since Xi Jinping became the Chinese Communist Party (CCP) ’s top leader in 2012, he has concentrated power by purging political opponents, promoting CCP ideology, and strengthening the Party’s control over society. The Cyberspace Administration of China (CAC) is the central agency for internet regulation, censorship, oversight, and control. The CAC reports to the Central Cyberspace Affairs Commission, led by Xi himself. It has various branches, including the Internet Commentary Work Bureau, the Mobile Network Management Bureau, the Cyber Security Coordination Bureau, and the Internet Public Opinion Center. Since 2018, the CAC directly manages the National Computer Network and Information Security Management Center, which oversees the Great Firewall (GFW). Previously, this responsibility belonged to the Ministry of Industry and Information Technology.

Since the early 1990s, China’s Ministry of Public Security (MPS) has operated the “Golden Shield Project,” a security system that includes a national citizen database and criminal information system. The MPS also established the Public Information Network Security

Supervision Bureau to monitor, intercept, and censor online activities. In 2001, the Chinese government began building the Great Firewall (GFW), a system to monitor and filter internet communications at national gateways. The GFW blocks internet transmissions, foreign internet tools, and mobile apps, forcing foreign companies to comply with domestic regulations.

The CCP has always sought to legitimize its regime by shaping public discourse, mobilizing support, and suppressing dissent. It subverts social media for its purposes, using algorithms, automation, and human curation to spread misinformation and enhance its propaganda. In 2015, an anonymous user leaked various email correspondences between propaganda officials onto social media, shedding light on the secretive work of the Fifty Cent Party. These archives include photos, directories of internet commentators, and summaries of individuals' online activities dating back to 2002. The leaked documents reveal that the Chinese government has mobilized over 10 million college students through its Communist Youth League to undertake various "online public opinion struggle" tasks.

Various organizations, including internet service providers, data analytics companies, and social media platforms, also contribute to this digital control. Mainstream apps like Sina Weibo, Toutiao, and Kuaishou employ thousands of censors to remove "illegal" content, often outsourcing to companies like Beyondsoft, which employs over 8,000 workers. In 2019, Citizen Lab revealed that WeChat can filter images to detect sensitive content.

Chinese social media reveals patterns in what is expressed and what is suppressed. Censors do not delete everything but focus on maintaining the legitimacy of the Chinese Communist Party (CCP). Questions about the CCP's rule, representation, decision-making, and public participation are sensitive topics. If the Great Firewall were dismantled, Tiananmen Square footage and criticism of Xi Jinping's indefinite rule would likely flood the internet. The entire censorship and propaganda mechanism in China, controlling both traditional and social media, relies on the Great Firewall for "regime security." Without it, suppressed content could become accessible to the Chinese public, threatening the CCP's control.

Great Firewall

The Great Firewall (GFW), officially known as the "State Data Cross-Border Security Gateway," comprises a collection of institutions and technologies (both hardware and software) employed by the Chinese government to monitor and filter content at international gateways. It serves as the primary national censorship apparatus of the People's Republic of China (PRC) and is directly overseen by the Cyberspace Administration of China (CAC).

The GFW restricts Chinese internet users' access to foreign information sources and services, such as Google Search, Facebook, Twitter, Netflix, Instagram, BBC, and Wikipedia. It actively blocks tools that attempt to circumvent its censorship. My research tracks 1,382 websites blocked in China, including YouTube, Google, Facebook, Twitter, and Instagram. Since early 2017, China has intensified its campaign against unauthorized Internet connections, including virtual private network (VPN) services that enable users to bypass the Great Firewall. Starting in March 2018, all VPN services not licensed by the government are subject to be blocked.

The GFW is deployed at various international internet gateways across mainland China, utilizing supercomputers, ordinary servers, routers, and related applications. The main blocking techniques include TCP connection resets, IP blocking, DNS poisoning, specific port blocking, SSL connection interruptions, Man-In-The-Middle (MITM) attacks, and traffic pattern recognition. Because the GFW operates through the backbone network's international gateways, it also causes frequent congestion at China's international gateway nodes. Essentially, the GFW acts as a national-level system that manipulates root nodes and conducts surveillance and filtering for internet users within China.

Chinese internet users employ various technologies to circumvent the GFW, including VPNs and Shadowsocks. However, as users evolve their circumvention techniques, the GFW enhances its blocking capabilities through methods like active probing and specialized responses to encrypted traffic. The CCP is also pushing to criminalize such circumvention efforts. Under Article 285 of the Criminal Law, "Crimes of Intruding into Computer Information Systems," these activities are increasingly persecuted. In November 2021, the CAC renamed the GFW as the "Data Cross-Border Security Gateway" in the "Regulations on Network Data Security Management (Draft for Comment)." This regulation includes a mandate against providing tools for bypassing censorship, with specific punishments for violations.

A remarkable case is Ruan Xiaohuan (阮晓寰). Born 10 June 1977, Ruan is a Chinese dissident, blogger, and InfoSec specialist who, in 2009, began an anonymous blog called ProgramThink (编程随想). The blog provided cybersecurity advice, methods to bypass China's internet censorship, political commentary critical of the Chinese Communist Party, and book recommendations. For twelve years, Ruan successfully avoided detection while challenging China's authoritarian regime. However, in May 2021, Ruan was arrested by Shanghai police. On 10 February 2023, he was convicted of "inciting subversion of state power" by the Shanghai No. 2 Intermediate People's Court and sentenced to seven years in prison.

Growing Surveillance State

Another component of digital authoritarianism under Xi Jinping is an intensification of the mass retrieval, collection, and processing of individual information through online activities. The CCP uses digital technology, especially artificial intelligence, to establish a mass surveillance system in the country in the name of building a "safe society", "smart cities", and "smart policing".

Government agencies use facial recognition, biometrics, surveillance cameras, and big data analytics to quickly profile and classify individuals, track activity, predict activity, and take preemptive action against any perceived threats to state power. For example, in China's north-west region Xinjiang, apart from the ubiquitous cameras, most residents are required to download apps on their phones that allow the authorities to monitor what they look at and track their movements. In 2019, data leaks revealed that Chinese authorities were closely tracking the locations of almost 2.6m people in real time through a facial-recognition company and police contractor called SenseNets.

The "Skynet Project," established by the Chinese government in 2003, installs video surveillance equipment in public places like traffic junctions, railway stations, and shopping malls. Using GIS maps and image collection technologies, Skynet connects cameras across various locations and can identify large numbers of people quickly. Companies like Hikvision, SenseTime, Huawei, and ZTE are involved, with 200 million plus surveillance probes across China. In 2015, the National Development and Reform Commission and other agencies launched the "Sharp Eyes Project" to provide rural surveillance. High-definition cameras were installed at main road entrances and public gathering spots, with surveillance information accessible via rural TV networks, aiming for comprehensive and controllable coverage. Sharp Eyes also places surveillance capabilities in citizens' hands and encourages their direct participation. It aims to achieve "full range coverage, full network sharing, available at all times and fully controllable" from the perspective of police.

In 2017, China aimed to become a "major AI innovation center" by 2030, selecting Baidu, Tencent, Alibaba, and iFLYTEK as national champions in AI. The Chinese state works with tech companies to strengthen the large-scale retrieval, collection and processing of personal information through online activities ranging from social media behaviors to buying habits. With no other choice, more than one billion Chinese use a handful of phone applications. Although these phone applications are extremely convenient, users' communications, transactions, and behavior are disclosed to large technology companies such as Ant Group and Tencent that are obliged to share this data with the Chinese government.

PRC's technology companies are among the world's largest and most innovative and can exert increasing levels of influence over industries and governments around the world. PRC's tech giants, whatever their ownership structure, are domestic monopolies that are tightly integrated with the CCP. Over 70% of private enterprises in China have party organizations and branches. These companies also often pursue commercial interests that align with PRC diplomatic goals.

Internationally, PRC has promoted the concept of "cyber sovereignty" to legitimize censorship, surveillance and localized control of data. CAC has continuously expanded the list of banned websites using strict cybersecurity laws. Companies must abide by stringent censorship regulations and need to conduct self-censorship to avoid government penalties. At the same time, all companies operating in PRC, including foreign companies, are required to store information, including personal data, in data centers or servers in PRC.

Pandemic

For the CCP, advanced censorship and surveillance technology reduces the cost of social coercion and precisely targets resistance. The COVID-19 pandemic has been a boon for digital authoritarianism.

The pandemic, which originated in China, spread widely partly due to the CCP's internet control. Dr. Li Wenliang, the Wuhan whistleblower, was admonished for "spreading rumors" before his death, triggering grief and anger among the Chinese people and brief calls for free speech.

Despite this, the CCP's surveillance strategy proved effective during the pandemic. The government used tracking apps, drones, and cameras for surveillance, with upgraded facial recognition identifying masked individuals. The "Health Code" app, beneficial for public health, posed privacy threats by controlling access to public spaces based on health ratings. The epidemic has thus become a long-term enabler of the CCP's digital authoritarianism.

Meanwhile, daily VPN users in China increased from about 2 million at the pandemic's start to nearly 10 million. More Chinese joined Twitter using VPNs, primarily communicating via direct messages. Although Twitter does not disclose user numbers in PRC, some researchers estimate a 10% increase in early 2020 as people sought COVID-19 news and during protests. Authorities are alarmed by the "backflow" of information from abroad.

On November 28, 2022, the CAC declared a "Level 1 Internet Emergency Response," requiring the highest level of content management. It ordered e-commerce sites to curb sales of circumvention tools, including VPNs and foreign Apple accounts, and instructed tech firms to scrub user-generated advice on bypassing the Great Firewall.

Digital Silk Road

The PRC government is aggressively promoting its "Digital Silk Road," encompassing fiber optic cables, mobile networks, satellite relay stations, data centers, and smart cities built by global Chinese tech companies. This initiative has amassed over $17 billion in loans and investments, funding global telecom networks, e-commerce, mobile payment systems, and big data projects. PRC has targeted North Africa and the Middle East, signing Digital Silk Road agreements with Egypt, Saudi Arabia, Turkey, and the UAE.

ZTE operates in over 50 of 64 countries involved in the "One Belt, One Road" initiative, providing fiber optic cables, mobile networks, surveillance, mapping, cloud storage, and data analysis services in cities across Ethiopia, Nigeria, Laos, Sri Lanka, Sudan, and Turkey. Huawei Cloud Services manages crucial infrastructure, such as oil production and fuel distribution in Brazil and power plant operations in Saudi Arabia. This allows Chinese companies to collect, control, and store data from other countries, enhancing their data analysis capabilities for artificial intelligence and improving control models.

PRC's expertise in digital tools for inspection and surveillance has made it the preferred supplier for authoritarian governments. The 2020 "Internet Freedom Report" by Freedom House noted that Chinese officials have trained representatives from 36 countries in new media and information management. Chinese companies are developing telecom infrastructure in 38 countries, and surveillance firms like Hikvision and CloudWalk are selling facial recognition technology to 18 countries, including Egypt and Qatar.

The CCP aims for these companies to exert political influence across the region. In the short term, the presence of Chinese engineers, managers, and diplomats reinforces the tendency of developing countries, especially authoritarian regimes, to adopt the PRC's closed Internet model.

Exportation of Surveillance and GFW Technology

China has become a leading exporter of surveillance technology, including closed-circuit television (CCTV) systems, facial recognition technology, and data analytics software. These technologies are being used by governments around the world to monitor their citizens, including countries with a history of human rights abuses. Chinese companies exported surveillance technology to at least 63 countries. Chinese security monitoring equipment companies Hikvision, Dahua, and Meiya Pico, all of which have close ties to the PRC government, have expanded their databases and improved their systems due to overseas development.

The PRC has formed alliances with other authoritarian regimes around the world, including Russia, Iran, and North Korea, to advance its digital repression efforts. For example, China and Russia have signed agreements to cooperate on the development of their respective digital monitoring and censorship systems and to share information on online censorship and surveillance. The PRC regularly conducts large-scale training programs for foreign officials to respond to public opinion, control civil society, and enforce the CCP-style internet surveillance policies.

Venezuela's "homeland" system, developed using ZTE technology, integrates national ID numbers with information such as car registration, voter rolls, and social media handles. This system allows ruling-party coordinators to leverage detailed citizen profiles for election mobilization and condition access to welfare services and medical treatments on compliance.

On November 30, 2020, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) designated the China National Electronics Import and Export Corporation (CEIEC) for providing the Venezuelan government with a commercialized version of China's "Great Firewall." CEIEC's involvement is significant, as since 2016, its Chief Scientist has been Fang Binxing, the creator of China's "Great Firewall."

Following the February 2021 coup, the Myanmar military junta has enhanced its internet censorship and surveillance with Chinese support. The junta has blocked social media, news, and civil society websites, and implemented electronic surveillance to monitor communications and track users.

In May 2024, the junta deployed a new system capable of intercepting and decrypting web traffic, blocking applications and websites, including VPNs, and monitoring network applications. The system employs Tiangou Secure Gateway (TSG) and Cyber Narrator from Geedge Networks, a Chinese company. TSG performs DPI on network traffic, classifies content, and provides security services. It can decrypt SSL and TLS encrypted traffic by bypassing security certificates, capturing metadata when decryption is not possible, and mirroring decrypted traffic for analysis. TSG also includes an application firewall to control over 1,000 applications. CEIEC has also been involved in a proposed location tracking system for the junta's communications ministry. Justice for Myanmar linked Geedge Networks and state-owned CEIEC to Fang Binxing, Chief-Scientist of both companies.

The Great Digital Contest

While democracies view information as an empowering force in the hands of the people, with the free and open flow of ideas, news, and opinions fueling deliberative democracy, authoritarian systems see this model as a threat. They view information as a danger to their regimes, something the state must control and shape.

Now, as the world enters the era of artificial intelligence, this technology presents both opportunities and risks. AI can be a force for good as a predictive, analytical, or automated decision-making tool. However, it can also be used for surveillance, censorship, and information manipulation. As a technology that relies heavily on the centralization of massive data, AI tends to empower centralized autocratic governments rather than decentralized democratic governance.

The PRC is already the richest, most powerful, and most technologically advanced dictatorship. By using these technologies, the CCP consolidates its power at home while weakening democratic competitors abroad. The CCP has provided the world with a blueprint for establishing a digital totalitarian state and presenting a threat to global peace. All democratic states and civil society actors must work in solidarity to counter the global expansion of Chinese digital authoritarianism to defend and preserve freedom and dignity at home and globally. This is one of the greatest challenges we must meet in the 21st century.

Policy Recommendations for Congress

Thank you to the House Select Committee for holding this timely and critical hearing on the Great Firewall and the Chinese Communist Party's export of its techno-authoritarian surveillance state. I recommend the following policies:

1. Enhance counter-digital authoritarianism efforts: Increase funding for agencies, non-profit organizations, and research institutions combating digital authoritarianism. This includes supporting R&D of new circumvention technologies and decentralized AI tools through increased access to resources, research, and collaboration opportunities.
2. Support media initiatives that can provide PRC citizens with access to a diverse range of fact-based information by ensuring adequate funding for federal media programs and activities.
3. Expand export control sanctions: Extend export control sanctions on PRC companies involved in exporting digital authoritarianism technology.
4. Prohibit investments in digital authoritarianism companies: Prohibit all U.S. investors, including institutional and retail investors, from purchasing or investing in the securities of companies identified by the U.S. government as being involved in digital authoritarianism.
5. Blacklist educational and research institutions: Add PRC educational and research institutions, commercial entities, and administrative bodies involved in the research and application of digital authoritarian technologies, such as the Great Firewall, to the U.S. Entity List under the Export Administration Regulations.
6. Enact digital authoritarianism sanctions: Implement sanctions on individuals who play a significant role in the research and application of digital authoritarian technologies, such as those responsible for the Great Firewall, including scientists and technical experts like Fang Binxing.

Thank you Mr. Chairman.