FRIEDRICH NAUMANN FOUNDATION For Freedom.

Stanford | Global Digital Policy Incubator
Cyber Policy Center

THE EVERYTHING EVERYWHERE CENSORSHIP OF CHINA

China is exporting its model of Internet governance based on digital repression. The free world must protect our values and take back our Internet.

Charles Mok

ANALYSIS

Imprint

Publisher

Global Innovation Hub
Friedrich Naumann Foundation for Freedom
15F.-6, No. 171, Songde Road,
Xinyi District, Taipei City 110030
Taiwan

/freiheit.org/taiwan
/FNFGIHUB
/FNFGIHUB
/FNFGIHUB

Author

Charles Mok

Editor

Global Innovation Hub of the Friedrich Naumann Foundation for Freedom

Contact

E-Mail: globalinnovation@freiheit.org

As of

June 2023

Notes on using this publication

This publication is an information offer of the Friedrich Naumann Foundation for Freedom.
It is available free of charge and not intended for sale.
It may not be used by parties or election workers for the purpose of election advertising during election campaigns (federal, state or local government elections, or European Parliament elections).

Disclaimer

The perspectives and opinions stated in this publication are those of the authors, and they do not necessarily reflect the view of Friedrich Naumann Foundation for Freedom.

Table of Contents

Glossary

Terminology	Explanation
ARPANET	"Advanced Research Projects Agency Network," the first wide-area packet-switched network that implemented the TCP/IP (the Internet Protocol Suite) that became the first foundation of the Internet
Augmented reality (AR)	An interactive experience that combines the real world and computer-generated content, enabling real-time interaction between virtual and real objects
Blockchain	A form of DLT that consists of blocks of records that are continually generated and securely linked using cryptographic technologies
Business-to-business (B2B)	A business or electronic transaction between one business and another
Business-to-consumer (B2C)	A business or electronic transaction between a business and a consumer
Cloud computing	Computer system storage and computing resources made available to users on demand but not directly owned or managed by the users
Constitutionalism	A compound of ideas, attitudes, and patterns of behavior elaborating the principle that the authority of government derives from and is limited by a body of fundamental law
Consumer-to-consumer (C2C)	A business or electronic transaction between one consumer or private individual with another
Deep packet inspection (DPI)	A data processing technique that inspects in detail the data being sent over a computer network and that can be used with positive uses, like ensuing data integrity or checking for malicious code, as well as for repressive uses, like eavesdropping and censorship

Terminology	Explanation
Distributed ledger technology (DLT)	Technology based on consensus-based digital data that is replicated, shared, synchronized, and distributed across many servers or sites and that forms the basis for the blockchain
Domain name service (DNS)	The hierarchical and distributed naming systems for computer and server resources on the Internet that are generated by associating and translating the numerical IP addresses to language-based domain names
Douyin (抖音)	A short-form video-based social media platform in China, similar to TikTok, which is used by people outside China, with both owned by Chinese company ByteDance (字节跳动)
Electronic data interchange (EDI)	The concept of electronic communication of information for transactional purposes based on certain commonly agreed-upon standards
Free Trade Zone (FTZ)	An area within a country in which goods can be landed, processed, and re-exported without the intervention of the customs authorities of that country
Great Firewall (GFW, 防火长城)	A combination of legislation and technologies used by the Chinese government to regulate the Internet in China
Information Warfare Monitor (IWM)	A research partnership between Ottawa-based think tank SecDev Group and the Citizen Lab at the Munk School of Global Affairs, University of Toronto, that operated between 2003-2012
Initial public offering (IPO)	The process of offering shares of a private corporation to the public in a new stock issuance for the first time

Terminology	Explanation
International Telecommunication Union (ITU)	A specialized agency working under the United Nations (UN) that is responsible for matters related to information and communications technologies (ICT)
Internet of Things (IoT)	Physical objects with sensors or other technologies that connect to a network to exchange data with other devices and systems over the Internet or other communications networks
Internet Society (ISOC)	Non-profit technical and civil society advocacy organization founded in 1992 with local chapters globally "to promote the open development, evolution, and use of the Internet for the benefit of all people throughout the world"
IP (Internet protocol)	The network layer communications protocol for relaying datagrams across different networks to enable internetworking, thus forming the technical basis of the Internet
IPv6	"Internet Protocol version 6," the most recent version of the IP protocol developed by the IETF to deal with the long-anticipated problem of the exhaustion of IPv4 (the current and most prevalently used version) addresses
IPv6+	An "intelligent IP network" proposed by Huawei for more flexible network connection, faster service provisioning, on-demand service customization, and a differentiated service performance guarantee
ISO/IEC 8802-11	Standards for telecommunications and exchange between information technology systems — requirements for local and metropolitan networks — that comprise part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications

Terminology	Explanation
ITU Telecommunication Standardization Sector (ITU-T)	A set of study groups that assembles global experts to develop international standards, known as ITU-T Recommendations, that act as defining elements in the global infrastructure of information and communication technologies (ICT)
Key opinion leader (KOL)	An active social media user who interprets events or provides views that influence other users
Monetization	The conversion of something into money or assets for an entity, such as a company, which may stretch beyond products or services and comprise things like business relationships, data, or other more intangible resources
New IP	A new set of proposals for a future Internet Protocol framework supported by Huawei (华为) that was introduced to the ITU, Internet Engineering Task Force (IETF), and various Institute of Electrical and Electronic Engineers (IEEE) conferences
Over-the-counter (OTC)	The trading of securities via a broker-dealer network as opposed to a centralized stock exchange
The Golden Shield project (金盾工程)	China's national network security infrastructure project that was first undertaken in the late 1990s and subsequently initiated a subproject that came to be known as the Great Firewall of China
Tor Browser	The browser that integrates Tor (short for "The Onion Router"), a free and open-source software that directs Internet traffic over a global volunteer-based network to conceal its users' content and locations

Terminology	Explanation
URL (uniform resource locaters)	A web resource that is used to specify and retrieve a computer network, such as, most commonly, a web page, and thus also often known as a “web address”
Virtual reality (VR)	A simulated experience that gives the user an immersive feel of a virtual world, usually by tracking the user’s pose and using 3D near-eye displays
Web 2.0	A term that became popular in the early 2020s and comprises web technologies and constructs with a participatory and interoperable culture that emphasize user-generated content (UGC), such as blogging
WeChat	Or Weixin (微　信) in Chinese, a Chinese “super app” developed by Tencent (腾讯) with functions including instant messaging, social media, mobile payment, etc.
Weibo	A general term for microblogging platforms in China, but may also be used to refer to the dominant microblogging platform Sina Weibo (新浪微博)
WPS	Or “WPS Office,” previously known as “Kingsoft Office,” stands for “Writer, Presentation and Spreadsheets” and is an office suite developed by Chinese software developer Kingsoft
Zero-day flaws	A software vulnerability that is discovered but was previously unknown even to the vendor or producer of the target software itself

Executive Summary

The Internet is facing its biggest crisis to date. Gone are the days when the Internet was generally seen as a force for good, equality, and empowerment. Now, the Internet is facing multiple threats from all directions, and the biggest threat it faces now may be that it is being fragmented "into separate networks, dominated by governments and corporations, which control what people see and what services they use."[1] Yet the world has become increasingly dependent on the Internet, and its people, businesses, and even governments are increasingly finding that they simply cannot function without it.

What they may not know is that what they really need is an Internet that is true to its original design and implementation — one that is open, collaborative, secure, and resilient — and for Internet users to know that their information and communications are private and that they can trust this medium to freely exchange, transact, and share.

A major part of the reason why the Internet is facing such an existential threat today is that there are forces, backed by powerful states, that want to turn the Internet into a framework of tools for surveillance and total control of each individual as well as whole societies. Today, more than 1 billion Internet users in China,[2] the country with the largest Internet population in the world, representing nearly one in five of the world's digital users,[3] live behind the Great Firewall (GFW). They have only been able to experience a censored and surveilled version of the Internet that is, with its own sets of platforms and applications that are highly controlled and monitored by the state, splintered and fragmented from the rest of the global Internet.

This is why we need to understand how the Chinese model of Internet governance came about, how it was first developed as a way to "keep the bad stuff out" through the state's filtering and absolute control and ownership of the core infrastructure in China, and how it gradually evolved into a sophisticated set of legal, technical, and operational apparatuses used by its totalitarian rulers to perfect a near real-time system of pervasive censorship across all platforms and channels to conduct propaganda and disinformation campaigns and to collect massive amounts of data.

What China is doing is more than mere censorship, but it is true that China's Internet governance model was based from the start on this censorship system — to regulate and rule by law through highly comprehensive and increasingly aggressive and progressive legislations and to exert economic and political control over all the major domestic commercial players as well as those global giants from abroad until they can no longer stand it. By the time they depart, China does not need these foreign companies anymore.

Meanwhile, China will seek to advance its vision for the Internet — surveillance, censorship, propaganda, data sovereignty, and so on — and thereby create a web of digital authoritarianism the likes of which the world has never seen. Authoritarian regimes can attack the Internet-based resources of their adversaries through, well, the Internet itself. The Internet, once feared as a potential Trojan horse, has turned out to be a great tool of political repression and geopolitical maneuvering.

Or has it?

As China seeks to transnationalize its digital repression regime, the democratic free world must respond strategically and decisively to protect the technology and the governance of the Internet and all the related technologies, platforms, standards, and frameworks.

Democracies must say no to the technologies, platforms, standards, and frameworks shrewdly proposed by China in various international fora and technical or standards bodies in order to make our Internet more like the one in China. Internet governance must be kept open and participatory for all stakeholders, not just governments. Research into and the development of privacy-preserving and anti-censorship technologies must be supported. A vision for a free and open global Internet must be integrated into future foreign policy formulation, not only because it should be, but also because China has already begun to integrate its own contrary vision.

Global Internet companies can see and learn from the mistakes they have made, just as we can be continually surprised at how prone they are to making the same mistakes again. They must also begin to understand the implications of their actions — and thus their responsibilities — for national security and global stability.

This paper will seek to examine how China's Internet governance and censorship regime has evolved, and what lessons can be learned from it so that democracies can find new ways or improve their existing strategy to preserve our core values and protect the Internet.

1 "Internet Society Action Plan 2023."https://www.internetsociety.org/action-plan/2023/
2 "Countries with the largest digital populations in the world as of January 2022." Statista. https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/
3 "Number of internet and social media users worldwide as of July 2022." Statista. https://www.statista.com/statistics/617136/digital-population-worldwide/

1. Introduction

The year was 2000, and U.S. President Bill Clinton was speaking on trade relations with China, which joined the World Trade Organization (WTO) the following year. In anticipation of the tools of communications becoming "cheaper, better, and more reliable," he said, "We know how much the Internet has changed America, and we are already an open society. Imagine how much it will change China." He went on to quip, "There's no question China has been trying to crack down on the Internet. Good luck. That's sort of like trying to nail Jell-O to the wall."[4]

While the quote was infamous for getting China's Internet control so ludicrously wrong, such sentiment was not unique to President Clinton at the time. The common perception widely shared by policymakers, the industry, and users then was that the Internet was an unstoppable force for good, equality, and freedom.

Ten years ago, when protests in the Middle East known as the Arab Spring were fading, the Internet and the new phenomenon of social media were generally credited with successfully organizing activists, exercising freedom of speech and civic engagement, as well as communicating to the rest of the world.[5]

Fast forward to today, and we see how far we have come in such a short time. Internet control in China is alive and striding — in the forms of hardened censorship, widespread surveillance, and even belligerent cyberattacks. The global view on the Internet itself has turned sour, with rampant disinformation, privacy issues, addiction, and every other social problem under the sun often blamed on the large Big Tech companies as well as inadequate government regulations, including those from democracies.

In 2022, the New York Times columnist and author Thomas Friedman "pleaded guilty" to his "premature optimism" that China would develop a more open information ecosystem, particularly to allow for a freer flow of uncensored news, when he became a columnist in 1995.[6] Indeed, in those earlier days of China's "opening up" to the world, the number of newly permitted news outlets was in stark contrast to the time just before it, and it was easy for anyone to be dazzled.

4 https://www.c-span.org/video/?c4893404/user-clip-clinton-firewall-jello
5 Heather Brown, Emily Guskin, and Amy Mitchell. "The Role of Social Media in the Arab Uprisings." Pew Research Center. November 2012. https://www.pewresearch.org/journalism/2012/11/28/role-social-media-arab-uprisings/
6 Thomas Friedman. "I Was Wrong About Chinese Censorship." July 21, 2022 https://www.nytimes.com/2022/07/21/opinion/thomas-friedman-china.html

Friedman is correct: We were wrong. Not only were we wrong about Internet censorship, but we were also wrong about the basic and widely held assumptions of the time about globalization, trade, diplomacy, geopolitics, and competition with a rising power, as well as where China was heading and how it would rise.

We overlooked the fact that our early optimism about the Internet and its positive forces were actually seen as existential threats for autocrats right from the start. And by shrewdly taking a long view, they were able to chart a course toward exercising absolute control by having the Internet serve their own regimes. In this sense, China's Internet strategy has been extremely consistent, highly adaptable, and evolutionary, while undergoing frequent refinements.

Over the years, China's goals have changed from isolation to competition, its tactics have turned from defensive to offensive, its focus has expanded from technical to governance, and its reach has been transformed from inside to outside, local to global, or national to transnational. This paper will examine China's evolution in its Internet control and governance, as well as the growing set of tools, components, actors for its censorship, and overall Internet policy. To that end, the paper will discuss the technical, operational, industrial, legal, regulatory, and diplomatic aspects of these topics.

Even if predictions were wrong two decades ago, this should not mean that there is no hope for the future. If we were, as Thomas Friedman accepted, only "prematurely optimistic," what should we do better now to ensure Internet freedom for people inside China and to prevent the "free world" from becoming "more China-like" so that freedom can prevail in the end? Indeed, "becoming China-like" has become an increasingly urgent threat that even democratic nations around the world are facing as populist domestic calls for more Internet control are gaining support from citizens and lawmakers alike: more censorship because of disinformation, election interference, and online child safety; more surveillance because of crimes and terrorism, and so on.

Policymakers in the so-called "free world" must realize that this is much more than just about protecting their citizens and their ways of life from the "dangers of the Internet." Instead, what we do may go a long way in setting the direction of the Internet's development as stakeholders compete over the Internet's infrastructure and the setting of its narrative, namely whether it becomes more authoritarian, splintered, or fulfills our original hopes of it being a positive game-changer. In order to compete, the industry, civil society, technologists, and users should understand China's game plan better.

2. China's Internet Governance — Censorship and Repression

China's Internet control and governance are, as this paper will show, more than just about censorship or the "Great Firewall" (GFW). Yet the objective of censorship was central to the initial establishment of filtering by the GFW. The concept of censorship has since evolved to cover a lot more than simply keeping certain websites or content out of reach for Internet users in China or the deletion of messages on China's Internet platforms.

If keeping things out was just one of the tactics, then the grand objective of censorship must be something more fundamental. To China's officials, "censorship" is not the right word to use: "management" is. As a country with a high number of Internet users, better management sounds like a justified reason to implement relevant rules and restrictions. After all, no nation would entirely regulate the Internet or leave it unmanaged, so China's rulers will say that it is not different from the rest of the world: There are rules, and if anyone breaks them, there should be consequences as laid out in the respective law[7].

2.1. How Many Internet Users Within China Circumvent the Great Firewall?

The term "Great Firewall" may lead to the impression that it is impermeable — but it never is and was most likely never even intended to be. Academics call this "porous censorship," where, rather than aiming at implausible watertight bans on all undesired content, censors impose a tax, or a high cost, on access to certain content rather than absolute prohibition by a matter of design choice.[8] By routinely making it more inconvenient to reach certain content, such as by delisting it in search engines, displaying a "404 Not Found" error, or slowing the access speed, most Internet users, if not all of them, will be adequately disincentivized. Eventually, users will turn to other more accessible alternatives the censors and authorities have permitted. If only a small percentage of users have the

7 外媒质疑中国网络审查制度日趋严格 鲁炜：用词不当 http://news.sina.com.cn/c/2015-12-09/doc-ifxmifzc0923447.shtml

8 Margaret E. Roberts. "Censored: Distraction and Diversion Inside China's Great Firewall." 2018. Chapter 1, 1.1.

persistence to find such data by using circumvention tools or a virtual private network (VPN), the censors may consider their job well-accomplished.

While there are no official statistics or accurate estimations regarding how many Internet users within China regularly circumvent the Great Firewall, studies over the past decades may shed some light. A 2000 Chinese Academy of Social Sciences (CASS) survey of Internet users across five Chinese cities discovered that 10 percent of the survey participants admitted to "regularly" using proxy servers to circumvent censorship and that 25 percent "occasionally" did the same.[9] By 2010, a much more technical and thorough Harvard study based on the use of proxies, VPNs, and other circumvention technologies found a much lower figure: No more than 3 percent of Internet users from countries that engage in substantial filtering (including China) were using circumvention tools, and "the actual number is likely considerably less."[10] Another 2015 user survey also suggested that only 5 percent of urban residents ever attempted circumvention.[11]

It is certainly noteworthy — and a testament to China's relative openness twenty years ago — that an official research institute of China, CASS, would conduct a survey that openly asks questions about bypassing government censorship regulations. On the other hand, if the percentages and numbers found in subsequent studies by western academics seem much lower, it is quite likely because in 2000, the early Internet adopters were more urban, technically savvy, well-resourced, and educated. In comparison, many of the surveyed users from subsequent studies were from rural regions. Moreover, the rapid growth of the Internet and mobile users in China after 2000 will have affected these results. Studies have also confirmed that citizens who circumvent the GFW tend to be younger, better educated and resourced, more knowledgeable about politics, have less trust in the government, and have connected with foreigners before.[12]

2.2. Toward More Draconian Rules and Propagandist Disinformation

Internet censorship is more than simply blocking or banning certain content. It is better defined as "the restriction of the public expression of or public access to information by authority."[13] A prominent Harvard study concluded that censorship "is aimed at curtailing collective action by silencing comments that represent, reinforce, or spur social mobilization, regardless of content," attempting to "forestall collective activities that are occurring now or may occur in the future."[14]

Prof. Margaret Roberts theorizes that there are three approaches to Internet censorship: fear, friction, and flooding.[15] Fear-based censorship is conveyed through laws, regulations, and potential punishments and acts as a legal deterrence and form of intimidation to restrain and suppress the expression of undesirable information by the media and influencers. Friction-based censorship would be applied to a wide range of users to make it difficult for them to reach or search for certain content. Finally, flooding-based censorship creates content diversions to transfer the users' attention from undesirable content to more mundane and sometimes even propagandist information. A 2017 Harvard study estimated that an army of Chinese government helpers wrote 488 million fake posts within a year and were collectively known as the "50 cents party" because each post made was said to be worth a RMB 50 cents reward.[16] During the recent waves of anti-COVID lockdown protests in China, bots, allegedly from China, flooded Twitter with explicit pornographic content by manipulating keywords and tags when users searched for news related to the demonstrations or even just the names of many Chinese cities.[17]

As Chinese Internet users tried to acquire health information during the COVID-19 pandemic, the use of circumvention to reach banned platforms, such as Twitter and Wikipedia, increased.[18] Although research shows that "awareness of censorship can draw consumers toward rather than away from information,"[19] rather than backing down, Chinese censors have stepped up their censorship efforts during this campaign. DYX, the country's leading digital health portal, was banned in 2022, with its social media accounts on Weibo, WeChat, and Douyin suspended for violations of "relevant laws and regulations" due to its indirect rebuke of China's zero-COVID policy by shunning traditional Chinese medicine and criticizing China's health system.[20]

9 "II. How Censorship Works in China: A Brief Overview" in "Race to the Bottom: Corporate Complicity in Chinese Internet Censorship." Human Rights Watch. 2006. https://www.hrw.org/reports/2006/china0806/3.htm

10 Hal Roberts, Ethan Zuckerman, Rob Faris, and John Palfrey. "2010 Circumvention Tool Usage Report." The Berkman Center for Internet & Society. October 2010. https://cyber.harvard.edu/sites/cyber.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf

11 Margaret E. Roberts. "Censored: Distraction and Diversion Insider China's Great Firewall." 2018. Chapter 5, 5.2.1.

12 Ibid. Chapter 5, 5.2.2.

13 Ibid. Chapter 2, 2.5.

14 Gary King, Jennifer Pan, and Margaret E. Roberts. "How Censorship in China Allows Government Criticism but Silences Collective Expression."2013. https://gking.harvard.edu/files/censored.pdf

15 Margaret E. Roberts."Censored: Distraction and Diversion Inside China's Great Firewall." 2018. Chapter 2, 2.7-2.9.

16 Gary King, Jennifer Pan, and Margaret E Roberts."How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument." Harvard University. April 9, 2017. https://gking.harvard.edu/files/gking/files/50c.pdf?m=1463587807

17 Ryan Fahey."Chinese bots flood Twitter with explicit porn to drown out news of lockdown protests." The Mirror. November 28, 2022. https://www.mirror.co.uk/news/world-news/chinese-bots-flood-twitter-explicit-28604491

18 "Circumvention of Censorship in China Has Increased During COVID-19 Pandemic." UCLA. January 19, 2022. https://luskin.ucla.edu/circumvention-of-censorship-in-china-has-increased-during-covid-19-pandemic

19 Margaret E. Roberts. "Censored: Distraction and Diversion Inside China's Great Firewall." 2018. Chapter 7, 7.2.

20 Zeyi Yang. "China has censored a top health information platform." MIT Technology Review. August 11, 2022. https://www.technologyreview.com/2022/08/11/1057592/china-censored-health-information-platform/

A different sort of censorship happened in the aftermath of U.S. House Speaker Nancy Pelosi's visit to Taiwan in early August 2022, demonstrating the complexity and sensitivity often involved in censorship. A tidal wave of negative comments against perceived Chinese military inaction, which fell short of the official rhetoric of "strong retaliations" prior to the visit, took over social media. Certain comment sections of WeChat threads were suspended, but censors did not completely ban most of the critical comments,[21] as nationalist netizens' emotions must be carefully managed and not further provoked.

But propagandist flooding tactics can also backfire. After Russia invaded Ukraine in February 2022, pro-Kremlin propaganda originating from Chinese social media platforms were translated from Chinese into multiple languages and cross-posted on Twitter and other social media platforms outside China's Great Firewall. This so-called "Great Translation Movement" was launched primarily by overseas Chinese.[22] These messages laid bare the pro-Russian disinformation being circulated inside China, contrasting with the relatively restrained official positions from Chinese diplomats. As a result of the embarrassment, China's official English-language mouthpiece, Global Times, blamed "anti-China forces from the U.S. and Taiwan" of "smearing China" by "selectively translating some relatively aggressive rhetoric on Chinese social media."[23]

Under the rule of President and Party Secretary Xi Jinping, China's censorship approach has shifted from being more porous to more fear-based, and intimidations are being applied beyond the elites and the media. In the past, Chinese authorities, fearing backlash, were more restrained during crises when the people typically became more motivated than usual to seek out information and overcome censorship restrictions. However, as the paper will show in a later section, China's interventions have become more rapid and repressive during times of crisis, including during the crackdowns in Xinjiang and Hong Kong or the "white paper" anti-zero-COVID protests across China in late 2022, when many were traced and apparently detained by authorities using phone and social media records as well as public surveillance systems. [24]

21 Li Yuan. "Perils of Preaching Nationalism Play Out on Chinese Social Media." https://www.nytimes.com/2022/08/04/business/new-world-nancy-pelosi-taiwan-social-media.html

22 "Great Translation Movement." https://en.wikipedia.org/wiki/Great_Translation_Movement

23 大翻译运动向全球展现中国网民言论 指中国官媒"说谎" https://www.rfi.fr/cn/%E4%B8%AD%E5%9B%BD/20220328-%E5%A4%A7%E7%BF%BB%E8%AF%91%E8%BF%90%E5%8A%A8%E5%90%91%E5%85%A8%E7%90%83%E5%B1%95%E7%8E%B0%E4%B8%AD%E5%9B%BD%E7%BD%91%E6%B0%91%E8%A8%80%E8%AE%BA-%E6%8C%87%E4%B8%AD%E5%9B%BD%E5%AE%98%E5%AA%92-%E8%AF%B4%E8%B0%8E

24 Paul Mozur, Claire Fu, and Amy Chang Chien. "How China' s Police Used Phones and Faces to Track Protesters." The New York Times. December 2, 2022. https://www.nytimes.com/2022/12/02/business/china-protests-surveillance.html

3. The Growing Legal and Technical Toolbox

Now, let us take a step back and take a closer look at China's Internet policy and governance, and how its Great Firewall (GFW) is constructed. Even though the Internet is a relatively new technology and phenomenon, censorship has been neither new nor foreign to China throughout its history: The Qin Dynasty was notorious for the "burning of books and burying of scholars,"[25] the actual Great Wall was ultimately built to keep out the foreigners almost 2,200 years ago,[26] and the modern day Chinese Communist Party (CCP)'s censorship system was elaborately crafted even from the time of Mao Zedong's rule.[27]

As China's GFW and its overall censorship mechanism have evolved over the years, its components have comprised technical, operational, commercial, legal, regulatory, and enforcement elements. As we shall see, these elements are increasingly transnational, extending beyond the borders of China.

3.1. Rule by Law

3.1.1. Controlling the Infrastructure

First, let's take a look at the beginning of the Internet in China. In the late 1980s, various academic institutions in China began to initiate private connections with North America and Europe through the establishment of the Chinese Academic Network (CANET) and the Chinese Research Network (CRNET). The country's top-level domain of .cn was obtained in 1990 from the Defense Data Network Network Information Center (DDN-NIC), the former international Internet information center operating under the Advanced Research Projects Agency Network (ARPANET) — the first public packet-switched computer network that was the predecessor of the Internet — of the U.S. Department of Defense.

25 "Burning of books and burying of scholars (焚書坑儒)." https://en.wikipedia.org/wiki/Burning_of_books_and_burying_of_scholars
26 "The Great Wall of China." https://en.wikipedia.org/wiki/Great_Wall_of_China
27 "Censorship in China." https://en.wikipedia.org/wiki/Censorship_in_China

By 1994, the China Science and Technology Network (CSTNET) was launched with the first formal Internet linkage both nationally and internationally, and the China Education and Research Network (CERNET) was set up later in the year to connect the countries' research institutions, colleges, and universities. By early 1995, China's domestic state-owned telecommunications incumbent carrier, China Telecom, obtained an agreement with the U.S. government to lease two 64kbps dedicated circuits to connect to the U.S. from Beijing and Shanghai, which became the blueprint for the backbone of China's future Internet, ChinaNet.[28]

CSTNET, CERNET, and ChinaNet, together with China Gold Bridge Network (CHINAGBN or GBNet),[29] a national economic information network for electronic data interchange (EDI), formed the initial backbone of China's Internet. All infrastructure and access routes are owned and controlled by the Chinese government, and this is important as a foundation for censorship. Only the three state-owned telecommunications carriers were initially allowed to provide commercial Internet services: China Telecom, China NetCom, which was later merged with China Unicom, and China Mobile. At first, there were only three external gateways connecting China's national network to the outside world, located in Beijing, Shanghai, and Guangzhou, but this was later expanded to seven more connection points in 2015.[30]

The Chinese central government's complete ownership of the Internet at the level of its infrastructure allows it to exert total control and authority over the backbone of China's Internet, from the physical to the service layers. In particular, its stranglehold on international connectivity makes it relatively straightforward for the authorities to filter incoming traffic and content from the beginning.

But one may also take note of the similar ways in which the Internet began in the U.S. and China — they both have strong government roots. The development from that point on, however, went in different directions. In the U.S., the Internet was privatized, and the government largely ceded control as the Internet became more commercialized and used by everyone. In China, the government retained complete and absolute control of Internet governance.

3.1.2. Setting the Baseline

The three earliest examples of central government legislation for the Internet in China were the Temporary Regulation for the Management of Computer Information Network International Connection (the Regulation, first passed by the State Council in January 1993 and rectified in February 1996), the Ordinance for Security Protection of Computer Information System (the Ordinance, issued on February 1994 by the State Council), and the Security Management Procedures in Internet Accessing (the Procedures, approved by the State Council and issued by the Ministry of Public Security in December 1997).[31]

The Regulation affirms the state's sole and absolute right to build, manage, and control the Internet, including "the principle of overall planning, unified standard, stratified management, and advance in development" toward international network connection, and specifically :

- No units or individuals are allowed to establish a direct international connection by themselves.
- All direct linkage with the Internet must go through ChinaNet, GBNet, CERNet, or CSTNet.
- A license is required for anyone who wants to provide Internet access to users, and the user must register to obtain access.
- Harmful information that is either subversive or obscene is forbidden.

The Ordinance stresses that the responsibility for Internet security protection falls under the Ministry of Public Security, which would "supervise, inspect, and guide the security protection work"; "investigate and prosecute illegal criminal cases"; and "perform other supervising duties." The Ordinance was later further developed to form the Procedure to further specify the nature of "harmful activities," covering acts of intrusion, misuse, hacking of programs or data without authorization, and intentionally producing or distributing viruses and other ways or causing harm to the computer information network.

28 "Evolution of Internet in China." January 1, 2001. https://web.archive.org/web/20120527120608/http://www.edu.cn/introduction_1378/20060323/t20060323_4285.shtml

29 CHINAGBN. https://baike.baidu.com/item/CHINAGBN/3438473

30 Chengdu (成都), Xian (西安), Wuhan (武汉), Shenyang (沈阳), Nanjing (南京), Chongqing (重庆), Zhengzhou (郑州) — 新增7个国家级互联网骨干直联点建设全面竣工. 2015.1.12. https://web.archive.org/web/20150121025150/http://www.miit.gov.cn/n11293472/n11293832/n11293907/n11368223/16402896.html and "The Chinese Internet Gets A Stronger Backbone." 2015. https://www.forbes.com/sites/lisachanson/2015/02/24/the-chinese-internet-gets-a-stronger-backbone/?sh=1ea5a16e1ff4

31 Jack Linchuan Qiu. "Virtual Censorship in China: Keeping the Gate Between the Cyberspaces." 1999/2000. https://ciaotest.cc.columbia.edu/olj/ijclp/ijclp_4/ijclp_4a.pdf

In the early days, most of the responsibilities for content control fell on the respective backbone networks. So, it was their regulations that defined what was allowed and wasn't. The rules were not entirely the same everywhere. For instance, GBNet's management procedures would not allow users to "produce, view, disseminate and announce harmful information that disturbs social security and contains obscene content" and asserted that "national security regulations must be strictly abided by." Meanwhile, CERNET's regulations stipulated that it must "resolutely delete articles with political problems."

By December 1997, the Computer Information Network and Internet Security, Protection and Management Regulations, issued by the Ministry of Public Security, specified the categories of banned content in its Article 5:[32]

"No unit or individual may use the Internet to create, replicate, retrieve, or transmit the following kinds of information:

(1) Inciting to resist or violate the Constitution or laws or the implementation of administrative regulations;
(2) Inciting to overthrow the government or the socialist system;
(3) Inciting division of the country, harming national unification;
(4) Inciting hatred or discrimination among nationalities or harming the unity of the nationalities;
(5) Making falsehoods or distorting the truth, spreading rumors, destroying the order of society;
(6) Promoting feudal superstitions, sexually suggestive material, gambling, violence, murder;
(7) Engaging in terrorism or inciting others to criminal activity; openly insulting other people or distorting the truth to slander people;
(8) Injuring the reputation of state organs;

Other activities against the Constitution, laws, or administrative regulations."

In addition, Article 8 of the same regulation also provided vast power to the public security apparatus to inspect and seize information from all individuals and other entities in China:

"Units and individuals engaged in Internet business must accept the security supervision, inspection, and guidance of the Public Security organization. This includes providing to the Public Security organization information, materials and digital document [sic!], and assisting the Public Security organization to discover and properly handle incidents involving law violations and criminal activities related to computer information networks."[33]

3.1.3. Dealing with the Commercial Internet

As the commercial Internet began to flourish in China at the turn of the millennium, more regulations emerged to enhance control over specific Internet operators or business models.

One of the first practical industry regulations imposed on Internet services was the real-name system. From the government's point of view, the authorities must first and foremost be able to identify any perpetrator. It would also want to make sure that the users had a tangible fear, knowing full well that any of their online actions could be traced back to their real identity and that they would thus be held accountable and liable to repercussions. Through requests by various government departments and regulators, as well as industry self-regulations, many Internet service providers, such as Internet cafes, fell in line to impose mandatory real-name registration requirements for users from as early as 2003.[34]

In December 2012, the Standing Committee of the National People's Congress passed the "Decision Relating to Enhanced Network Information Protection,"[35] requiring the collection of personal identification information when users registered for services including website access, fixed and mobile telephone services, or other online information services. But before the law came into effect in March 2012, all four major micro-blogging platforms (Weibo) run by Sina, Sohu, Netease, and Tencent had already voluntarily adopted the real-name system altogether.[36]

As more people turned to VPNs to circumvent restrictions, in 1996, the Ministry of Commerce issued the Interim Regulations of the PRC on the Management of International Networking of Computer Information to prohibit connection to "international networks" using channels outside government-approved providers.[37]

Also, regulations targeting information service providers emerged later to directly regulate operators that provided services over the telecommunications network providers. For instance, Article 57 of the Telecommunications Regulations of The People's Republic of China, issued by the State Council in September 2000, stated that:

32 "Freedom of Expression and the Internet in China: A Human Rights Watch Backgrounder." Human Rights Watch. https://www.hrw.org/legacy/backgrounder/asia/china-bck-0701.htm
33 "Freedom of Expression and the Internet in China: A Human Rights Watch Backgrounder." Human Rights Watch. https://www.hrw.org/legacy/backgrounder/asia/china-bck-0701.htm
34 "沈阳网吧今起实名上网." July 10, 2003. https://web.archive.org/web/20180221100747/http://hnfy.chinacourt.org/article/detail/2003/07/id/679048.shtml
35 "授权发布：全国人民代表大会常务委员会关于加强网络信息保护的决定." https://web.archive.org/web/20130203205216/http://www.npc.gov.cn/npc/xinwen/2012-12/29/content_1749526.htm
36 "中国官方继续清网 全面推行实名制." https://www.dw.com/zh/%E4%B8%AD%E5%9B%BD%E5%AE%98%E6%96%B9%E7%BB%A7%E7%BB%AD%E6%B8%85%E7%BD%91-%E5%85%A8%E9%9D%A2%E6%8E%A8%E8%A1%8C%E5%AE%9E%E5%90%8D%E5%88%B6/a-18187414
37 "Interim Regulations on the Management of International Networking of Computer Information." http://www.asianlii.org/cn/legis/cen/laws/irotmoinoci880/

"No organization or individual may use telecommunications networks to make, duplicate, issue, or disseminate information containing the following:

(1) Material that opposes the basic principles established by the constitution;
(2) Material that jeopardizes national security, reveals state secrets, subverts state power, or undermines national unity;
(3) Material that harms the prosperity and interests of the state;
(4) Material that arouses ethnic animosities, ethnic discrimination, or undermines ethnic solidarity;
(5) Material that undermines state religious policies, or promotes cults and feudal superstitions;
(6) Material that spreads rumors, disturbs social order, or undermines social stability;
(7) Material that spreads obscenities, pornography, gambling, violence, murder, terror, or instigates crime;
(8) Material that insults or slanders others or violates the legal rights and interests of others;
(9) Material that has other contents prohibited by laws or administrative regulations."[38]

Then, in order to regulate the popular Internet news portals in the early 2000s, the State Council Order No. 292 was issued, which required licensing for websites to operate legally as "Internet information services related to news, publication, education, medical care, pharmaceuticals and medical equipment, etc." Non-licensed websites could only redistribute news from other licensed news media. After that, websites could no longer link to overseas news websites without separate approval — regardless of whether the overseas sites were blocked by the Great Firewall. A news publication qualifications permission system was also established that effectively halted the proliferation of private websites in China carrying news items; for instance, it was reported that by the end of 2008, only 8 websites out of 430,000 in Guangdong Province were able to obtain news publication licensing permits to continue operation.[39]

These are just a snapshot of the laws comprising the early stages of the formation of Internet regulations in China. It should be noted that one characteristic of this phase of regulation was that these laws tended to overlap and were administered by multiple regulatory functions at various levels of government. This was partly out of administrative competition as well as by design to ensure completeness and the flexibility to use the "most appropriate" law for the particular circumstance. In general, leadership was still placed in the hands of the security and propaganda functions of the government.

However, in 2014, this changed with the leadership of Xi Jinping as the CCP's General Secretary and China's President. The line between the state and the party blurred even further, particularly with regard to Internet regulations.

Previously, China's Internet policies were managed by the State Internet Information Office (SIIO), which operated under the State Council Information Office (SCIO). However, the SIIO was transformed to become the Party Office of the new Central Cybersecurity and Informatization Leading Small Group and later upgraded to the Central Cyberspace Affairs Commission. This commission was chaired by Xi Jinping himself as director. By 2018, the new Cyberspace Administration of China (CAC) had sealed its place as the operating arm of the Commission, with a clear line of command to the top of the CCP leadership and the state as well as complete authority and overall responsibilities for the entire cyber policy system.[40]

Commonly referred to as China's "Internet censor" or "Internet regulator," the CAC would consolidate China's Internet laws with a series of even more comprehensive legislation in the years to come, starting with the Cybersecurity Law (CSL) of 2017, the more recent Data Security Law (DSL), and the Personal Information Protection Law (PIPL). These laws signaled a push for more control over data collection, use, and transfer by introducing the concept of "data sovereignty." They also empowered the state by giving it more extraterritorial authority under Chinese law.

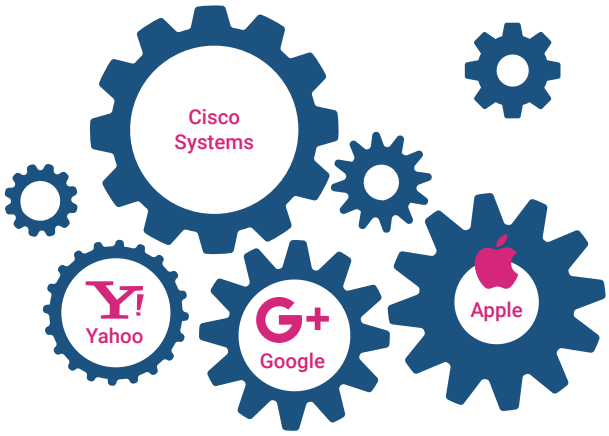
The Cybersecurity Law, passed by the Standing Committee of the National People's Congress in November 2017, is an amalgamation of previous Internet and censorship laws. It unified and institutionalized the legal and administrative framework for control. This law required network operators to store data locally in China and turn over information when requested by state security agencies. The so-called "critical information infrastructure" became subject to a national security review with obligations over data security, procurement, cross-border data flows, etc. Persons or organizations using the networks should not "incite subversion of national sovereignty, overturn the socialist system, incite separatism, break national unity, advocate terrorism or extremism, advocate ethnic hatred and ethnic discrimination, disseminate violent, obscene, or sexual information, create or disseminate false information to disrupt the economic or social order."[41]

The definitions used were quite vague, leading to a number of issues. For one, domestic and foreign companies in China were often uncertain about what actually fell under "critical information infrastructure" and whether or how they should comply with the Cybersecurity Law. So, some clarifications were made in 2021 with the State Council's

38 "Freedom of Expression and the Internet in China." Human Rights News. https://www.hrw.org/legacy/backgrounder/asia/china-bck-0701.htm
39 Bei Feng. "China's Internet Censorship System." Human Rights in China. July 14, 2010. https://www.hrichina.org/en/content/3244
40 Nathan Attrill and Audrey Fritz. "China's Cyber Vision: How the Cyberspace Administration of China is building a new consensus on global Internet governance." ASPI. 2021. https://www.aspi.org.au/report/chinas-cyber-vision-how-cyberspace-administration-china-building-new-consensus-global
41 Rogier Creemers, Paul Triolo, and Graham Webster. "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)." 2018. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

release of the "Critical Information Infrastructure Security Protection Regulations," effective from September 2021. This release specified that, for example, companies that handled data and were listed on foreign stock exchanges would be considered as "critical information infrastructure." It was this specification that led to the 2021 crackdown on Didi Chuxing, China's leading ride-hailing company, when it was listed in the U.S.[42]

3.2. The Tools



3.2.1. Filtering

Although today the Chinese censorship system is generally referred to as the "Great Firewall" (GFW), the actual official project was called the Golden Shield Project, built as a nationwide security management information system. The GFW was a subproject for censorship and surveillance, operated by the Ministry of Public Security from 1998 and entering into full operation in 2003.

The GFW initially focused on the active filtering of Internet traffic to keep out sensitive content, including the filtering of IP (Internet protocol) address ranges, DNS (domain name service), URL (uniform resource locaters), as well as deep packet inspection (DPI), which is based on learning about the pattern of traffic units on the Internet called packets. A comprehensive and dynamic list of keywords was developed and maintained for the purpose of filtering. As more users started using proxies such as the Tor browser or VPNs to circumvent the filters, GFW censors turned to active probing to try to identify and block such traffic too.[44]

Very soon after the initiation of the Golden Shield project, blogging and then micro-blogging and social media appeared and became popular with users around the world — including China. With the so-called user-generated content taking centerstage during the Web 2.0 phenomenon, such content would quickly overtake the volume of production from the media and other traditional and Internet news and content sources. The censors found themselves having to contend with not only blocking incoming foreign content but also a rapidly growing volume of content generated within China's own borders, especially from the users. In addition to filtering at the backbone level, the GFW system now also had to delegate to the major Internet services and social media platforms in China the task of filtering content generated on their platforms.

Platforms often set up lists of filter keywords based on government-supplied lists. The operation became increasingly dynamic and had to respond rapidly to new changes. Chinese Netizens are well-known for using homonyms or homophones (characters having the same pronunciation but different meaning), "mis-written" or variants of characters, and even typos to act as substitutes for blocked sensitive characters, keywords, or phrases to evade the GFW censorship.[45] So, in 2017, Weibo (formerly Sina Weibo), China's leading Twitter lookalike micro-blogging platform, publicly recruited 1,000 users to become their "Weibo supervisors" to help monitor and report "pornographic, illegal, or harmful" messages.[46] In a recent wave of crackdowns on these evasion-tactics, Weibo announced that it would improve its "phrase management mechanism" and perfect its "keyword identification model" to induce a positive encouragement system to "guide users to properly use Chinese characters" on its platform.[47] However, with the complexity of the Chinese language and the creativity of the users — by using the Chinese words for Holland ("Helan") to represent Henan Province when discussing the 2022 banking crisis there, for example — the collateral damage of blocking characters, words, and phrases will be large, and such censorship will come at a high cost to user experience.

A series of leaked documents in 2022 from Xiaohongshu, a Chinese Instagram-like platform, revealed that content moderators of the site had uncovered 546 nicknames for Xi Jinping over a period of two months.[48] The leak confirms the use of real-time responses by operators during major political events, disturbances or their anniversaries, and natural disasters or accidents to conform to the requirements of the Cyberspace Administration of China, the nation's chief online censor.[49]

It is clear that censorship operations have become more systematic and automated but less transparent over the years. In 2016, the Citizen Lab reported that users of WeChat — Tencent's messaging "super-app" — would no longer receive notifications if their messages were

42 Paul Triolo, Samm Sacks, Graham Webster, and Rogier Creemers. "After 5 Years, China's Cybersecurity Rules for Critical Infrastructure Come Into Focus." August 8, 2021. https://digichina.stanford.edu/work/after-5-years-chinas-cybersecurity-rules-for-critical-infrastructure-come-into-focus/

43 Charles Arthur. "China tightens 'Great Firewall' internet control with new technology." The Guardian. December 14, 2012. https://www.theguardian.com/technology/2012/dec/14/china-tightens-great-firewall-internet-control

44 "Learning more about the GFW's active probing system." September 14, 2015. https://blog.torproject.org/learning-more-about-gfws-active-probing-system/

45 Victor Mair. "Typos as a means for circumventing censorship." https://languagelog.ldc.upenn.edu/nll/?p=55382

46 https://m.weibo.cn/status/4156562153528739

47 "Weibo vows to regulate homonyms, 'misspelt' words, if they are used to evade China's strict censorship." July 14, 2022. https://www.scmp.com/tech/policy/article/3185299/weibo-vows-regulate-homonyms-misspelt-words-if-they-are-used-evade

blocked, whereas they did before. Also, more keywords are blocked on group chats than in one-to-one chats, indicating a stronger censorship mandate for messages that might reach a larger audience and thus lead to organized group actions. The app would also allow for a more flexible environment for registered users outside China than for domestically registered users, although users outside China still face censorship.[50]

And so, the GFW has started to extend beyond China's border, along with these Chinese apps and services. In 2020, the Citizen Lab uncovered that WeChat surveilled accounts registered outside China and used those messages to train their censorship algorithm to be used against accounts registered in China. For users, there was no transparency or any disclosure in its policy documents.[51]

In July 2022, a Chinese novelist complained on Weibo that she had been locked out of her own unpublished work of 1.3 million characters stored online in the WPS cloud word processor platform of the Chinese software developer Kingsoft. The reason that was given was that "the file may contain sensitive content and access has been disabled."[52] The allegation confirmed that GFW surveillance and censorship have extended to cloud-based applications and service providers. The novelist's Weibo post prompted many other Chinese users to share their own similar experiences. Some even claimed that WPS had the function of deleting not only users' online but offline files as well. Kingsoft responded to the accusations by saying that it was the user in question who was suspected of violating its "platform regulations."[53]

Fang Binxing, often credited as the "Father" of the GFW of China, disclosed in a 2011 interview that 1998 was the year of the turning point in China's Internet development, namely when Internet portals Sina and Sohu appeared and the number of Chinese Internet users surpassed one million. According to him, the government had to start paying attention then, and he claimed that "building the Great Firewall was a natural reaction to something newborn and unknown." He also justified the GFW by claiming that such practice was "a common phenomenon around the world" and that "about 180 countries including South Korea and the U.S. monitored the Internet as well." This statement is misleading, however, as it equates Internet regulations in democratic countries with draconian censorship in autocratic nations. Fang had no qualms about admitting the political nature of his position, saying that "China objected to any country's interference with China's internal affairs under the banner of Internet freedom."[54] To this date, this statement is still representative of the Chinese mentality in justifying its decision to deprive its citizens of their online freedom.

3.2.2. Spyware

In retrospect, it is ironic that while the Golden Shield project was at full speed, China was joining the World Trade Organization (WTO) in 2001, ushering in an atmosphere of global anticipation for its opening up to the world economy. The list of China's failed WTO commitments to this date is long, particularly regarding the opening up of the Chinese market to foreign producers for information and communications technology and telecommunications.[55] In fact, the year after China entered the WTO, in 2002, its investment in censorship via the Golden Shield project rose to $770 million, and the number of police and security officers working on censorship was estimated to be as high as 30,000. Despite criticism from the west, participants in the project proudly proclaimed at the time that they expected the censorship project to be completed before the 2008 Beijing Olympics, another event that the west thought could lead to China's integration into the world, with such hopes proving to be only wishful thinking.

With all that investment and manpower, the Golden Shield project would of course never be just about filtering, although that function was always the core of Chinese censorship. Chinese censors also tried other methods, though with uneven levels of success. The most notable high-profile example is "Green Dam" in 2009:

In May 2009, the Ministry of Industry and Information Technology (MIIT) announced that personal computers sold in China must be preloaded with a "green online filtering software" called "Green Dam Youth Escort" by July 1.[56] Manufacturers would be required to report the number of pre-loaded machines shipped to the government. The software would automatically download and update a list of websites and keywords, blocking access to those websites and shutting down a word processing program if a censored keyword was typed. The software would supposedly even recognize pornographic images by spot-

48 Joseph Brouwer. "List of derogatory nicknames for Xi leaked amid crackdown on 'typos'." July 20, 2022. https://chinadigitaltimes.net/2022/07/list-of-derogatory-nicknames-for-xi-leaked-amid-crackdown-on-typos/

49 Joseph Brouwer. "How Xiaohongshu censors 'sudden incidents'." July 27, 2022. https://chinadigitaltimes.net/2022/07/how-xiaohongshu-censors-sudden-incidents/

50 Lotus Ruan, Jeffrey Knockel, Jason Ng, and Masashi Crete-Nishihata. "One App, Two Systems: How WeChat uses one censorship policy in China and another internationally." The Citizen Lab. November 30, 2016. https://citizenlab.ca/2016/11/wechat-china-censorship-one-app-two-systems/

51 Miles Kenyon. "WeChat Surveillance Explained." The Citizen Lab. May 7, 2020. https://citizenlab.ca/2020/05/wechat-surveillance-explained/

52 Coco Feng. "Chinese word processor WPS accused of censorship after author says she was locked out of 1.3 million-character document." July 14, 2022. https://www.scmp.com/tech/big-tech/article/3185239/chinese-word-processor-wps-accused-censorship-after-author-says-she

53 "Kingsoft's Office Software WPS Denies Deleting User Local Files." https://pandaily.com/kingsofts-office-software-wps-denies-deleting-user-local-files/

54 "Great Firewall father speaks out." Global Times. February 18, 2011. https://web.archive.org/web/20110225205053/http://english.sina.com/china/p/2011/0217/360409.html

55 Stephen Ezell. "False Promises II: The Continuing Gap Between China's WTO Commitments and Its Practices." Information Technology and Innovation Foundation. July 26, 2021. https://itif.org/publications/2021/07/26/false-promises-ii-continuing-gap-between-chinas-wto-commitments-and-its/

56 "关于计算机预装绿色上网过滤软件的通知. 工业和信息化部." May 19, 2009. https://web.archive.org/web/20090612021926/http://www.miit.gov.cn/n11293472/n11293832/n11293952/12398220.html

ting skin colors in images. At the time, many of the Asian personal computer brands from Taiwan, Japan, and China itself followed the order and complied, such as Acer, Sony, Lenovo, Asus, and BenQ, while many of the U.S. brands, such as Hewlett-Packard (HP) and Dell, resisted.[57]

From its onset, Green Dam was a disaster. US-based software company Solid Oak Software claimed that source codes from its CYBERsitter product were copied.[58] The software was buggy, did not work well, and was relatively easy for knowledgeable users to get around. Even the password to unlock and disable the software was hacked and widely shared online.[59] In a rare and embarrassing turn of events, the MIIT announced that the program was indefinitely suspended before the program was supposed to go into effect. Green Dam was effectively abandoned in August, when the MIIT announced that sold retail computers would no longer be required to pre-install Green Dam and that only computers for schools, Internet cafes, or public use would still need to do so.[60]

Although Green Dam failed, it was important as the first comprehensive attempt to directly install a de facto spyware into all Chinese users' computers. It would certainly not be the last attempt to decentralize censorship down to the device level. Since around 2013, it has been reported that the government of Xinjiang began to install malware on Android phones used by the local Uyghur population on a massive scale. This was either done by hacking or by simply confiscating citizens' phones and returning them later with malware installed. In some cases, the citizen had a totally different phone returned to him or her. The spyware installed would allow officials to observe all activities carried out by the phone users on a real-time basis.[61]

Indeed, mobile apps on smartphones today have opened the door for hackers to lure unsuspecting users into downloading apps with malware or spyware, or for autocratic regimes to simply order their people to download those programs. For example, the criminal investigation branch of the Chinese Ministry of Public Security has created an app called "National Anti-Fraud Center," whose supposed purpose is for users to report online or telephone fraud to the police. It is estimated to have been downloaded over 200 million times. However, the app was found to be collecting excessive data from users' phones, including their personal information, browsing history, chat content, location data, etc. Some app users even reported that they were contacted by the police after they accessed certain foreign financial websites. [62]

3.2.3. Virtual Private Networks

Although regulation of international networks provides the basis for banning the use of virtual private networks (VPN) or other proxy services like Tor to bypass the government's sanctioned network services without approval, China has been known to only occasionally turn up the heat to make public warnings or individual administrative warnings for people who have been found to have been using VPNs. In 2019, however, it was reported for the first time that a fine of 1,000 yuan was imposed on a user in Guangdong Province for using a VPN.[63]

In fact, it was only in 2017, under the Xi administration, that the MIIT announced a 14-month "cleanup" of the Internet. The government used more drastic administrative and technical means to make the circumvention of censorship more difficult: The state-owned Internet providers China Telecom, China Mobile, and China Unicom were ordered to block VPN protocols on their networks, except those approved by the state that are typically reserved for some government enterprises or agencies.[64] One of the techniques used by Chinese censors is active probing, whereby they check instances of any previously unknown outbound VPN connections to attempt to verify their VPN blacklist.[65] These lists may be compiled dynamically by scraping the IP connection records of Tor and VPN servers over time, causing many VPN and proxy providers to counter by improving their dynamic IP addressing and other more robust evasive techniques.

Crackdowns on VPN are especially inconvenient for foreign companies operating in China since they make it harder for them to access the global Internet services they need to do their business, such as any non-Chinese social media, email, and news platforms. Some resort to using SIM cards from outside China to access such services. In July 2017, Apple followed China's order to remove VPN apps from its Chinese version of the App Store — VPN apps are now deemed "illegal content" in China. This makes it more difficult for domestic Chinese users to access such tools. At the same time, it is a dangerous precedent for a company of such size and market power

57 Joe McDonald. "PC makers voluntarily supply web filter in China." The Global and Mail. The Associated Press. July 2, 2009. https://web.archive.org/web/20090706135434/http://www.theglobeandmail.com/news/technology/pc-makers-voluntarily-supply-web-filter-in-china/article1203981/

58 Charles Mok. "Green Dam: Bad Idea." Computerworld Hong Kong. July 2009. https://charlesmok.blogspot.com/2009/07/green-dam-bad-idea.html

59 "绿坝-花季护航软件遭破解 使用者绕开密码限制." https://www.163.com/tech/article/5BHDPD8F000915BD.html

60 "Green Dam Youth Escort." Wikipedia. https://en.wikipedia.org/wiki/Green_Dam_Youth_Escort#cite_note-6

61 Paul Mozur and Nicole Perlroth. "China's Software Stalked Uyghurs Earlier and More Widely, Researchers Learn." The New York Times. July 1, 2020. https://www.nytimes.com/2020/07/01/technology/china-uighurs-hackers-malware-hackers-smartphones.html

62 "国家反诈中心, 中國數字空間." https://chinadigitaltimes.net/space/%E5%9B%BD%E5%AE%B6%E5%8F%8D%E8%AF%88%E4%B8%AD%E5%BF%83

63 David Spencer. "China's VPN crackdown now targeting individual users." February 3, 2020. https://www.vpncompare.co.uk/china-vpn-crackdown-individual-users/

64 Olivia Solon. "China cracks down on VPNs, making it harder to circumvent Great Firewall." January 23, 2017. https://www.theguardian.com/technology/2017/jan/23/china-vpn-cleanup-great-firewall-censorship

65 "Learning more about the GFW's active probing system." September 14, 2015. https://blog.torproject.org/learning-more-about-gfws-active-probing-system/

to adopt censorship on its platform on behalf of an autocratic government.[66] Sadly, it is no longer a surprise that in October 2022, when users in China were discovered using AirDrop, an Apple iPhone feature, to share photos related to the protest and slogan used by a protester called the "Bridge Man" with nearby iPhone users without accessing any mobile or Wi-Fi network, Apple promptly put a limit on AirDrop use exclusively for Chinese users through a China-only software update.[67]

3.2.4. Internet Shutdowns

Internet shutdowns are the most extreme form of censorship, whereby all access to the network is shut down completely or to a large extent, for example for major communications or information services. A 2022 report on Internet shutdowns, published by The Office of the United Nations High Commissioner for Human Rights (UN-OHCHR), concluded that "Internet shutdowns create significant obstacles that damage economies, democratic processes, and the flow of information, which may erode trust in electoral processes and increase the likelihood of hostilities and violence," and called on member states to refrain from "disrupting Internet access, including throttling or limiting bandwidth."[68]

Nevertheless, more and more governments around the world are using Internet shutdowns to curtail free expression or political dissent. But for China, it can be acknowledged that, possibly due to its meticulous "management" of the Internet through its sophisticated system of censorship and surveillance, the country rarely has to resort to this drastic "shortcut" of totally cutting off connections. But there are notable exceptions.[69]

Since the ethnic unrest in Urumqi, Xinjiang on July 6, 2009, which the authorities claimed led to 200 deaths, China has escalated its crackdown and control over the region and its Muslim population both offline and online. Regulations against "misinformation" and punishments for website operators for posting "unverified content" were imposed. The Internet was shut down for all residents in Xinjiang, allowing them access only to government-approved websites, essentially reducing the experience to a walled-off, one-way, receive-only "intranet."[70] In mid-May 2010, it was suddenly announced that the shutdown would be "lifted." In response, citizens flocked to cyber cafes to check through months of unread emails or to play online games. And while many struggled to recall their passwords, everything was, of course, still under strict surveillance.[71]

66 Saheli Roy Choudhury. "Apple removes VPN apps in China as Beijing doubles down on censorship." August 1, 2017. https://www.cnbc.com/2017/07/31/apple-removes-vpn-apps-in-china-app-store.html

67 Karen Gilchrist. "Apple limited a crucial AirDrop function in China just weeks before protests." CNBC. November 30, 2022. https://www.cnbc.com/2022/11/30/apple-limited-a-crucial-airdrop-function-in-china-just-weeks-before-protests.html

68 Hanna Kreitem. "The U.N. Calls on States to Stop Shutting Down the Internet." July 11, 2022. https://pulse.internetsociety.org/blog/the-u-n-calls-on-states-to-stop-shutting-down-the-internet

69 James Griffiths. "Internet shutdowns used to be rare. They're increasingly becoming the norm in much of the world." December 21, 2019. https://www.cnn.com/2019/12/21/asia/internet-shutdowns-china-india-censorship-intl-hnk

70 Edward Wong. "Xinjiang, Tense Chinese Region, Adopts Strict Internet Controls." December 10, 2016. https://www.nytimes.com/2016/12/10/world/asia/xinjiang-china-uighur-internet-controls.html

71 Edward Wong. "After Long Ban, Western China Is Back Online." May 14, 2010. https://www.nytimes.com/2010/05/15/world/asia/15china.html

4. The Stakeholders

4.1. The Internet-Based Civil Society That Isn't

Civic empowerment was never a concept accepted by the rulers of China. Since 2013, when the Xi Jinping era began, the concept of civil society joined a long list of liberal values deemed "western views" that the regime saw as competing in an "intense struggle" against its legitimacy. In the ninth such circular distributed in 2013, the "Communique on the Current State of the Ideological Sphere" or the so-called "Document Nine," civil society was listed as one of the concepts threatening the country, along with constitutionalism, market economics, universal values, freedom of the press on the Internet, and reassessments of China's history.

In the document civil society was depicted as follows: "Civil society is a sort of social and political theory originating from the West, it holds that individual rights are supreme in the social sphere, and that the State may not interfere with these. In recent years, the concept of civil society has been dressed up as a political tool by Western anti-China forces, some people in our country also propagate it with ulterior motives. This mainly manifests itself as: using civil society to propagate Western political concepts, stating that establishing civil society in China is a precondition to guarantee individual rights, and is the basis for realizing constitutionalist democracy; seeing civil society as a 'panacea' to move grass-roots social management forward in China, and engaging in all kinds of so-called citizens' activities. The essence of propagating civil society is that it is aimed at eliminating grass roots Party organization leadership and grass roots regimes from grass roots self-governance by the masses, and even opposing them with each other, so as to shape political opposition forces."[72]

This hostile and politicized view on civil society is not new for the CCP, but it has become more extreme under Xi's leadership. The CCP has always been paranoid about the threat to the stability of its regime induced by any group that may be able to rally around a cause, however acceptable its nature or unthreatening it may seem to most people; whether it is about protecting the environment, labor

72 Roger Creemers (translated). "Communique on the Current State of the Ideological Sphere (Document No. 9)." DigiChina. April 23, 2013. https://digichina.stanford.edu/work/communique-on-the-current-state-of-the-ideological-sphere-document-no-9/

rights, patients' rights, sexual or racial equality, poverty, LGBTIQ rights, or even fandoms, the Party always casts a suspicious eye.[73] As a result, the room for civil society to organize itself in the online space in China has shrunk in the past decade.

On the other hand, the Internet itself was built on the premise that it is owned by no one, particularly not by the governments. Yet at the same time the internet is owned by everyone: through multi-stakeholder participation, especially at the level of global Internet governance, with communities working together from the technical sector, civil society, as well as the commercial fields and governments. For more than 15 years, the Internet Governance Forum (IGF), formed under the mandate of the United Nations, has brought together multiple stakeholder groups to deliberate on policy issues, and civil society has always been seen as a critical part of this process.

So, who can represent the Internet-based civil society in China? The Internet Society of China (ISC) claims to be a non-governmental organization with over 1,300 members comprising both individuals and organizations, including "renowned experts," "distinguished scholars," and industry companies and research institutions. It is supported by various government ministries and its current president is a former minister of the MIIT and former chair of China Mobile.[74] The ISC's most notable achievement was to cooperate with the government in issuing and promoting "self-disciplinary regulations," particularly the 2002 Public Pledge on Self-Discipline for the Chinese Internet Industry,[75] with broad and benign aims such as the promotion of Internet use, prevention of cybercrime, fostering healthy industry competition, and avoiding intellectual property violations. But at the same time, the pledge also included more politically oriented calls to refrain from "producing, posting or disseminating pernicious information that may jeopardize state security and disrupt social stability," including "illegal information" or "superstition and obscenity"; otherwise, such materials would be removed.[76] The pledge became especially controversial when a number of U.S. Internet service providers including Google, Microsoft, and Yahoo! signed it in order to obtain permits to enter the Chinese market, further proving the quasi-government nature of the Society.

As such, the group can hardly be seen as a proper non-governmental organization (NGO) or civil society group. It is at best a quasi-governmental organization, and yet the ISC may be the only organization representing China or its users in international forums, such as by hosting sessions in Internet Governance Forums and World Summit on the Information Society (WSIS) Forums that are organized by various United Nations agencies, a role typically taken up by genuine players in civil society from other countries. In other words, one may conclude that true civil society does not really exist in China, and its Internet users do not have any real voice when it comes to the governance of the Internet.

4.2. Chinese Big Tech: Picking Winners

It has always been the policy of China's Internet industry to pick winners by forcing out the foreign market leaders and grooming a small number of domestic players in each domain to dominate instead, thereby making it easier for censors to keep these companies obedient in exchange for expanded market shares. The government still maintains exclusive control over state-owned enterprises in infrastructure and basic telecommunications services. Beyond that, in the service layers, consolidation would take place and winners would be picked.

The Chinese search engine Baidu is estimated to hold an over 75 percent market share today.[77] But when Google was operating in China between 2000 to 2010, the situation was rather different: In 2009, the year before Google quit the Chinese search engine market, it still held over 30 percent of market share.[78]

For Twitter-like microblogging, Fanfou was the first imitation service in China in 2007. It was a "crowd favorite," providing a relatively open environment in which liberal discussion was permitted, but it soon received heavy competition from other imitators from the Internet portal and messaging space, such as Sina Weibo, Sohu Weibo, Netease Weibo, and Tencent Weibo. Being a smaller independent company, Fanfou's service was frequently interrupted in its early days, and in 2009, it was suspended in the aftermath of the Urumqi unrest in Xinjiang[79] for a year before being allowed to resume.[80] Smaller companies such as Fanfou would find it hard to compete because of its lack of resources to hire a multitude of content moderators to comply with government orders to censors. In the end, Sina Weibo was able to consolidate the market, with other major competitors like Sohu, Netease, and Tencent giving way and terminating their services, leaving it easier for the government to deal with just one big incumbent. Today, as of the first quarter of 2022, Sina Weibo reported around 582 million monthly active users and 252 million daily active users.[81]

73 Lawrence Deane. "Will There Be a Civil Society in the Xi Jinping Era? Advocacy and Non-Profit Organising in the New Regime." July 15, 2021. https://madeinchinajournal.com/2021/07/15/will-there-be-a-civil-society-in-the-xi-jinping-era-advocacy-and-non-profit-organising-in-the-new-regime/

74 Internet Society of China, https://www.isc.org.cn/en

75 "Public Pledge of Self-Regulation and Professional Ethics for China Internet Industry." https://govt.chinadaily.com.cn/s/201812/26/WS5c23261f498eb4f01ff253d2/public-pledge-of-self-regulation-and-professional-ethics-for-china-internet-industry.html

76 "Chinese sites agree to censor content." The Guardian. July 16, 2002. https://www.theguardian.com/technology/2002/jul/16/onlinesecurity.internetnews

77 "Top 5 Chinese Search Engines in 2022 [With Market Share]." https://www.adchina.io/top-chinese-search-engines/

78 Joe McDonald. "Google defends shrinking China market share. Google history in China." Associated Press. September 20, 2010. http://ig-legacy.ft.com/content/faf86fbc-0009-11df-8626-00144feabdc0

79 Mark Ward. "China clampdown on tech in Urumqi." BBC. July 6, 2009. http://news.bbc.co.uk/2/hi/technology/8136944.stm

80 "王兴确认饭否域名逐步解封 暂无互动功能." https://tech.sina.com.cn/i/2010-11-11/23354855959.shtml

81 "Average number of daily active users of Weibo Corporation from 1st quarter 2018 to 1st quarter 2022." https://www.statista.com/statistics/1058070/china-sina-weibo-dau/

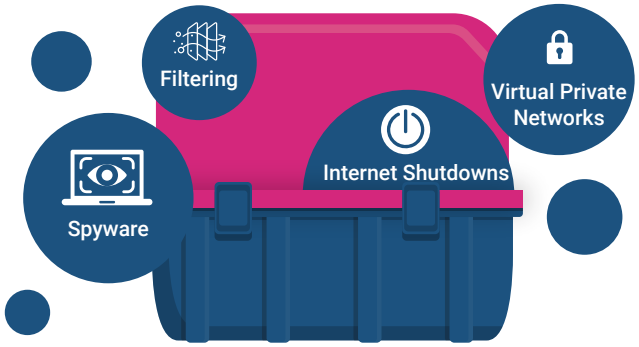
This does not mean that Chinese Internet services are completely void of successful indigenous innovation. Tencent's WeChat is the most notable example. The company was founded in 1998 as a messaging service provider, first with a product called QICQ, later renamed QQ. Its flagship WeChat service today is often called a "super app" that combines instant messaging, social media, mobile commerce, and payment as well as "mini programs" that run on its platform ecosystem. In the first quarter of 2022, WeChat had 1.26 billion active users. While WeChat accounts for close to 20% of the company's total revenues,[82] Tencent has also diversified to become the world's largest online game company.[83] In addition, the company has been investing extensively in several sensitive U.K. technology sectors, including the digital banking leader Monzo.[84] Recently, Tencent even invested in British military software developer Hadean. This is unusual for a company entrenched in Chinese surveillance and censorship, both domestic and overseas.

A year later, in 1999, Alibaba was founded to provide a business-to-business (B2B) e-commerce portal and transaction services, leveraging China's growing status as "the world's factory" to gain domestic and international dominance. Since then, it has diversified into consumer-to-consumer and business-to-consumer e-commerce services, with marketplace platforms Taobao and Tmall respectively, supported by its payment platforms, including AliPay. Its financial technology subsidiary Ant Financial Group also provides online banking and other financial services and operates licensed virtual banks outside China Mainland in Hong Kong and Singapore.

The trend is clear: These market leaders are becoming conglomerates, benefiting from decades of favorable policies and being picked and groomed as winners in one service area first, only to see themselves diversify and dominate in other online sectors horizontally, often competing against and winning over traditional market players, such as the state-owned banks. These Big Tech companies are also going international by offering their own services to overseas users — like AliPay, WeChat, and Weibo for the Chinese diaspora or TikTok for young people all over the world — as well as through acquisition, especially in Southeast Asia, Japan, India, and Europe. The Beijing rulers must feel that they are losing control of tycoons like Alibaba's Jack Ma or Tencent's Pony Ma and their companies.

4.3. Global Big Tech

Journalist and Internet advocate Rebecca McKinnon has called the global Internet companies "the stewards and handmaidens, the tools and enforcers, of China's inner layer of Internet censorship."[85] Without a doubt, a number of foreign companies from the U.S., U.K., and Israel were "credited" by China to have supported the construction of the Golden Shield project and setting up the Great Firewall.[86] In this section, we take a look at the roles played by foreign companies in the early days of the establishment of the GFW, how most of them eventually exited China, and what remains for those who are still around.



4.3.1. Cisco Systems

Over the years, Cisco Systems has received the most criticism for its role in the building of China's GFW. It, along with U.S.-based Juniper Networks, as the two leading Internet router providers at the time, assisted China's backbone operators in upgrading their networks in 2004.[87] Cisco was said to have sold several thousand routers to China and its engineers helped set them up to identify "subversive" keywords in messages.[88] An internal Cisco document from 2002, leaked to the media in 2008, also revealed that the company regarded the Chinese government's "rigid Internet censorship program" as an opportunity to "do more business."[89]

82 Manor Iqbal. "WeChat Revenue and Usage Statistics (2022)." https://www.businessofapps.com/data/wechat-statistics/
83 Lulu Yilun Chen and Yuji Nakamura. "Inside Tencent's Struggle to Bring World's Hottest Game to China." Bloomberg. August 23, 2018. https://www.bloomberg.com/news/articles/2018-08-23/fortnite-tencent-and-the-fate-of-world-s-biggest-game-market#xj4y7vzkg
84 "China's Tencent builds stake in UK digital bank Monzo." Reuters. December 31, 2021. https://www.reuters.com/markets/europe/chinas-tencent-builds-stake-uk-digital-bank-monzo-2021-12-31/
85 Rebecca McKinnon. "Consent of the Networked: the world-wide struggle for Internet freedom." 2012. P. 36.
86 "金盾工程." https://web.archive.org/web/20150416093636/http://www.gdhongan.com:80/industroy.asp?ChannelID=7#
87 Robert McMahon and Isabella Bennett. "U.S. Internet Providers and the 'Great Firewall of China'." Council for Foreign Relations. February 23, 2011. https://www.cfr.org/backgrounder/us-internet-providers-and-great-firewall-china
88 Jonathan Mirsky. "China's tyranny has the best hi-tech help." International Herald Tribune. January 15, 2006. https://www2.kenyon.edu/Depts/Religion/Fac/Adler/Reln270/Internet%20censorship.htm
89 "Cisco Leak: 'Great Firewall' of China Was a Chance to Sell More Routers." Wired. May 20, 2008. https://www.wired.com/2008/05/leaked-cisco-do/

At about the same time, Cisco and a Chinese networking hardware startup, Huawei Technologies, were already embroiled in intellectual property litigations, in which Cisco accused Huawei of stealing its router software codes.[90] Clearly, at that time, Huawei was not capable yet of fulfilling the filtering needs of the Chinese censors on its own, and Cisco was called in to help. The U.S. company might have felt that that was its moment to demonstrate its technical advantages and differentiations to government users in the country with the largest potential Internet population in the world, without realizing yet how disposable it was in the Chinese's eyes.

On the other hand, if Cisco had not jumped at that business opportunity in China then, the development of the GFW would most likely have been delayed or its initial functionalities slimmed down. If the development of the GFW had been delayed by a few years, would that window have provided more time for free expression among Chinese users to take root, or for other foreign companies such as Google and Yahoo! to be under less pressure from government censors at least for a few more years? What difference, if any, would that have made for Internet freedom in China afterwards? We will never know.

4.3.2. Google

It may feel like a long time ago, and the scenario might seem unbelievable, but Google's search engine was actually once a significant player with a sizable market share in China.

Soon after Google was founded in 1999, a Chinese version of its search service was already available, although from China it was occasionally unreachable, and access was slow and unreliable due to interference from the GFW. The company set up its Chinese subsidiary and, in January 2006, launched a localized service, Google.cn, for whose sake Google agreed with the Chinese authorities to block certain websites in exchange for permission to provide its services. In the same year, Google signed the Internet Society of China's Public Pledge on Self-Discipline for the Chinese Internet Industry. (It was the last of the big three U.S. Internet online service providers — along with Microsoft and Yahoo! — to do so.)[91] However, Google promised its users that they would be informed when search results were filtered or censored and that services like Gmail and Blogger, which involved user content or data, would not be offered in Mainland China.[92]

By accommodating Chinese censorship in this way, the company was widely criticized back home in the U.S. for reneging on its supposed corporate motto of "Don't be evil." In the meantime, in September 2007, Google China finally received a license for the Google.cn service that started more than a year and a half ago. But in the ensuing years, Google was also heavily criticized by China for carrying search results linked to pornographic content. Finally, Google was ordered by the authorities to suspend its ability to search foreign websites and its associative-word search function in June 2009. When Google resisted the demand, Google's global site, Google.com, and Gmail were blocked for the first time in China for several hours.[93] Incredible as it may sound now, before then, these Google sites were actually reachable most of the time inside China!

Under pressure from both the U.S. and China, David Drummond, senior vice president of corporate development and chief legal officer of Google, published a blog post titled "A new approach to China" on January 12, 2010. In this post, he alleged that a "highly sophisticated and targeted attack" had occurred that resulted in the theft of intellectual property from Google. He also stated that other large international companies in various sectors including technology, financial, media, and chemical, as well as the accounts of human rights activists, were targeted. Suggesting that the company had always maintained that it would "carefully monitor conditions in China" to decide what to do for its future in the country, Google announced that it would no longer continue censoring its search results on Google.cn, even though it might potentially mean an end to Google.cn and possibly Google's presence in China as well.[94]

Eventually, Google's censorship of its search results ended in March 2010, and all search requests for its Chinese site would be redirected to their Chinese-language site in Hong Kong, which lay outside of the GFW.[95] But in the end, the redirection to Hong Kong was not carried out, and only a static landing page was created for Chinese users with an option to click on a link to the uncensored Hong Kong site. That was of course more symbolic than anything else as the Chinese censors could block the Google.com.hk site as well, which they did.

90 Scott Thurm. "Huawei Admits Copying Code From Cisco in Router Software." The Wall Street Journal. March 24, 2003. https://www.wsj.com/articles/SB10485560675556000

91 "Public Pledge on Self-Discipline for the Chinese Internet Industry." https://en.wikipedia.org/wiki/Public_Pledge_on_Self-Discipline_for_the_Chinese_Internet_Industry

92 More Dickie. "Google to launch censored China service." Financial Times. January 24, 2006. https://www.ft.com/content/0cf3fc52-8d0b-11da-9daf-0000779e2340

93 Kathrin Hille and Richard Waters. "China blocks Google websites." Financial Times. June 24, 2009. https://www.ft.com/content/8e4ccdce-60cf-11de-aa12-00144feabdc0

94 David Drummond. "A new approach to China." Financial Times. January 12, 2010. https://googleblog.blogspot.com/2010/01/new-approach-to-china.html

95 Richard Waters. "Google ends censorship in China." Financial Times. March 22, 2010. https://www.ft.com/content/0081dbd4-35e9-11df-aa43-00144feabdc0

There was an initial outcry from some users who were disappointed about the demise of Google in China, and some Beijing citizens flocked to lay flowers outside Google's office in the Zhongguancun district of the city. The flowers were promptly removed by security guards because permits had to be obtained before flowers could be laid, and so such a memorial was actually deemed an "illegal flower tribute."[96] Even discussions about this illegal activity were censored by other search engines and portals in China, including Google's main rival and chief beneficiary from Google's exit, Baidu.

But has Google learned its lessons? Under the leadership of CEO Sundar Pichai since 2015, the company actually contemplated a return to the Chinese search market in 2018 with an internal project called Dragonfly, designed for the Android and iOS operating systems, to be "compatible" with Chinese censorship requirements. A leaked document revealed that the prototype search engine would require the Chinese user's movement to be tracked along with his or her personal information, IP addresses, and search history and that all the information would be shared with a Chinese partner which would have "unilateral access" to the data.[97]

As a result, a group of Google employees published a signed open letter urging the company to terminate the project.[98] Facing internal and external pressures from its staff as well as opposition from President Donald Trump's administration and the U.S. Congress, the company flip-flopped over its position on the project. After claiming that the project was "effectively ended" in December 2018,[99] there were still rumors that the project was not completely cancelled. Finally, in July 2019, Karan Bhatia, Google's vice president of government affairs and public policy, told the U.S. Senate Judiciary Committee that the project had been terminated.[100]

Why did Google want to make the same mistake twice? Even if a company had only profit in mind and thought that it must pursue the Chinese market, it was extremely simple-minded for corporate executives to expect that any American company could deal with the insatiable demands of the Chinese censors that even the domestic Chinese Big Tech firms can hardly handle, even after giving up board seats to government officials. It was also totally naive for company officers to believe that they could handle the domestic political heat from Washington for "cozying up" to China. These same mistakes were made by U.S. Internet companies less than ten years ago, and the lessons have already been forgotten.

On the other hand, Eric Schmidt, CEO of Google from 2001 to 2011, is now a leading alarmist on China's technological competition with the U.S. Under his reign, Google tried unsuccessfully to carve out a business model in China, and at the time when the Google search service ended in China, he still insisted that the company was "not pulling out of China" and that it had "lots of other business opportunities in China." Today, he is warning of a "national emergency" concerning competition between the U.S. and China over artificial intelligence, research, and talent development.[101]

4.3.3. Yahoo!

Yahoo! entered the China market as early as 1999, setting up an office in Beijing. In 2002, it was the first among the major U.S. Internet companies to sign the Internet Society of China's Public Pledge on Self-Discipline for the Chinese Internet Industry in spite of protests by human rights groups.[102] The search engine service provided by Yahoo! China was actively censored. But more troublesome for the company's reputation and involvement in China would be its provision of email services under the Yahoo.com.cn service. At least four Chinese citizens were arrested and sentenced in China to substantial jail terms because of emails they sent on Yahoo! China's email platform.

The most high-profile of these cases involved Shi Tao, a Chinese journalist, who in April 2004, upon receipt of a CCP document instructing reporters not to report on the upcoming fifteenth anniversary of the "June 4th event," forwarded it to a Chinese-language website in New York using a Yahoo! China email.[103] When so requested by the Chinese police, Yahoo! provided unspecified records relating to Shi's email account and his messages, and the journalist was eventually arrested, charged, and convicted of revealing state secrets. By June 2005, he was sentenced to ten years in prison.

Shi was not alone. Other Chinese Yahoo.com.cn email users sentenced because of messages sent on the platform included Li Zhi, a writer sentenced to eight years in prison in December 2003 for "inciting subversion of the state authority"[104]; Jiang Lijun, a writer sentenced to four years in prison in November 2003 for "subversion"[105]; and Wang Xiaoning, a writer sentenced to ten years in prison in September 2003 for "incitement to subvert state power."[106]

96 Evan Osnos. "China and Google: 'Illegal Flower Tribute'." The New Yorker. January 14, 2010. https://www.newyorker.com/news/evan-osnos/china-and-google-illegal-flower-tribute

97 Ryan Gallagher and Lee Fang. "Google Suppresses Memo Revealing Plans to Closely Track User Searches in China." The Intercept. September 21, 2018. https://theintercept.com/2018/09/21/google-suppresses-memo-revealing-plans-to-closely-track-search-users-in-china/

98 Google Employees Against Dragonfly. "We are Google employees, Google Must Drop Dragonfly." November 27, 2018. https://medium.com/@googlersagainstdragonfly/we-are-google-employees-google-must-drop-dragonfly-4c8a30c5e5eb

99 Jen Copestake. "Google China: Has search firm out Project Dragonfly on hold?" BBC. December 18, 2018. https://www.bbc.com/news/technology-46604085

100 "Google's Project Dragonfly 'terminated' in China." BBC. July 17, 2019. https://www.bbc.com/news/technology-49015516

101 Ina Fried, Margaret Harding McGill, and Ashley Gold. "Eric Schmidt's China alarm." Axios. April 1, 2022. https://www.axios.com/2022/04/01/eric-schmidt-china-alarm-tech-competition

102 "Yahoo! Risks Abusing Rights in China." https://www.hrw.org/legacy/press/2002/08/yahoo080902.htm

103 Joseph Kahn. "Yahoo helped Chinese to prosecute journalist." The New York Times. September 8, 2005. https://www.nytimes.com/2005/09/08/business/worldbusiness/yahoo-helped-chinese-to-prosecute-journalist.html

104 Roland Soong. "The case of Li Zhi." http://www.zonaeuropa.com/20060209_2.htm

105 "Yahoo accused of helping jail another Chinese writer." Reuters. May 19, 2006. https://www.cnet.com/tech/tech-industry/yahoo-accused-of-helping-jail-another-chinese-writer/

106 "Cina dissident Wang jailed on Yahoo information freed." BBC. August 31, 2012.

4.3.4. Apple

Apple is arguably the U.S. Big Tech firm that is most dependent on the Chinese market. In the fourth quarter of 2021, the company's iPhone reached a record 23 percent market share in China, reclaiming the top spot for the first time in six years,[107] overtaking Huawei. More importantly, Apple relies on Chinese contract manufacturing, with analysts estimating that 90 percent of its products are made in China in spite of recent efforts by the company to diversify its supply claims.[108]

Chinese authorities must understand the significance of such dependency of a company that produces the world's most popular smartphones and operating system. They also clearly understand the importance of the data that is saved on these devices and collected by them. In accordance with the country's data sovereignty requirements, Chinese iPhone users accessing Apple's various services over iCloud must store the data within China's borders. So, Apple invested $1 billion to build a data center in Guizhou Province in southwestern China, just to have it operated by its local state-owned partner, Guizhou-Cloud Big Data Industry Co. Ltd. (GCBD), beginning in May 2021. Although Apple claimed that the move would "further improve Chinese users' experience in terms of access speed and service reliability, as well as improve the overall reliability of Apple's products and services on the Chinese mainland,"[109] the reality is that GCBD acts as a middleman for the also state-owned China Telecom by moving user data to the incumbent Internet backbone operator and thus one of the country's main operators of routine censorship.[110]

An investigative report by the New York Times listed a number of key issues related to "how Apple has risked its Chinese customers' data and aided the Chinese government's censorship," summed up as follows: [111]

- Apple stores customer data on Chinese government servers — Chinese state workers physically control and operate the data center. Apple agreed to store the digital keys that unlock the data in China, and it also could not use the encryption technology it uses in other data centers as the Chinese government would not allow it.

- Apple now shares customer data with the Chinese government — U.S. law prohibited Apple from turning over data to the authorities of other countries. But Apple created a legal arrangement with its Chinese state-controlled partner to bypass U.S. restrictions. By making GCBD the legal owner of Chinese customers' iCloud data, Chinese authorities only need to approach GCBD to get those data. Apple is off the hook.

- Apple proactively removes apps inside mainland China to placate Chinese officials — a report from The Times found that "Apple trains its app reviewers and uses special software to inspect apps for any mention of topics Apple has deemed off-limits in China," which amounts to proactive censorship rather than only acting on complaints. The Times estimates that, since 2017, a whopping 55,000 active apps have disappeared from Apple's App Store in China, although most of them remain available in other countries. Over 35,000 of these were games, which must be licensed in China, but the remaining 20,000 include foreign news outlets, gay dating services, encrypted messaging apps, tools that may be used to organize pro-democracy protests, and, of course, VPNs. In July 2017, Apple was reported to have pulled 60 VPNs off the Chinese App Store.[112]

- Apple also proactively removes apps outside mainland China to placate Chinese officials. This means that Apple also self-censors outside the jurisdiction of China's laws. An example is HKmap.live, an app from Hong Kong that appeared during the 2019 anti-extradition bill protests. The app displayed large concentrations of police and would thus, according to its developers, allow protestors and bystanders to avoid rather than confront them. Facing an online outcry against Apple, CEO Tim Cook told the company's employees in a letter that the app "was being used maliciously to target individual officers for violence and to victimize individuals and property where no police are present." But the app's developer responded that Apple was "taking the claims of the Hong Kong police at face value" and the removal was "clearly a political decision to suppress freedom and human rights in Hong Kong."[113] Additionally, Apple apparently simply ignored and never replied to the developer or anyone else, including the author of this paper, who was a Hong Kong legislator at the time.[114]

Apple's self-censorship is probably the most serious as well as the most pervasive among the U.S. Big Tech firms to the point, in some cases, of being rather trivial and even comical. In an October 2019 update to its iOS 13.1 operating system, Apple removed the Taiwanese flag emoji from its virtual keyboard for Hong Kong and Macau users.[115] The Citizen Lab researchers found in August 2021 that there is a long list of 1,045 keywords blocked by Apple's

107 Arjun Kharpal. "Apple reclaims No. 1 spot in China, hits record iPhone market share in the fourth quarter." January 27, 2022. CNBC. https://www.cnbc.com/2022/01/27/apple-china-iphone-maker-hits-record-market-share-claims-nopoint1-spot.html

108 Yang Jie. "Apple Looks to Boost Production Outside China." The Wall Street Journal. May 21, 2022. https://www.wsj.com/articles/apple-looks-to-boost-production-outside-china-11653142077

109 Antony Savvas. "Apple opens its $1b data center in China." May 28, 2021. https://www.capacitymedia.com/article/29otd6mddjpstgh31u1hc/news/apple-opens-its-1bn-data-centre-in-china

110 Nick Statt. "Apple's iCloud partner in China will store user data on servers of state-run telecom." https://www.theverge.com/2018/7/18/17587304/apple-icloud-china-user-data-state-run-telecom-privacy-security

111 Jack Nicas. "Apple's Compromises in China: 5 Takeaways." The New York Times. May 17, 2021. https://www.nytimes.com/2021/05/17/technology/apple-china-privacy-censorship.html

112 "Apple 'pulls 60 VPNs from China's App Store'." BBC. July 31, 2017. https://www.bbc.co.uk/news/technology-40772375

113 Alex Hern. "Tim Cook defends Apple's removal of Hong Kong mapping app." The Guardian. October 10, 2019. https://www.theguardian.com/technology/2019/oct/10/tim-cook-apple-hong-kong-mapping-app-removal

114 https://twitter.com/charlesmok/status/1182336160611201024

115 Matthew De Silva. "Apple bows to China by censoring Taiwan flag emoji." Quartz. October 7, 2019. https://qz.com/1723334/apple-removes-taiwan-flag-emoji-in-hong-kong-macau-in-ios-13-1-1/

engraving service for its AirPod, AirTag, and iPod products in China, 542 in Hong Kong, and even 397 in Taiwan, with many of those terms related to China's political system, names of dissidents and news organizations, and terms about democracy or human rights. As a benchmark comparison, the researchers checked keywords in Japan, Canada, and the U.S.: The numbers are much smaller at 170-206 keywords, mostly owing to racist or sexist epithets. Apple justifies its action as concerning "cultural sensitivities." And, more recently in August 2022, Apple warned its manufacturers and suppliers of Taiwanese-made parts and components that they should only label them as made in "Taiwan, China" or "Chinese Taipei."[116]

4.3.5. It Only Tightens, Never Loosens

Over the years, China has become more sophisticated in managing to make global technology companies their accomplices in censorship. Thanks to China's huge market potential and manufacturing capabilities, companies are attracted to the country's market. The formula of self-justification for presence in China is simply, "we follow local laws" and "China's Internet environment is freer because we stay" — that is, until even these companies are forced to leave. The reality is, after the mid 2010s, most of the major global search engines, social media, messaging, and other online services platforms have been either driven out of China after losing out to competition from Chinese alternatives or, possibly fortunately, never even had a chance to get started there, such as Facebook. Others like Apple have grown overdependent on the country, mainly due to its hardware revenues and manufacturing supply chain.

In addition to a collection of legal regulations to make sure foreign firms will assist in China's censorship, the country also requires that the foreign firm has to seek out a domestic Chinese partner in a joint venture to conduct most services. Otherwise, the foreign company will not receive the required license. These Chinese partners, typically state-owned and tailor-made for the foreign firm, would not only have access to the technology, operations, financial information, and data of the services of these foreign firms, but would even get a share of the money made.

No matter what, China remains successful in convincing western firms looking for a growth market that it is irreplaceable in spite of increasingly harsh market conditions in China, intellectual property thefts, and heavy regulations. Firms must recognize that the increased risks from a much more draconian and riskier Chinese business environment, as well as global tensions with China, will make operating in the country more untenable.[117]

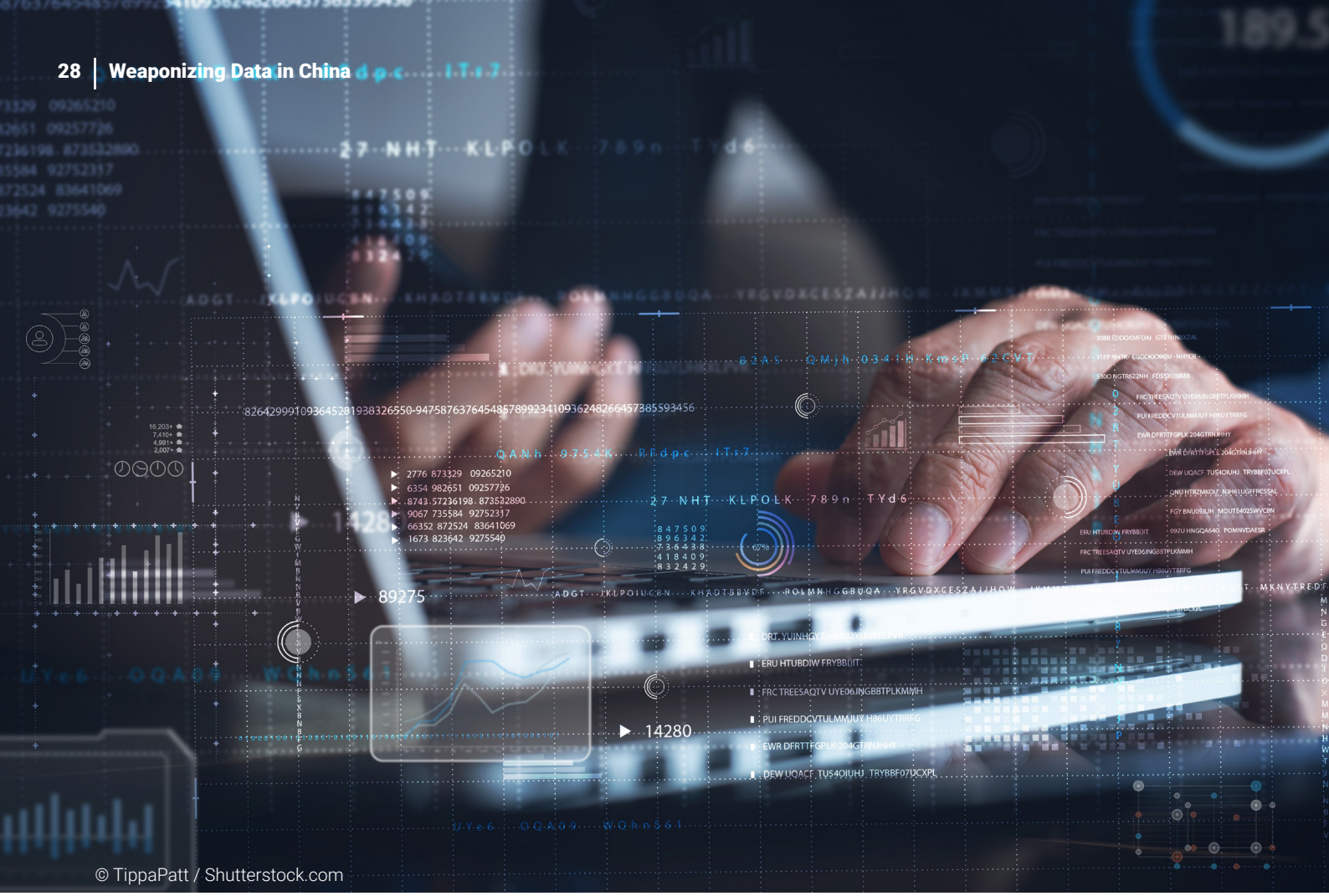
Internal documents in 2022 from Roblox, a major online game platform, disclosed that in order to operate in China, the company must partner with a Chinese company. In Roblox's case this is Tencent, a competitor. The company is also required to host its user data on local Chinese servers. Roblox even expected to be hacked by its partner and have its games reverse-engineered and any code on Chinese servers copied.[118] Despite all these risks that the company probably would not have borne and taken in its home country, it went ahead in China. Roblox's internal document even showed the steps the company was going to take in order to comply with Chinese censorship: They would formally recognize China's claim on Taiwan, avoid names or images of national leaders, and not present any forces or organizations that invade China's territory.

These same mistakes are repeated by different companies, even if these concessions seldom seem to pay off for them in the long run.

116 Cheng Ting-Fang and Lauly Li. "Apple warns suppliers to follow China rules on 'Taiwan' labeling." Nikkei Asia. August 5, 2022. https://asia.nikkei.com/Spotlight/Supply-Chain/Apple-warns-suppliers-to-follow-China-rules-on-Taiwan-labeling

117 Charles Mok and Dennis Kwok. "China's Neo-Nationalism Poses Risks for International Businesses." November 2, 2021. https://thediplomat.com/2021/11/chinas-neo-nationalism-poses-risks-for-international-businesses/

118 Joseph Cox. "Revealed: Documents Show How Roblox Planned to Bend to Chinese Censorship." July 25, 2022. https://www.vice.com/en/article/wxndpx/revealed-documents-show-how-roblox-planned-to-bend-to-chinese-censorship



© TippaPatt / Shutterstock.com

5. Weaponizing Data in China

The CCP sees the Internet and its information flow not only as threats, but also as opportunities. Ever since the term "Big Data" — extremely large data sets that may be analyzed computationally to reveal patterns, trends, and associations[119] — gained prominence, China's government has taken the lead to harness power from data, from collection to analysis to taking actions based on the results of such exercises. From its "advantageous" vantage point as a large-scale censor of information and data on a daily basis, China's rulers understood early on the significance of the huge amount of data collected by its domestic Big Tech players: from the big three conglomerates of "BAT" — Baidu, Alibaba, and Tencent — to other sectoral leaders such as Weibo, JD.com, Didi, Douyin (owner of TikTok), as well as infrastructural players such as the state-owned telecommunications and Internet backbone providers — China Telecom, China Unicom, and China Mobile — and data center platforms such as GDS and 21ViaNet.[120]

Cross-sector services, especially those involving e-commerce and online payment, caught on much more quickly in China than elsewhere, aided by Tencent's super app platform WeChat. Chinese companies started to exploit the promises of big data analytics to customize consumer targeting and customer experience like nowhere else in the world. They had more data to aide their artificial intelligence (AI) and machine learning research than companies in the west because of the relatively loose privacy regulations. Chinese authorities took notice and began to plan how to implement tighter controls.

5.1. Smart City or Surveillance City?

The 2010s saw China's centralized effort to invest in a national drive to develop "smart cities" in order to digitize and "informatize" city management, citing transportation, public services, public safety, education, healthcare, and environmental protection as focus areas for better services and protection for citizens. It became clear rather quickly that Chinese city officials were utilizing technologies — particularly the Internet of Things (IoT), 5G communications, mobile Internet, cloud computing, big data, and AI — for more surveillance purposes and activities. This was also consistent with China's traditional CCP

119 From Oxford Languages. https://languages.oup.com/google-dictionary-en/
120 Herbert Poenisch. "Big Data Management in China." Oxford Business Review. May 11, 2021. https://oxfordbusinessreview.org/big-data-management-in-china/

thought of "mass defense, mass rule" to "crowdsourcing" of volunteers and citizens to monitor the wider public.[121]

However, the local and global information technology industry saw this "smart city" talk as a massive marketing opportunity. Alibaba took leadership in developing its City Brain system, combining surveillance tools, network infrastructure, and AI to provide real-time management for traffic and public transportation management. Its first project was in collaboration with the city of Hangzhou, where Alibaba claimed to have reduced traffic jams by 15 percent.[122] By late 2019, City Brain is said to have been exported to more than 20 cities in mainland China, plus Macau and Kuala Lumpur, Malaysia.[123] Similarly, Huawei has also partnered with a number of Chinese cities, leveraging its 5G technology to provide advance communications for airport and transport controls.[124]

Once again, overseas players did not want to be left out Cisco was particularly aggressive when it signed an agreement with the city of Guangzhou in 2016 to build the Cisco (Guangzhou) Smart City Project in its Panyu district. The agreement included seven areas of cooperation, including smart manufacturing, smart cities, a wireless network, cloud computing, tech company incubation, IT talent training, and innovation leadership development to create "a high-standard system of smart industries, and to build a world-class industrial park with an annual output value of over RMB 100 billion."[125] However, years into the grand development plan of an entire business-residential hi-tech region, Cisco, facing the reality of the economic slowdown of China and the world, especially due to the COVID-19 pandemic, has decided to slow down its global smart city effort by "stopping sales and eventually support" for its related product line.[126]

However, the massive surveillance infrastructure built in the name of traffic management or crime prevention is alive and well in many Chinese cities, and still being expanded. To that extent, the SkyNet project to build the largest surveillance system in the world, combining facial recognition technology with big data and AI to connect as many cameras in public locations, such as train, subway, and bus stations as well as restaurants, shopping malls, and cinemas, was supported by vendors such as HikVision, SenseTi, Huawei, ZTE, and many others. In turn, these companies were rewarded by lucrative state contracts and subsidies.[127]

In 2017, BBC reporter John Sudworth was given "rare access" to the police department of Guiyang, Guizhou Province, to test the CCTV surveillance system of the city. To demonstrate the capability of the system, the police flagged him as a suspect, and he then tried to walk to the train station. He was "caught" within seven minutes. China Daily, the country's state-run English-language mouthpiece, proudly featured the story, with an ending quote from the reporter that made it sound as though he endorsed the system: "If you don't have anything to hide from, there is no need to worry."[128] But if you watch the actual video report,[129] the "quote" was actually a question the reporter posed to a police officer in an interview, as in: "If you have nothing to hide, you have nothing to fear?" Call that fake news from a state media outlet.

5.2. Are COVID-19 Contact Tracing Apps Really Going Away?

When the COVID-19 pandemic first hit China in late 2019 to early 2020, it quickly became the perfect opportunity for China to put digital technology, social credit, and the experience of decades of Internet surveillance and censorship to work. This was not only a beta test for a real-life emergency, but also an experiment to test the bottom line of its citizens' obedience and their degree of acceptance: How many restrictions and how much loss of personal freedom and privacy are the Chinese people willing to accept in exchange for health and public safety?

A series of health apps were central to China's digital response to the pandemic. The apps not only tracked the contacts of infected people but were also used to restrict the movements of everyone during the pandemic. China's high mobile phone penetration enabled the state to make the use of these health apps mandatory. The issue of the digital divide and those people who did not have a mobile smartphone with a data connection or who were elderly, physically handicapped, or unable to comfortably use digital technology was ignored.

In China, the popularity and extremely high penetration rates of two apps, Tencent's WeChat and Ant Group's AliPay, provided the basis for a quick rollout and adoption of the contact tracing apps, health codes, and other health apps in China. For one, real-name registration with national ID numbers was already taken care of when users signed up for these apps. The health code apps developed by local governments, such as provincial or municipal governments, may have different names and features, and policies on restrictions may differ. However, all health

121 Katherine Atha, Jason Callahan, John Chen, Jessica Drun, Ed Francis, Kieran Green, Brian Lafferty, Joe McReynolds, James Mulvenon, Benjamin Rosen, and Emily Walz. "China's Smart City Development." January 2020. https://www.uscc.gov/sites/default/files/China_Smart_Cities_Development.pdf

122 Abigail Beall. "In China, Alibaba's data-hungry AI is controlling (and watching) cities." Wired. May 30, 2018. https://www.wired.co.uk/article/alibaba-city-brain-artificial-intelligence-china-kuala-lumpur

123 "City Brain Now in 23 Cities in Asia." Alibaba Cloud. October 28, 2019. https://www.alibabacloud.com/blog/city-brain-now-in-23-cities-in-asia_595479

124 Alexander Rosas. "What To Know About China's Smart Cities and How They Use AI, 5G, and IoT." The China Guys. August 26, 2021. https://thechinaguys.com/china-smart-cities-development/

125 Hilton Romanski. "Cisco to bring in resources for innovation and digital transformation." September 25, 2017. https://www.newsgd.com/node_2ba302884e/2f-6cd5b7bd.shtml

126 Aaron Tilley. "Cisco Systems Pulls back From Smart City Push." The Wall Street Journal. December 28, 2020. https://www.wsj.com/articles/cisco-turns-off-lights-on-smart-city-push-11609178895

127 "天网工程."China Digital Times.https://chinadigitaltimes.net/space/%E5%A4%A9%E7%BD%91%E5%B7%A5%E7%A8%8B

128 "China's Skynet Project finds people in minutes." China Daily. December 12, 2012. http://www.chinadaily.com.cn/a/201712/12/WS5a2fa4f7a3108bc8c6727f5c.html

129 "In Your Face: China's all-seeing state." BBC. December 10, 2017. https://www.bbc.com/news/av/world-asia-china-42248056

code apps generally contained three color modes: green, yellow, or red, signaling healthy, potential exposure to the virus, and COVID-19 positive, respectively. Facial recognition was often required for registration and usage.[130]

While different provinces or municipalities may have different policies, a green code on the app was required to enter most public venues, a yellow code might have meant seven days of isolation, and a red code would require a more stringent quarantine, such as 14 days in a government facility, as was the case in Hangzhou, Zhejiang Province in February 2020.[131]

Other COVID-19 health apps included a travel history code. This code tracked travel history from data provided by the major state-owned mobile and telecommunications carriers, as well as boarding and travel information from public transportation. It also included data from electronic payment service providers to track potential exposure to suspected or diagnosed patients. And when vaccination became available, the state continued to rely on a comprehensive system of frequent testing and thorough tracking of citizens over time. Vaccination and PCR test records were stored in health apps that received data from the National Health Commission. Often these apps were then further combined with the original health app, as some venues in some locations required proof of vaccination or a negative test result for entry.

While the development of these apps was decentralized and handled by different regional government agencies, coordination was achieved by centralizing the data at the level of the National Government Service Platform, and citizens were able to check or display their health status through at least four channels: an official government website, a State Council app, a mini-program on WeChat, and a mini-program on AliPay. In terms of data privacy, the CAC emphasized from the very beginning, in early February 2020, that the apps and the related data collected would not be used for any other purpose than pandemic control.[132]

But doubts persisted among academics, citizens, and, of course, dissidents: As the use of these health apps became more widespread in China, and the tracking capabilities became more sophisticated, would the Chinese government really not touch this treasure trove of data? A law professor from the leading Tsinghua University raised this very question on her Weibo when Beijing began to consolidate public transportation data into the tracking apps during an earlier wave of the COVID-19 Omicron resurgence in 2022. The professor questioned the practice of combining facial recognition, health code data, and public transportation history as potentially excessive and "detrimental to the protection of public information by linking all kinds of databases without proper laws or regulations." Unsurprisingly, her post was deleted from Weibo in less than 24 hours.[133]

It quickly became clear that concerns about the misuse and abuse of the health codes and apps and the data they contained were well founded. One human rights lawyer complained that a red code appeared on his health app when he was about to travel to Beijing to visit his mother in November 2021 after police officers failed to persuade him not to make the trip.[134] During the 2022 banking crisis in Henan Province, affected bank customers also found red codes in their apps,[135] preventing them from using public transportation, entering public venues, participating in protests, making reports to the police, attending trials related to the issue of their frozen funds from a number of rural banks in the province,[136] or simply leaving their own homes. The incident was the largest to date in terms of potential government abuse of the health code app in China.

With China's COVID-free policy so firmly in place until its sudden reversal after waves of protests erupted in late 2022, it was frankly unthinkable that China would ever roll back this most ubiquitous and effective tracking device they had already put in everyone's pocket. While the government announced the deactivation of some health tracking and contact tracing tools, such as the "mobile itinerary card," the health code scanning system for proving one's COVID-free status was initially still required in a reduced number of places in China.

The sudden reversal of the zero-COVID policy can be seen as either a concession to popular discontent or an inevitable step to save China's failing economy. Either way, the leadership in Beijing must be confident that this surveillance tool has been tried and tested and can be reinstated at any time.

130 Mia Zhong. "China's COVID Apps: A Primer." DigiChina. July 14, 2022. https://digichina.stanford.edu/work/chinas-covid-apps-a-primer/

131 Almond Li. "Explainer: China's Covid-19 health code System." Hong Kong Free Press. July 14, 2022. https://hongkongfp.com/2022/07/13/explainer-chinas-covid-19-health-code-system/

132 "Notice on Protecting Personal Information and Using Big Data to Support Joint Prevention and Joint Control Work." Cyberspace Administration of China. February 9, 2020. https://digichina.stanford.edu/work/translation-chinese-authorities-emphasize-data-privacy-and-big-data-analysis-in-coronavirus-response/

133 https://digichina.stanford.edu/wp-content/uploads/2022/07/Screen-Shot-2022-07-14-at-1.52.49-PM.png

134 https://twitter.com/xieyang911/status/1456741388519804933

135 https://twitter.com/wangcongxh/status/1536978429479747585

136 "China Covid pass system allegedly used to block protest, sparking furious condemnation online." AFP via Hong Kong Free Press. https://hongkongfp.com/2022/06/15/china-covid-pass-system-allegedly-used-to-block-protest-sparking-furious-condemnation-online/

5.3. From Data Security Law to Cyber Sovereignty

As China's censorship regime matures and stabilizes, data is the new focus of attention for the regime as it strives to become a "cyber superpower." In addition to strengthening its domestic and global capabilities to collect and analyze data, the governance of data has become a top national priority. This contrasts greatly with the predominant U.S. or European view on data governance, where the latter has thus far viewed the matter as a market competition issue with the U.S., and the U.S. has until recently shown hardly any interest in the topic at all. And when they do think about this subject, reining in U.S. Big Tech takes centerstage. This should leave China with more room for maneuver to sell its data economy vision to the world, but China has also been preoccupied with cyber and data sovereignty at the same time. Taken together, the two may spell quite the contradiction.

Call it data sovereignty, for which China has started building a legal foundation with the Cybersecurity Law of 2017. This law requires data owners and processors in China to keep their data within China. In September 2021, the Data Security Law (DSL) came into effect and further expanded the scope of the Cyber Security Law. It imposed more controls on global firms operating in China and is applicable to any data that may have anything to do with China or even just passes through China.

The DSL states that the law is "formulated in order to standardize data handling activities, ensure data security, promote data development and use, protect the lawful rights and interests of individuals and organizations, and safeguard national sovereignty, security, and development interests."[137] This is to be achieved by establishing "a system of data classification and obligations for organizations handling data, including security requirements and assessments for its protection, collection, use, and transfer domestically and overseas."[138]

However, uncertainties about data transfer rules remained after the DSL came into effect: What must stay in, what can go out, and what are the procedures for assessment? In July 2022, the highly anticipated Outbound Data Transfer Security Assessment Measures were finally announced by the Cyberspace Administration of China (CAC).[139] The definitions in the previous laws for critical information infrastructure (CII) operators and the requirements for approval had been rather confusing. The new Measures are more detailed, but not necessarily more helpful.

Companies will have to carry out self-evaluations and apply for a CAC assessment in the following cases: if they intend to make important data available abroad, if they are CII operators and would export personal information overseas, or if they handle the personal data of more than one million users and would take that data abroad. But what is considered important data? The Measures define it as data that, "if it is altered, destroyed, leaked, illegally acquired or used, etc., may harm national security, economic operations, social stability, public health or security" — which is a mouthful, but not very helpful.

So, the industry will continue to struggle with such unclear terminology and vague definitions. With little to no enforcement records to refer to, lawyers or analysts can only advise on the side of caution for compliance as the CAC and other Chinese regulators are simply retaining as much discretion as they can. This gives them the most flexibility to trigger compliance procedures when they want to, and politics will continue to shape their decisions.[140]

While on the one hand China establishes its data sovereignty to control sensitive data from flowing out of the country, making it the "most data-restrictive country in the world,"[141] it also wants to harness power from the data. The CCP has consistently proposed making data a "factor of production" alongside the traditional factors of productions like land, labor, capital, and technology. A number of planning documents of the 14th Five Year Plan, such as the ones on National Informatization[142] and Digital Economy,[143] all referred to the importance of developing the governance and standards for optimizing the circulation of "data factors."[144]

But in spite of this intention, China may face huge obstacles in putting their vision into practice. Their plan for data requires vigorous direction from the state over the data economy market, treating data first and foremost as a national asset at the state's discretion. In line with the country's dual circulation strategy to stimulate both the domestic and international marketplaces, China may prioritize domestic circulation first and build cross-border flows and alliances in a tightly controlled manner.[145]

137 "Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021)." DigiChina. June 29, 2021. https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/

138 "China's Evolving Data Governance Regime." U.S.-China Economic and Security Review Commission (CECC). July 26, 2022. https://www.uscc.gov/sites/default/files/2022-07/Chinas_Evolving_Data_Governance_Regime.pdf

139 "Outbound Data Transfer Security Assessment Measures." Cyberspace Administration of China. July 7, 2022. https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-effective-sept-1-2022/

140 "Global companies need to look out for China's new data transfer rules." MERICS China Essentials. July 14, 2022. https://merics.org/en/merics-briefs/data-transfer-rules-g20-exports

141 Nigel Cory and Luke Dascoli. "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them." Information Technology & Innovation Federation. July 19, 2021. https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/

142 Rogier Creemers, Hunter Dorwart, Kevin Neville, Kendra Schaefer, Johanna Costigan, and Graham Webster. "Translation: 14th Five-Year Plan for National Informatization – Dec. 2021." DigiChina. January 24, 2022. https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/

143 "十四五"数字经济发展规划. 中国国务院." December 21, 2021. http://www.gov.cn/zhengce/content/2022-01/12/content_5667817.htm

144 Charles Mok. "The Making of China's Future Internet." Friedrich Naumann Foundation for Freedom. February 18, 2022. https://www.freiheit.org/taiwan/making-chinas-future-internet

145 Rebecca Arcesati. "China activates data in the national interest." MERICS. July 4, 2022. https://merics.org/en/short-analysis/china-activates-data-national-interest#msdynttrid=Z24YXo9vA-OMrEblhl1y4nLwz6rKly3Tt88FbVdCZH0

5.4. What's Next? e-CNY, Blockchain, Metaverse, Web3, and IoT

China's surveillance tech strategy can be forward-looking too. Authorities keep close tabs on the latest trends in digital technology development and will jump in as early as they can to experiment and find a way to dominate.

The Digital Renminbi, or e-CNY, is a shining example of this. This CBDC, central bank digital currency, issued by the People's Bank of China (PBOC), the country's central bank, has already been publicly tested for more than two years, with research having started back in 2014.[146] The publicly stated goals of the PBOC are to combat money laundering, terrorist financing, and other illegal activities and to improve the efficiency of transactions in its financial system. Critics fear that the system will allow the government to snoop on all the financial transactions of citizens and businesses down to the most minute details.

The project conducted a test run at the 2022 Beijing Winter Olympics, although attendance of the event was hampered by COVID-19 restrictions. Nevertheless, with a number of high-profile promotion campaigns in several major cities, over 260 million wallets were issued there, with total transaction values reaching over RMB 87 billion.[147] But e-CNY adoption remains relatively low for a country with over 1.4 billion inhabitants. Those who have downloaded the e-wallets have kept a low balance on their e-CNY account, and the amounts used in transactions remain equally low. This might be because the e-payment service market in China is already dominated by platforms like AliPay and WeChat Pay, which between them have over 80 percent market share.[148] However, with PBOC also playing the role of e-payment regulator for AliPay and WeChat Pay, and with the ongoing "deepening probe" into anti-trust issues in the e-payment sector,[149] it is not inconceivable that very soon the e-CNY service may be further integrated into these payment services. The state might also decide to "nationalize" one or both of these private e-payment services so as to immediately attain the high market adoption and improved technology used for transaction times, throughput, and reliability.

To many people, blockchain may mean more privacy as most cryptocurrencies, like Bitcoin, have adopted distributed ledger technology (DLT) and run on decentralized, permission-less blockchains that are open and trustless and available for anyone to join. But China's dominant, officially endorsed Blockchain-based Service Network (BSN) takes on a centralized nature as a permissioned blockchain. The project is backed by a consortium of Chinese government or state-owned entities, including the State Information Center (SIC) under the powerful National Development and Reform Commission (NDRC), along with China UnionPay and China Mobile, although it is fronted and powered by a Hong Kong-based company, Red Date Technology.[150] As the backbone blockchain infrastructure technology for China between the government, companies, and individuals, BSN will also extend to the Digital Silk Road, China's international project for its Belt and Road partnering countries, for applications to connect over its infrastructure, much like a cloud service.[151] Needless to say, the BSN's centralized and state-owned characteristics will mean that the infrastructure will once again be fully controlled and likely monitored by the government and will therefore not be your average blockchain.

The metaverse is also another buzzword. While the definition of the metaverse can be elusive, broadly it may mean a virtual world that combines aspects of the physical and digital worlds, with the user experience accessed through virtual reality (VR) and augmented reality (AR). Chinese Big Tech firms such as Tencent, Baidu, and Alibaba have made substantial investments in metaverse-related hardware, such as VR headsets or cameras, and software, such as games, live entertainment, and productivity applications. In terms of the state's overall planning for the metaverse, China has already issued a legal consultation for potential regulations on what is called "deep synthesis activities in Internet information services" that would cover virtual reality environments, facial or sound and music generation, etc., to stipulate that, like any other Internet services, they would have to "carry forward the core Socialist value vision, to safeguard national security and the societal public interest,"[152] and work on the basis of other laws such as the CSL, DSL, Internet Information Service Management Measures, and Personal Information Protection Law (PIPL). In other words, the metaverse in China has pretty much been put under regulations before its birth as actual services. In a sense, the metaverse may run different courses in China and the West from the very start, as a "splinterverse."

And in spite of the present economic slowdown in China and the ongoing tech crackdown, regional governments are already racing to incubate metaverse-related businesses in their own locales. Shanghai has proposed plans to build a "$52 billion" metaverse industry and to establish ten innovative companies there by setting up a series of funds and subsidies to attract and support

146 Jonathan Cheng. "China Rolls Out Pilot Test of Digital Currency." The Wall Street Journal. April 20, 2020. https://www.wsj.com/articles/china-rolls-out-pilot-test-of-digital-currency-11587385339

147 Ananya Kumar. "A Report Card on China's Central Bank Digital Currency: the e-CNY." Atlantic Council. March 1, 2022. https://www.atlanticcouncil.org/blogs/econographics/a-report-card-on-chinas-central-bank-digital-currency-the-e-cny/

148 Iori Kawate and Daisuke Maruyama. "China struggles to launch digital yuan after 8 years of trials." Nikkei Asia. July 22, 2022. https://asia.nikkei.com/Business/Markets/Currencies/China-struggles-to-launch-digital-yuan-after-8-years-of-trials

149 Frank Tang. "China to 'deepen' antitrust probe into mobile payment sector despite 'interim progress'." South China Morning Post. September 24, 2021. https://www.scmp.com/economy/china-economy/article/3149985/china-deepen-anti-trust-probe-mobile-payment-sector-despite

150 Arjun Kharpal. "China has been quietly building a blockchain platform. Here's what we know." CNBC. May 15, 2022. https://www.cnbc.com/2022/05/16/china-blockchain-explainer-what-is-bsn-.html

151 Michael Sung. "China's National Blockchain Will Change the World." CoinDesk. April 24, 2020. https://www.coindesk.com/policy/2020/04/24/chinas-national-blockchain-will-change-the-world/

152 Roger Creemers and Graham Webster. "Translation: Internet Information Service Deep Synthesis Management Provisions (Draft for Comment) – Jan. 2022." DigiChina. February 4, 2022. https://digichina.stanford.edu/work/translation-internet-information-service-deep-synthesis-management-provisions-draft-for-comment-jan-2022/

research and development.[153] Beijing's Tongzhou District announced a project to redevelop an old industrial area to set up a 32,000-square-meter metaverse art zone to form a "metaverse-styled virtual ecosystem," and, ironically, for a "virtual project," it will develop offices, co-creation spaces, bookstores, cinemas, etc.[154] Call it metaverse or Web3, the city of Beijing has also announced plans to "cultivate one to two" leading "virtual human" companies with over five billion yuan in turnover and to develop a related governance mechanism. The race to subsidize and pick winners seems to be repeating the old "government formula" for tech development.

Last but not least, there is also the Internet of Things (IoT) — addressable objects or appliances with sensors, processing abilities, and software technologies used to connect and exchange data with other devices over the Internet or other communications networks, usually over Wi-Fi, 5G, or specialized wireless networks. With China as the world's factory, many of the IoT appliances and modules available today are unavoidably made in China, and many such modules have been used in western products by car, computer, electrical, and electronic appliances makers. The U.S. cybersecurity agency, Cybersecurity and Infrastructure Security Agency (CISA), has warned of critical vulnerabilities in Chinese-made GPS-enabled IoT devices installed in cars and motorcycles, as well as risks of data breaches whereby vehicular control might be potentially ceded to hackers.[155]

China will continue to use its centralized policy and technology control model to compete with the West. That is not the model the free world should imitate because it is not one that is conducive to free thinking, creativity, and innovation. But democracies should be always aware about these risks, especially due to their interconnectivity and interdependency with China, and take appropriate measures to protect their infrastructure, investments, institutions, and people.

153 Sergio Goschenko. "Shanghai Aims to Grow a $52 Billion Metaverse Cluster by 2025." Bitcoin.com. July 15, 2022. https://news.bitcoin.com/shanghai-aims-to-grow-a-52-billion-metaverse-cluster-by-2025/

154 Zijing Fu. "Beijing to establish a 32000 square meter metaverse art zone in Tongzhou." Pingwest. https://en.pingwest.com/a/10099

155 Alexi Drew. "Chinese technology in the 'Internet of Things' poses a new threat to the west." August 10, 2022. https://www.ft.com/content/cd81e231-a8d3-4bc0-820a-13f525a76117

6. China's Everywhere Firewall — Transnationalization of Digital Authoritarianism

6.1. Digital Silk Road

China's Digital Silk Road (DSR) initiative started out in 2015 as a part of the Belt and Road Initiative (BRI), the country's global infrastructure investment, development, and diplomatic strategy. The initiative is not well defined and is more commonly used as a branding term for Chinese technology firms entering into sales or business cooperation with customers or partners in BRI countries around the world, often with Chinese investments or financing included in the deals.[156]

Thus far, experts differ as to whether the DSR is a "masterplan by Beijing to deploy its techno-authoritarian model"[157] to BRI countries. Some believe that while facial recognition technology and privacy-invasive cyber infrastructure may indeed be exported to BRI countries, these are more demand-driven than dictated by Beijing, and China's intention may have more to do with supporting the export of its vendors' proprietary technologies to influence global technology standard-setting.[158] But either way, China stands to win.

156 Assessing China's Digital Silk Road Initiative. Council for Foreign Relations. https://www.cfr.org/china-digital-silk-road/

157 Ibid.

158 Robert Greene and Paul Triolo. "Will China Control the Global Internet Via its Digital Silk Road?" Carnegie Endowment for International Peace. May 8, 2020. https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857

To other observers, many of the companies involved in DSR projects are producing dual-use goods for military and industrial purposes, and some of these projects must obviously fall into the category of digital authoritarian tools, such as the "next generation national firewall." Infrastructure buildout projects for BRI countries often include services for active surveillance and data analytics.[159]

Yet all experts agree that China's political influence and policy focus on DSR will only grow. Beijing has a keen interest in leveraging its firms in order to obtain a better competitive position in the BRI countries, especially in areas such as 5G, mobile, cloud, data analytics, AI, and even satellite positioning and navigation. This is also partly seen as a way to counter the technology decoupling effort driven by western countries against China.

In Africa, for example, Chinese companies have made strong inroads into the continent's digital technology markets, with governments such as Tanzania, Cameroon, Kenya, Nigeria, Ethiopia, Guinea, Côte d'Ivoire, and Sierra Leone accepting Chinese state financing for network infrastructure projects serviced primarily by Huawei and ZTE, with funding between US$30 million to US$337 million.[160] Some African nations may be less concerned about the alleged security risks and backdoors posed by Chinese-made network equipment, and some may even welcome surveillance aid. A 2019 investigation by the Wall Street Journal revealed that Huawei technicians indeed assisted government cybersecurity forces in Uganda and Zambia to intercept encrypted communications and social media messages and used cell location data to track political opponents.[161]

In Asia, countries like Pakistan, Laos, Brunei, and Thailand have already adopted BeiDou, China's satellite global positioning system (GPS), and it has also been increasingly adopted in BRI regions such as Central Asia, the Middle East, and Africa.[162] Cambodia's planned "national Internet gateway," which would "facilitate and manage Internet connections to enhance government revenue collection, national security, and preservation of social order, culture, and tradition," is an echo of China's Great Firewall, although its rollout has been delayed.[163] Thailand's military government has also resurrected a failed attempt in 2015 to erect its own Chinese-style national firewall in the name of national security and preventing online crime, restricting access to external online content, and regulating online news.[164] Although these projects may not have been branded under DSR or received direct Chinese financing as some of the African projects have, they certainly belong to a trend of autocratic governments admiring and imitating China's censorship, often based on Chinese technologies. So, it should come as no surprise that the National Cyber Security Agency of Thailand has just signed a memorandum of understanding (MOU) with Huawei to collaborate on developing cybersecurity skills in the country.[165]

Some will surely argue that it is not only Chinese tech firms that provide surveillance technologies to authoritarian states. Cisco did, and so do other companies from Israel and the U.S. It is those governments that want those surveillance and other digital authoritarian tools. But unlike the aforementioned firms, Chinese firms do not have to worry about backlash at home. If this looks like a perfect match of shared illiberal and totalitarian values, democracies cannot just watch from the sidelines and let it continue.

6.2. The Nationalist Public-Private Partnership Hackers

The notion of a Great Firewall often conjures an image of a defensive guard keeping out incoming undesirable content, but as we have seen, it really is much more aggressive than that. Many people have received warnings of potential state-sponsored hacking or phishing attempts on their Google accounts, such as "Government-backed attackers may be trying to steal your password." The company said it sent roughly 50,000 alerts like that by October 2021, a nearly one-third increase from the same time a year ago.[166] Not all of those came from China, with Russian and Iranian hackers sharing the "honor" of conducting the most "notable" campaigns, but Chinese hackers are also not to be ignored.

159 "数字丝绸之路." https://chinadigitaltimes.net/space/%E6%95%B0%E5%AD%97%E4%B8%9D%E7%BB%B8%E4%B9%8B%E8%B7%AF

160 Motolami Agbebi. "China's Digital Silk Road and Africa's Technological Future." Council for Foreign Relations. https://www.cfr.org/sites/default/files/pdf/Chinas%20Digital%20Silk%20Road%20and%20Africas%20Technological%20Future_FINAL.pdf

161 Joe Parkinson, Nicholas Bariyo, and Josh Chin. "Huawei Technicians Helped African Governments Spy on Political Opponents." The Wall Street Journal. August 15, 2019. https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017

162 Richard Ghiasy and Rajeshwari Krishnamurthy. "China's Digital Silk Road and the Global Digital Order." The Diplomat. April 12, 2021. https://thediplomat.com/2021/04/chinas-digital-silk-road-and-the-global-digital-order/

163 Adrian Wan and Charles Mok. "Internet Impact Brief: Cambodia National Internet Gateway." Internet Society. February 18, 2022. https://www.internetsociety.org/resources/2022/internet-impact-brief-cambodia-national-internet-gateway/

164 Joseph O'Connor. "Minister signals a move to resurrect a national internet gateway and stronger online controls." ThaiExaminers.com. February 22, 2022. https://www.thaiexaminer.com/thai-news-foreigners/2022/02/22/minister-resurrects-internet-gateway-scheme/

165 "National Cyber Security Agency signs MoU with Huawei." Bangkok Post. August 3, 2022. https://www.bangkokpost.com/thailand/pr/2360342/national-cyber-security-agency-signs-mou-with-huawei

166 Sergio Gatlan. "Google sent 50,000 warnings of state-sponsored attacks in 2021." Bleeping Computer. October 14, 2021. https://www.bleepingcomputer.com/news/security/google-sent-50-000-warnings-of-state-sponsored-attacks-in-2021/

One early example of such activities was GhostNet, a large-scale cyber-spy operation discovered and named by researchers from the Information Warfare Monitor (IWM) in 2009. It was used to spy on targets from the Dalai Lama to embassies and government offices of many countries around the world, including India, South Korea, Indonesia, Romania, Cyprus, Thailand, Germany, and Pakistan. The hacking network was said to have infiltrated 1,295 computers in 103 countries in 2009.[167] The main trojan horse malware used by GhostNet was Gh0st RAT, which stood for Gh0st Remote Administrative Tool, targeting Windows computers by creating files and executables in their system folders, launching and running the spy programs when the computers were restarted, and setting up backdoors to communicate with the command-and-control servers, which were found to be in China's Hainan Province. The remote "ghost" could watch every keystroke made and access every file created on the infected computers.[168]

It is difficult to be certain about the nature of the Chinese hacking units. Besides efforts directly run by government units, particularly the military, there are also active unofficial units such as the so-called cyber militia and the hacktivist units.[169] Cyber militias are groups comprised of hackers, scientists, network engineers, and foreign language translators, as well as IT companies, and they play an important but ambiguous role outside the military.

Hacktivists, on the other hand, are by far more combative and aggressive. One example is the Red Hacker Alliance, which has been active with hundreds of thousands of hacker members since the early 2000s. It was also cited as the perpetrator in a planned high-profile DDoS attack against CNN.com in April 2008. The group appeared to be self-organized but were tacitly acknowledged by the government. They were mentioned in a news article in April 2005 from China's official news agency Xinhua, where the group was called an "anti-hacking group." The article further boasted that the Alliance's members could "design a computer virus in a few minutes," but they would not do that because their mission was to "protect the Web sites[sic!] from being attacked," especially from foreign countries.[170]

The relationship between the state and the hacktivists can be complicated. Research concerning data between 1990 to early 2012 indicates that, as Chinese hacktivist cyber-attacks became more politically motivated, public, and attributable, the groups also became more closely tied to the Chinese state's disputes and threats with its adversaries, similar to Russian and Iranian hacker groups. It seems clear that China allowed these attacks to help make coercive threats and signals against its adversaries. At the same time, the attackers might be seen as "more nationalist than the state," and could impose a diplomatic cost on China if it were seen to "back down" in a given dispute. In that case, there would be the risk that the hacktivists could turn against their own state or escalate its overseas attacks "out of control" to cause irreversible state-to-state conflict.[171] Although these scenarios have not happened yet, such risks remain, especially for nationalistic issues such as Taiwan, which has become more and more highly charged.

But it was the Chinese military's direct role in overseas Chinese attacks that has been drawing increased attention from western law enforcement. In May 2014, the U.S. Department of Justice announced a grand jury indictment of five officers from the People's Liberation Army Unit 61398 on charges of theft of confidential business secrets and intellectual property from U.S. companies, including Alcoa, Allegheny Technologies, U.S. Steel, Westinghouse, and others, and installing malware on their computers.[172] Their hacker group became known as "APT1," for Advanced Persistent Threat 1.

Then, in June 2015, the United States Office of Personnel Management (OPM) disclosed a data breach of about 22.1 million personnel details and records of government employees, including those who underwent security clearance checks. The incident was particularly sensitive as the identities of numerous intelligence agents were exposed. The hack had been carried out since late 2013, in at least two rounds of attacks. The attackers were widely considered to be state-sponsored hackers working for the Chinese government, and in subsequent years, a number of Chinese nationals were arrested or charged in the U.S. for cyberattacks related to the OPM hacks.[173]

In the immediate aftermath of the revelation of the OPM hack, President Barack Obama announced a "common understanding" with China on cyber espionage in late 2015, when Chinese President Xi Jinping visited the U.S. Their shared understanding was that, while stopping short of refraining from "traditional government-to-government" cyber spying, the two governments would avoid knowingly supporting the cyber theft of corporate secrets or business information. Xi, of course, reiterated that China was a victim of hacking, that the Chinese government had no role in hacking U.S. targets, and that the issue should not be "politicized."[174]

167 "Major cyber spy network uncovered." BBC. March 29, 2009. http://news.bbc.co.uk/1/hi/world/americas/7970471.stm
168 James Griffiths. "The Great Firewall of China." Chapter 13.
169 Mike Raud. "China and Cyber: Attitudes, Strategies, Organization." NATO CCD-COE. August 2016. https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf
170 "China's anti-hacking alliance regrouped." Xinhua and Shenzhen Daily. April 26, 2005. https://web.archive.org/web/20090622160745/http://news.xinhuanet.com/english/2005-04/26/content_2879866.htm
171 Jeffrey Kwong. "State Use of Nationalist Cyber Attacks as Credible Signals in Crisis Bargaining. China and Cybersecurity. Political, Economic, and Strategic Dimensions." Report from Workshops held at UCSD. April 2012. http://www.bdo3c.f-sc.org/archives/921.pdf
172 Jim Finkle, Joseph Menn, and Aruna Viswanatha. "U.S. accuses China of cyber spying on American companies." November 20, 2014. https://www.reuters.com/article/us-cybercrime-usa-china-idUSKCN0J42M520141120
173 Josh Fruhlinger. "The OPM hack explained: Bad security practices meet China's Captain America." CSO. https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html
174 Matt Spetalnick and Michael Martina. "Obama announces 'understanding' with China's Xi on cyber theft but remains wary." September 25, 2015. https://www.reuters.com/article/us-usa-china/obama-announces-understanding-with-chinas-xi-on-cyber-theft-but-remains-wary-idUSKCN0RO2HQ20150926

In those days of somewhat less frigid relations between the U.S. and China, the Xi-Obama cybersecurity agreement was cautiously welcomed, but most observers were skeptical of China's adherence to those loose promises. While initial data by the information security firm FireEye showed that there was a "noticeable decline" in Chinese intrusions against companies and 25 other countries in 2016, it was also possible that the Chinese hacker groups were told to temporarily turn their attention to other targets, such as Russia, as reported by Russian security firm Kaspersky Lab.[175]

The reality, though, is that since 2016, the number of groups named APT — "advanced persistent threat" actors typically supported by a state — has kept increasing. And it is China who has remained a dominant source of these APT groups. In March 2022, six U.S. state governments were hacked by a Chinese group of organized civilian crime syndicates known as APT41,[176] or "Double Dragon." This was done through a vulnerability in a livestock disease-tracking software used in those states.[177] Seven individuals from the group were charged by the U.S. Department of Justice in September 2020, with two of them arrested in Malaysia and the other five remaining fugitives in China.[178]

China's cyberattack capabilities and range are only escalating. One of the latest is another APT group identified as TA418. Its focus is set on attacking targets in Asia and Eastern Europe, including Russia. The group primarily uses Microsoft Office vulnerabilities, allowing the hackers backdoor access to files in the affected computers and sending the stolen data to servers in China, according to Kaspersky Lab.[179]

There are also examples of Chinese hacking that are closely tied to its political and military actions. In the wake of U.S. Speaker of the House Nancy Pelosi's visit to Taiwan, cyber-attacks and disinformation campaigns targeting Taiwan were evidently stepped up, with Taiwanese defense officials noting that "cognitive warfare operations" were started even before China's announcement of military exercises, creating concerns for the emergence of a hybrid warfare model against Taiwan. Most notably, digital signage in 7-Eleven convenience stores around the country and a large railway station in the city of Kaohsiung were hijacked to display protest messages against Pelosi, and the official website of Tsai's Presidential Office was taken down for 20 minutes due to a cyberattack.[180] While such levels of targeted attacks do not appear to be carried out by the Chinese military, they may be examples of the kind of cyber disruptions a large number of Chinese civilian hackers are capable of carrying out.

6.3. China's Global Data Harvest

If China believes that domestically it should create and maintain as many channels of data collection as possible about its people, businesses, organizations, and their activities, this mentality does not stop at its border. So, China's growing exports of its technology products and services have become the perfect avenue to collect more data globally, both in targeted ways as well as indiscriminately.

6.3.1. 5G and Infrastructure: Huawei et al.

In this regard, Huawei has been always at the center of attention, insofar as the accusations are concerned of its equipment containing covert "backdoors" to gather information and data without the knowledge of its customers or users. Part of it was because its equipment, sold to and used by telecommunications and mobile providers all over the world, is highly complex, and backdoors are murky by nature and difficult to prove.

In February 2020, a Wall Street Journal report cited U.S. officials saying that Huawei had secretly preserved ways to access networks secretly. This was done over interfaces maintained on their equipment without the knowledge of their carrier customers. The officials stated that they had been observing the situation for more than a decade but declined to say whether the U.S. had observed the company actually using this access. They also refused to give further details about these backdoors.[181]

This ambiguity has led some to believe that these accusations were only speculative or political in nature, and thus false. Nonetheless, the U.S. has called for the ban of Huawei's equipment in its own networks as well as those of its allies, and a growing list of countries have followed the lead of the U.S., such as Britain, Canada, Australia, and New Zealand. Some have also banned Huawei's main Chinese competitor, ZTE, such as the U.S. and Canada.[182] In November 2022, the Biden administration banned the approval of the purchase of any new telecommunications

175 James Griffiths. "The Great Firewall of China." Chapter 16.
176 APT 41 Group. "FBI Most Wanted." https://www.fbi.gov/wanted/cyber/apt-41-group
177 Garrett O'Brien. "Who is APT41?" The Wire China. July 31, 2022. https://www.thewirechina.com/2022/07/31/who-is-apt41/
178 "Seven International Cyber Defendants, Including 'Apt41' Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally." Department of Justice news release. September 16, 2022. https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer
179 Sergio Gatlan. "Chinese hackers use new Windows malware to backdoor govt, defense orgs." Bleeping Computer. https://www.bleepingcomputer.com/news/security/chinese-hackers-use-new-windows-malware-to-backdoor-govt-defense-orgs/
180 Hsia Hsiao-hwa and Raymond Chung. "China steps up cyberattacks, disinformation campaigns targeting Taiwan." Radio Free Asia. August 8, 2022. https://americanmilitarynews.com/2022/08/china-steps-up-cyberattacks-disinformation-campaigns-targeting-taiwan/
181 Bojan Pancevski. "U.S. Officials Say Huawei Can Covertly Access Telecom Networks." The Wall Street Journal. February 12, 2022. https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256
182 "Canada bans China's Huawei Technologies from 5G networks." Associated Press. May 20, 2002. https://www.npr.org/2022/05/20/1100324929/canada-bans-chinas-huawei-technologies-from-5g-networks

equipment from Huawei, ZTE, and several other Chinese surveillance technology companies because they posed "an unacceptable risk" to U.S. national security.[183]

Much of the concerns from the U.S. and other western nations about Huawei were centered initially on the close ties of the Chinese military to the company and its founder, Ren Zhengfei.[184] And as the company is private and not publicly listed, information about it is even more opaque than many other listed Chinese tech companies. Huawei of course denies these allegations publicly and points to the notion that backdoors for the purposes of "lawful interception" for law enforcement or for maintenance are normal and used only with strict oversight, and that the company has never installed a vulnerability in its network.[185]

But it should be pointed out that the vulnerabilities of a network due to its equipment being misused without the knowledge of the carrier do not just include the presence and use of backdoors. Backbone network equipment for carriers is complex, and typically equipment and technology suppliers will play a role in designing the network architecture and operation details with the carrier customers. They don't just sell standardized hardware: They will acquire a lot of information about the customers' network designs and operations. Such knowledge, if it falls into the wrong hands, may be a reason for concern too, as nations would not want their critical infrastructure's overall design or weakest points be made known to their adversaries.

Even if some countries may ban the purchase of Huawei's equipment, replacing what is already in use is no easy task. It is believed that in the U.S., for example, a large number of rural networks are saddled with old Chinese equipment that the local carriers cannot afford to replace and that, even if they want to replace it, subsidies from the U.S. government have dipped.[186] Dependence on Huawei and other Chinese network technologies by European countries is also significant for its existing 4G infrastructure, if not yet for 5G, not to mention in many other parts of Asia and Africa where Huawei's market share may actually be increasing.

Besides Huawei and ZTE, many other Chinese technology companies have also received attention as being part of China's covert data grab. They fall into several categories: surveillance devices, digital products and service platforms, and social media.

6.3.2. Surveillance-ware: HikVision et al.

Some people call HikVision "the world's biggest surveillance company you've never heard of."[187] Whether it is the biggest or not, its name has become synonymous with its involvement in China's human rights violations in Xinjiang. Its surveillance CCTV video cameras are deployed by police and other authorities all over the world to surveil citizens everywhere, often with facial recognition capabilities. The company has quickly gained notoriety and the list of sanctions it has received from the U.S. and other western countries is surely and rapidly growing.

In October 2021, the U.S. House of Representatives passed the Secure Equipment Act of 2021 to effectively ban imports and sales of all new products from HikVision and another Chinese company, Dahua Technology. Furthermore, it formally required the Federal Communications Commission (FCC) to adopt proposed rulemaking measures that the FCC itself introduced earlier for companies whose products and technologies have been deemed to pose a national security threat.[188] Since March 2021, the products and services of companies including Huawei, ZTE, HikVision, Hytera Communications, Dahua Technology, China Mobile, China Telecom, along with Russian information security company AO Kaspersky Lab, have been placed on the FCC "covered list."[189] According to reports, there are still discussions in Washington about escalating these sanctions, including placing HikVision on the "most wanted" category of Specially Designated Nationals and Blocked Persons (SDN) list.[190]

As is the case with Huawei, part of the concerns with HikVision are its close ties to the Chinese government. The company has transferred 48% of its shares to China Electronics Technology Group Corporation (CETC), making it an effective subsidiary of a state-owned entity. In addition, HikVision's deep involvement in Chinese oppression in Xinjiang, where the company has received at least $275 million in government contracts to build its surveillance network, has certainly made it stand out negatively.

In addition to the U.S., U.K. members of Parliament have also pushed for a ban on the sales and use of HikVision and Duhua equipment in their country, linking the widespread use of these surveillance cameras to the "dystopian surveillance state," as in Xinjiang.[191] Studies by the U.K. group Big Brother Watch found that 73 percent of U.K. councils (district governments), 57 percent of secondary schools, 60 percent of National Health Service trusts, as

183 Diane Bartz and Alexandra Alper. "U.S. bans new Huawei, ZTE equipment sales, citing national security risk." Reuters. November 30, 2022. https://www.reuters.com/business/media-telecom/us-fcc-bans-equipment-sales-imports-zte-huawei-over-national-security-risk-2022-11-25/

184 Kate O'Flaherty. "Huawei Security Scandal: Everything You Need to Know." Forbes. February 26, 2019. https://www.forbes.com/sites/kateoflahertyuk/2019/02/26/huawei-security-scandal-everything-you-need-to-know/?sh=2814f40473a5

185 "What exactly is a backdoor? Here's a quick tutorial." Huawei. https://www.huawei.com/ie/media-center/transform/01/what-is-a-backdoor

186 Jon Heldel. "Why suspected Chinese spy gear remains in America's telecom networks." Politico. https://www.politico.com/news/2022/07/21/us-telecom-companies-huawei-00047045

187 Zeyi Yang. "The world's biggest surveillance company you've never heard of." MIT Technology Review. June 22, 2022. https://www.technologyreview.com/2022/06/22/1054586/HikVision-worlds-biggest-surveillance-company/

188 Joel Griffin. "Congress passes bill banning new FCC equipment authorizations for HikVision, Dahua and others." SecurityInfoWatch.com. October 29, 2021. https://www.securityinfowatch.com/video-surveillance/article/21243600/congress-passes-bill-banning-new-fcc-equipment-authorizations-for-HikVision-dahua-and-others

189 "List of Equipment and Services Covered By Section 2 of The Secure Networks Act." Federal Communications Commission. https://www.fcc.gov/supplychain/coveredlist

190 Demetri Sevastopulo. "US moves towards imposing sanctions on Chinese tech group HikVision." Financial Times. May 3, 2022. https://www.ft.com/content/7bc70335-138e-4f56-afe1-ae4383eefb2b

191 Chris Vallance. "MPs call for UK ban on two Chinese CCTV firms." July 4, 2022. https://www.bbc.com/news/technology-62003253

well as universities, police, and other government departments all use these Chinese wares.[192] Lord David Alton also cautioned about data collection, expressing his concern that data from security cameras in the U.K. might be leaked to other countries.[193] In November 2022, the U.K. government announced a ban on the installation of HikVision's security cameras in any British government buildings and facilities,[194] and the U.S. government also banned any new import of Chinese surveillance equipment from HikVision as well as Dahua Technology and Hytera Communications.[195]

By design or as a bug, backdoors in video cameras from HikVison and other companies are yet another major concern. IPVM, a leading surveillance technology media outlet, has reported on HikVision backdoor exploits since 2017.[196] In 2021, the company itself posted a security advisory about a "command injection vulnerability that could allow threat actors to have complete control of compromised devices," which was discovered by an external cybersecurity researcher.[197] The use of such equipment can certainly put the data collected from the public at a high risk level — it could go directly to Beijing or to other hackers.

6.3.3. Consumer products and services

The category of products and services that may have the capability to collect the most amount of data and redirect such information straight to China must be those consumer products that are in the hands of millions of users worldwide, that is, those they sign into to use and carry out transactions on a daily basis: smartphones from vendors such as Xiaomi and, of course, Huawei and its new brand HONOR, as well as financial, transportation, and other popular platforms, such as AliPay, Didi, and others, that are used all over the world.

As of July 2022, Xiaomi is the third-largest smartphone company in the world by market share at 12.86 percent, only behind Samsung and Apple and ahead of other Chinese rivals Huawei, Oppo, and Vivo. These four Chinese brands combined amount to 28.91 percent of the global market share.[198] Many of these Chinese smartphones are popular in the developing world due to their economical pricing strategy. But Xiaomi has come under fire for its data privacy practice from as early as 2014. At that time, information security firm F-Secure exposed that the company collected data from the cloud address books and messaging services of their users outside mainland China and transferred the data to servers in Beijing without authorization.[199] The company quickly apologized and claimed that it would move the exchange and storage of its international user data outside China.[200] But accusations of unauthorized data transfers continued for Xiaomi.

A report from Forbes in 2020 revealed that browsers on Xiaomi phones were secretly collecting browsing data from users, even if users set them to the private or "incognito" mode.[201] After initially denying the finding as a "misunderstanding," the company promptly provided a browser update to allow users the choice to turn off data collection in incognito mode. However, such data should not have been collected in the first place.[202]

Also, global services platforms such as AliPay and Didi have also expanded rapidly into the global market, both for Chinese travelers overseas and local users in other countries. Since 2017, Didi has expanded its services to Brazil, Mexico, Australia, Japan, Chile, Colombia, Costa Rica, Russia, New Zealand, South Africa, Kazakhstan, and Egypt and has formed strategic partnerships with other companies in Africa and Europe for joint operations. (In 2022, citing market challenges, the company withdrew from Kazakhstan and South Africa.)[203] In some of these countries, Didi's services may not even operate under its own brand, as was the case in Brazil and other Latin American countries, where it operated under the guise of "99."[204]

192 "Who's Watching You? The dominance of Chinese state-owned CCTVs in the UK." Big Brother Watch. February 7, 2022. https://bigbrotherwatch.org.uk/wp-content/uploads/2022/02/Whos-Watching-You_The-dominance-of-Chinese-state-owned-CCTV-in-the-UK-17746.pdf

193 "Eyes everywhere: China's surveillance equipment spreads worldwide." Nikkei Asia. February 16, 2022. https://asia.nikkei.com/Spotlight/The-age-of-Great-China/Eyes-everywhere-China-s-surveillance-equipment-spreads-worldwide

194 Ryan Morrison. "UK government ban for Chinese HikVision CCTV cameras." TechMonitor. November 25, 2022. https://techmonitor.ai/government-computing/HikVision-ban-uk-government-oliver-dowden

195 Diane Bartz and Alexandra Alper. "U.S. bans new Huawei, ZTE equipment sales, citing national security risk." Reuters. November 30, 2022.https://www.reuters.com/business/media-telecom/us-fcc-bans-equipment-sales-imports-zte-huawei-over-national-security-risk-2022-11-25/

196 "HikVision Backdoor Exploit." IPVM. September 3, 2017. https://ipvm.com/reports/hik-exploit

197 Benjamin David. "Cybersecurity Vulnerability Could Affect Millions of HikVision Cameras." September 24, 2021. https://www.infosecurity-magazine.com/news/vulnerability-HikVision-cameras

198 "Mobile Vendor Market Share Worldwide - July 2022." Statcounter GlobeStats. https://gs.statcounter.com/vendor-market-share/mobile/worldwide/

199 Gerry Shih. "China smartphone maker Xiaomi apologizes for unauthorized data access." Reuters. August 11, 2014. https://www.reuters.com/article/us-china-mobilephone-xiaomi/china-smartphone-maker-xiaomi-apologizes-for-unauthorized-data-access-idUKKBN0GB0WY20140811

200 Liam Tung. "Xiaomi moving international user data and cloud services out of Beijing." ZDNet. October 23, 2014. https://www.zdnet.com/article/xiaomi-moving-international-user-data-and-cloud-services-out-of-beijing/

201 "Xiaomi accused of sending 'private' user data to China; company denies claims." The Indian Express. May 3, 2020. https://indianexpress.com/article/technology/mobile-tabs/xiaomi-accused-of-secretly-sending-private-user-data-to-china-6389861/

202 Suzana Dalul. "Is selling your privacy for a cheaper phone really a good idea?" Android Authority. June 4, 2022. https://www.androidauthority.com/xiaomi-privacy-cheap-phone-1118444/

203 https://en.wikipedia.org/wiki/DiDi#Globalization

204 Ingrid Lunden. "Didi confirms it has acquired 99 in Brazil to expand to Latin America." TechCrunch. January 3, 2018. https://techcrunch.com/2018/01/03/didi-confirms-it-has-acquired-99-in-brazil-to-expand-in-latin-america/

When the Cyberspace Administration of China finally punished Didi in July 2021 as part of its final probe, Didi was found to have illegally collected nearly 12 million screenshots and 107 million pieces of passengers' facial recognition data and more than 167 million records of their location data, among other information, since June 2015.[205] These numbers probably concerned only those occurrences within China, and if such infractions were committed inside China, there should be no reason to expect that similar practices did not happen in any of the other countries Didi operated in, especially in markets with weaker privacy protection regimes. While earlier Didi executives did emphasize that the company "stored all domestic user data at servers in China" and that it would be impossible that data would be passed on to the U.S., there were never any formal comments on whether any data would be sent the other way, from outside to inside China.[206]

Experts have also pointed out similar issues with other popular Chinese apps such as AliPay and WeChat Pay, the two leading mobile payment apps used by Chinese residents domestically as well as internationally and increasingly used by foreign users outside China as well. Researchers point out that the owners of these apps, Ant Group and Tencent, are controlled by and cooperate with the Chinese government. They have no choice — companies are required to fully obey the orders of the Chinese government by law. And, according to information provided through Apple's App Store, AliPay and WeChat Pay "over-collect" information from its users, including health and fitness data, location, contacts, user content, and search and browsing history, and more. While this is not unique to Chinese apps, and many apps in the west do the same, there is nothing to stop these Chinese companies from complying with Beijing's request to hand over the collected data. As one legal expert put it simply: "What China is doing is saying, 'if your systems touch Chinese citizens, we have the right to scrutinize your systems.'"[207]

In addition, there are reports of China using its software vulnerability disclosure rules to preview potentially hazardous zero-day flaws in systems for its own intelligence purposes. Current rules in China require companies to report any vulnerabilities they find to the government within two days of discovery and state that companies cannot make such findings public "during major national events."[208] During the Log4j bug incident, an Alibaba engineer who identified the flaw first notified Apache, the global non-profit foundation that maintained the software tool. For that, Alibaba was punished, with the government suspending a cybersecurity partnership with the company.[209] It must be further clarified that in this case, Apache is not even a Chinese or Alibaba's own software: It was a vulnerability in an open-source software from outside China. Nonetheless, the Chinese government considers even this information to be a "secret" owned by China, just because someone in China discovered it.

In the final days of his administration, President Trump ordered Chinese services including AliPay, CamScanner, TikTok, QQ Wallet, SHAREit, Tencent QQ, VMate, WeChat, WeChat Pay, and WPS Office to be banned in the U.S. The executive order was revoked by President Biden when he came into office.[210] Biden's new directive supposedly requires the Commerce Department to review whether apps tied to foreign adversaries pose an "unacceptable risk," with the criteria being whether "it is owned, controlled, or managed by persons that support foreign adversary military or intelligence activities, or are involved in malicious cyber activities, or involve applications that collect sensitive personal data.[211]

While it is true that the Trump order may be more symbolic than practicable in the U.S.'s open Internet environment, more needs to be done than simply rolling back those suggested bans. Many of these applications continue to collect data from people all around the world and in the U.S. every day, and journalists continue to break story after story about such apps, services, or devices collecting and shipping user data to China every day.

6.3.4. Social Media: TikTok

It may be an understatement to say that TikTok has changed the face of social media. The viral short video sharing app — the international version of parent company ByteDance's Chinese app Douyin, launched in 2016 — has taken users and especially the younger generation by storm all over the world in the short time since its launch in 2017. However, a host of problems with TikTok has arisen, such as its toxic addiction, censorship, misogynistic content, discrimination, disinformation — and the list keeps growing.

TikTok's problem for the west is more than it being a "profit-above-all" Big Tech platform. It is, just like our previous examples, a subsidiary of a Chinese firm that is obliged to follow Chinese laws completely, despite TikTok's own assertion that it operates completely independently from its parent company.

205 Zen Soo. "China's Didi Global fined $1.2 billion for data violations." Associated Press. July 21, 2022. https://apnews.com/article/technology-china-data-privacy-cheng-wei-d7c76a253e50d5b5aa8218eb1d3cebbd

206 Scott Murdoch and Yilei Sun. "Didi says it stored all China user and roads data in China." Reuters. July 3, 2021. https://www.reuters.com/world/china/riding-hailing-giant-didi-says-it-stores-all-china-user-data-china-2021-07-03/

207 Elisabeth Braw. "JPMorgan's Deal With Alipay Will Put the PLA in Your Pocket." Foreign Policy. October 12, 2021. https://foreignpolicy.com/2021/10/12/china-jp-morgan-barclaycard-wechat-alipay-data-intelligence-national-security-threat/

208 Suzanne Smalley. "China could be reviewing security bugs before tech companies issue patches, DHS official says." Cyberscoop. August 10, 2022. https://www.cyberscoop.com/dhs-official-chinese-rules-exploit/

209 Zeyi Yang. "Beijing punishes Alibaba for not reporting Log4j loophole fast enough." Protocol. December 22, 2021. https://www.protocol.com/bulletins/alibaba-cloud-log4j

210 Campbell Kwan. "Biden revokes Trump-era executive orders that sought to ban AliPay, TikTok, WeChat." ZDNet. June 9, 2021. https://www.zdnet.com/article/us-president-biden-revokes-trump-era-executive-orders-that-banned-alipay-tiktok-wechat/

211 "Fact Sheet: Executive Order Protecting Americans' Sensitive Data from Foreign Adversaries." The White House. June 9, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/09/fact-sheet-executive-order-protecting-americans-sensitive-data-from-foreign-adversaries/

Documents leaked to the media in 2019 suggested that TikTok instructed its global moderators to censor videos that mentioned political topics sensitive to Beijing, such as the religious group Falun Gong, Tiananmen Square, Tibet, or Xinjiang, with the bulk of the banned content classified under a category internally called "hate speech and religion." Banned materials may be deleted from the site, and the user may be banned from the service, or in cases of lighter violations, the content may be marked as "visible to self," where the content will be left on the site but not fed to other users.[212] But not only that, TikTok censors apparently globally adopted the Chinese censors' sensitivity toward socially controversial issues: Some users have reported that even "black lives matter"-related phrases were flagged as inappropriate.[213]

TikTok also has the same issue as the previously mentioned Chinese apps: excessive data collection and unauthorized transfers. The Australian-U.S. security firm Internet 2.0 reported TikTok's excessive data collection in July 2022, including access to contact lists, calendars, hard drive scanning, and an hourly geolocation check. Also, if a user refuses to give permission to data collection and sharing, TikTok will "persistently" ask again and again until the user gives in. Most of all, the research found that, by using tracked bots, data is consistently being geolocated to unidentified servers in China.[214]

After a public outcry and official enquiry from the country's shadow cyber security minister, James Paterson, TikTok Australia finally admitted that selected staff in China can access Australian users' data "to do their jobs." Paterson pointed out that TikTok Australia has contradicted its own previous assurance that the data would be stored in the U.S. and Singapore, whereas now it turned out to be in China. As other experts also noted, any data held by TikTok in China would be accessible by the Chinese government, according to Chinese law.[215]

By examining their LinkedIn profiles, a 2022 Forbes investigative report also found that hundreds of employees at ByteDance, TikTok's Chinese parent company, had previously worked for China's various state media outlets. These former state media employees now occupy middle to senior roles in ByteDance in content partnership, strategy, policy, monetization, and media cooperation, further fueling concerns that TikTok's users are being exposed to direct manipulation from Beijing.[216]

Despite all these problems, TikTok was among the apps that were spared by the Biden administration in 2021 from Trump's last-ditch attempt to ban them. Similarly, Trump's earlier order in August 2020 for TikTok to be divested to a U.S. owner was also suspended by the incoming Biden administration.[217] Somehow, U.S. lawmakers and the administration seem preoccupied about giving their own American social media and Big Tech firms more of a hard time than Chinese platform players that may present even more serious national security risks.

6.3.5. The U.S. Response: The Clean Network

When the Clean Network initiative was announced by U.S. Secretary of State Mike Pompeo in August 2020, it was described as a measure to address "long-term threats to data privacy, security, human rights, and trusted collaboration." With initial support for the program from leading Democratic congressional leaders, it was bipartisan to a large extent.[218] Most of the public knew of the initiative as keeping Huawei and ZTE gear out of the telecommunications networks in democratic nations, with supposedly more than 60 nations having signed up. But the scheme was designed as much more than just covering 5G backbone and back-end telecom devices.

Indeed, six lines of effort were defined:[219]

(1) Clean Carrier — to ensure that untrusted Chinese carriers are not connected with U.S. telecommunications networks.

(2) Clean Apps — to prevent untrusted Chinese smartphone manufacturers from pre-installing, or otherwise making available for download, trusted apps on their app stores. Trusted apps from the U.S. and other countries should in turn remove their apps from Huawei and other Chinese app stores.

(3) Clean Store — to remove untrusted apps from U.S. mobile app stores. This included two Trump executive orders against TikTok and WeChat that were later revoked by the Biden administration.[220]

212 Alex Hern. "Revealed: how TikTok censors videos that do not please Beijing." The Guardian. September 25, 2019. https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing

213 Abby Ohlheiser. "Welcome to TikTok's endless cycle of censorship and mistakes." MIT Technology Review. July 13, 2021. https://www.technologyreview.com/2021/07/13/1028401/tiktok-censorship-mistakes-glitches-apologies-endless-cycle/

214 Rafqa Touma. "TikTok has been accused of 'aggressive' data harvesting. Is your information at risk?" The Guardian. July 19, 2022. https://www.theguardian.com/technology/2022/jul/19/tiktok-has-been-accused-of-aggressive-data-harvesting-is-your-information-at-risk

215 Jake Evans. "TikTok admits Australian data can be accessed in China, prompting warnings app may be compromised." ABC News. https://www.abc.net.au/news/2022-07-13/tiktok-admits-australian-data-accessible-in-china/101233320

216 Mia Sato. "Go read this report on ByteDance employees with ties to Chinese state media." The Verge. https://www.theverge.com/2022/8/11/23301724/go-read-this-bytedance-tiktok-employees-chinese-state-media-propaganda-connections

217 Natalie Gagliordi. "Oracle, Walmart deal for TikTok shelved indefinitely, reports WSJ." ZDNet. February 10, 2021. https://www.zdnet.com/article/oracle-walmart-deal-for-tiktok-shelved-indefinitely-reports-wsj/

218 Michael Mink. "How the Clean Network Alliance of Democracies Turned the Tide on Huawei in 5G." Life & News. December 2, 2020. https://www.lifeandnews.com/articles/how-the-clean-network-alliance-of-democracies-turned-the-tide-on-huawei-in-5g/

219 "The Clean Network Safeguards America's Assets." U.S. State Department Fact Sheet. August 11, 2020. https://2017-2021.state.gov/the-clean-network-safeguards-americas-assets/index.html

220 Campbell Kwan. "Biden revokes Trump-era executive orders that sought to ban AliPay, TikTok, WeChat." ZDNet. June 9, 2021. https://www.zdnet.com/article/us-president-biden-revokes-trump-era-executive-orders-that-banned-alipay-tiktok-wechat/

(4) Clean Cloud — to prevent U.S. citizens' most sensitive personal information and businesses' most valuable intellectual property from being stored and processed on Chinese clouds such as Alibaba, Baidu, China Mobile, China Telecom, and Tencent.

(5) Clean Cable — to ensure that the underseas cables connecting the U.S. to the rest of the world will not be subverted for intelligence gathering by the PRC "at hyper scale," and that new undersea cables built around the world with foreign partners would exclude untrusted vendors.

(6) Clean Path — to protect the voice and data over 5G networks entering and exiting U.S. diplomatic facilities domestically and abroad by making sure that there is an end-to-end communications path that does not use any transmission, control, computing, or storage equipment from untrusted IT vendors such as Huawei and ZTE. This portion substantiated the original focus on banning Huawei and ZTE from partner nations' 5G networks.

To be sure, some parts of the Clean Network initiative are more successful than others, such as the ban on unsafe network equipment from companies like Huawei in partner countries. But in some cases that was not accomplished without debate and further deliberation. In Germany, for example, there was initially resistance from telecommunications operators as well as the government. This was due to a number of factors, including their dependence on Huawei for the country's previous 4G network systems and the potential high cost of switching. An additional issue was the fact that there was no notable independent German and European debate on the issue, making the effort too akin to being totally American-led. To better prepare, Europe should establish long-term efforts to strengthen and support its own technology suppliers and get an earlier head-start on adopting future open technology standards by cooperating with like-minded partners to reduce its dependency on Chinese vendors.[221]

For the rest of the Clean Network initiative, Clean Cable is simply consistent with U.S. policies that are already in place: Chinese partners have to be excluded from the development of undersea cables that will be connected to the U.S., and cables connecting to the U.S. are forbidden to end in Chinese cities such as Hong Kong.[222] The U.S. authorities can control these decisions through licensing requirements from the FCC and other departments. The effects of these decisions have already been felt: East Asian regional telecommunications and data center hubs are shifting from Hong Kong to other locations, such as the Philippines, Taiwan, Korea, and others, not to mention the existing hubs of Singapore and Japan.[223] These portions of the Clean Network initiative have essentially been preserved by the Biden administration.

On the other hand, Chinese cloud services have never been competitive or widely adopted in the U.S. anyway, so Clean Cloud is easy to achieve. Those Clean Network initiatives that concern large telecommunications companies or large cloud service providers are easier to achieve, but accomplishing the two initiatives relating to apps and app stores has proven more elusive. As mentioned, the Trump executive orders against TikTok and WeChat were difficult to implement in the U.S.'s open market environment. There is also the risk that the orders could be challenged in court if fully implemented. Also, TikTok already has almost 80 million users in the U.S.[224], and WeChat recorded over 1.7 million downloads in 2021 in the U.S.[225] This makes the U.S. the second largest market for the super app behind China. Any effort to forcibly remove these apps from the U.S. market is sure to face strong domestic backlash from users and even advertisers and creators dependent on those apps' ecosystems for income.

If completely banning these apps may not be immediately achievable for the U.S. and other democracies, more targeted regulations to control the misinformation, disinformation, foreign interference, election meddling, and other harms on these platforms must be considered and undertaken with urgency.

Finally, how did China respond to the Clean Network? In September 2020, China actually proposed its own framework to deal with global data security and digital commerce, named "the Global Data Security Initiative (GDSI)." Stressing "multilateralism, secure development, fairness and justice," the initiative broadly defines principles of cooperation concerning data security and cybersecurity. China is using the initiative to garner support to form its own loose alliance on data and technology with friendly countries such as Russia, Tanzania, Pakistan, Ecuador, and some of the members of the Arab League and ASEAN.[226]

221 Thorsten Benner. "Seven Lessons From the German 5G Debate." Global Public Policy Institute. December 30, 2021. https://gppi.net/2021/12/30/seven-lessons-from-the-german-5g-debate

222 Shermaine Yung. "Trans-Pacific Cable Chaos, Shifting Asian Hubs." TeleGeography BLOG. May 20, 2021. https://blog.telegeography.com/trans-pacific-cables-asian-hubs-plcn-status

223 Charles Mok. "Taiwan can be East Asia's new internet and data hub." CommonWealth Magazine. May 5, 2022. https://english.cw.com.tw/article/article.action?id=3219

224 "Number of TikTok users in the United States from 2020 to 2023." Statista. January 28, 2022. https://www.statista.com/statistics/1100836/number-of-us-tiktok-users/

225 "Leading markets of Tencent's WeChat in 2021, based on app downloads." Statista. February 7, 2022. https://www.statista.com/statistics/1287237/tencent-wechat-app-downloads-by-country/

226 Chaeri Park. "Knowledge Base: China's 'Global Data Security Initiative'" (全球数据安全倡议). DigiChina. March 31, 2022. https://digichina.stanford.edu/work/knowledge-base-chinas-global-data-security-initiative/

6.4. Internet Standards and Governance Meet Foreign Policy

6.4.1. Technical Standards Setting: From WAPI to New IP

China understands the importance of influencing global standard setting — firstly, in order to advance its domestic industry in the international market, and secondly, to elevate its scientific and academic research, thereby steering the market in a direction favorable to the country. By doing so, elements of CCP techno-authoritarian control philosophy will also find its way into the global standards.

The Chinese authorities attempted as early as 2003 to try to leverage its domestic market to impose a "Chinese national standard" for wireless LAN (WLAN) to operate on top of the Wi-Fi standards adopted by global standard bodies. Called WAPI, for WLAN Authentication and Privacy Infrastructure, it was originally set to be unilaterally and mandatorily adopted in China by June 1, 2003. The reason given for this decision was that this should deal with a supposed loophole in the WLAN international standard of ISO/IEC 8802-11. In the early days of China just entering the WTO, the issue quickly became one of market access denial for foreign networking firms: In order to produce a separate line of WAPI-compliant products for China's market, foreign companies would most likely have been forced to collaborate with one of the limited numbers of Chinese firms with access to the standard.

In April 2003, the U.S. and China reached an agreement, and China agreed to delay the WAPI requirement indefinitely.[227] The U.S. at the time considered it a successful trade negotiation. Meanwhile, Chinese media were already pointing out that in exchange for the Chinese agreeing to delay WAPI and promising improvements in intellectual property enforcement against piracy, they received in turn a relaxation on the stringent requirements for the export licensing of U.S. high-tech gear to China.[228]

The stalemate over WAPI continued for several years. China submitted its proposal to the ISO standards organization for it to be recognized as an international standard in 2006, but this was rejected. The application was resubmitted in 2009, but in 2011, China withdrew the WAPI application for good.

The WAPI saga was an important lesson for China, namely that its timing was premature. China's market could be a huge leverage, but the country lacked its own leading technology provider with global influence. If the technical standards would have been "splintered" at the time, China would have had more to lose than it had to gain, for example, by putting its emerging domestic technology companies, such as Huawei, at a global competitive disadvantage. China also realized that it must increase its level of participation in global standard-setting bodies to have a larger say in future decisions. China bid its time and would try again.

Fast forward to today. China is now actively proposing two new and related conceptual standards: New IP and IPv6+. In the last decade, China has built up much more experience in participating in the international standards process, gained national allies, and now has its well-endowed corporate giant of an advocate in Huawei.

In September 2019, Huawei submitted a set of proposals to the Telecommunications Standardization Advisory Group (TSAG) of the ITU Telecommunication Standardization Sector (ITU-T) to initiate its "New IP" contribution developed with China Mobile, China Unicom, and the China Academy of Information and Communications Technology (CAICT). In January 2020, Huawei submitted a "New IP" proposal to ITU-T's Focus Group on Technologies for Network 2030, which had been drafting the requirements for a future network with higher throughput, a faster response rate, and higher precision communications demands. New IP claimed to be the solution. In July 2020, Huawei modified its proposal to change the term "New IP" to "Future Vertical Communication Network," with the goal being to "interconnect a multiplicity of vertical networks, each running its own protocol," while the content of the proposals remains the same. ITU-T study groups decided in December 2020 not to adopt the New IP proposal until further determination, but elements of the proposal keep popping up in various other study groups, keeping the effort alive.[229]

The concerns about New IP fall under two aspects: first, as a technology, and second, as a standard-making process. As a technology proposal, the Internet Society (ISOC) — a leading global civil and technology society organization — pointed out that Huawei's New IP proposals made a number of false claims in order to substantiate its premise that there is a need to completely overhaul the existing Internet Protocol (IP) and its architecture. For example, Huawei has claimed that the current networking environment consists of only the Internet, ignoring a wealth of

227 Richard Shim, Michael Kanellos, and Evan Hansen. "China, U.S. strike trade accord." April 21, 2004. https://web.archive.org/web/20050407222112/http://news.zdnet.com/2100-9584_22-5197087.html

228 Charles Mok. "WAPI 內地標準暫緩實行中美貿易爭端得以紓緩." Hong Kong Economic Journal. April 29, 2003. https://charlesmok.blogspot.com/2003/04/wapi.html

229 "Huawei's 'New IP' Proposal - Frequently Asked Questions." Internet Society. February 22, 2022. https://www.internetsociety.org/resources/doc/2022/huaweis-new-ip-proposal-faq/

non-Internet networks that exist and function well. It has also claimed that current network technologies cannot handle heterogeneous networks, which is technically untrue; indeed, the design of the Internet precisely allows for sub-networking, which has been proven to embrace flexible inter-networking. By misdirecting the focus on a particular variant of the transport protocol, TCP, Huawei claims that the Internet cannot handle ultra-high throughput, ignoring the effective and continuous evolution in TCP and IP performance. Another false claim concerned New IP's need for an extremely low latency, which critics ridicule as "incompatible with the laws of physics," leading to overstated claims of speed that, on closer examination of the numbers, would actually exceed the speed of light.[230]

In addition to that unsound technical proposal, industry bodies also point out the key concern about New IP: its lack of compatibility with the existing Internet. New IP unnecessarily aims to revamp the whole Internet rather than take the normal incremental approach. Telecommunications operators have also objected to the suggestion of New IP's proponents that the current designs lack certain capabilities — this is just because some features were not deployed due to a lack of business cases. The redesign of the whole protocol was deemed unnecessary and detrimental to the extent that it may end up splitting up the "new" and "old" Internets.[231]

And there are still more signs pointing to a hidden agenda behind New IP. The Internet Corporation for Assigned Names and Numbers (ICANN) — the multi-stakeholder organization that administers global Internet resources such as domain names — cautions that New IP "advances the idea of a strong regulatory binding between an IP address and a user." If deployed, "pervasive monitoring" — that is, surveillance — will be much easier, allowing any intermediary network device element to have full access to "exactly which user is doing what." Similarly, content providers will also know the identity of everyone who connects to them. In short, the New IP Internet will become a big surveillance machine. Further citing the New IP's incompatibility with the existing IPv4 and IPv6 infrastructures, its deployment will have to take place separately and in parallel, and any significant deployment and interconnection will take decades.[232]

Meanwhile, Huawei and China are also strategically taking the case to the ITU despite the fact that currently ITU jurisdiction does not cover the Internet. Internet technology standards have traditionally been developed in a multi-stakeholder process that involves groups like the Internet Engineering Task Force (IETF), Internet Architecture Board (IAB), Internet Research Task Force (IRTF), World-Wide Web Consortium (W3C), Institute of Electrical and Electronics Engineers (IEEE), and indirectly the Internet Society, which provides support to IETF, IAB, and IRTF, while the multi-stakeholder ICANN would administer the policies and numbering rules. Authoritarian regimes have long wanted to take control of Internet governance away from ICANN and the multiple stakeholders, which comprise industry, civil society, the technical community, academics, consumers, and put all the power in the hands of governments through the ITU, an inter-governmental body under the United Nations.[233]

China believes that the multi-stakeholder approach "should not be lopsided, and any tendency to place sole emphasis on the role of businesses and non-governmental organizations while marginalizing governments should be avoided," as it said in its submission to the 2015 Ten-Year Review of the World Summit on the Information Society, a multi-stakeholder process under the UN and the ITU. China said that ICANN should be "internationalized" — a code-word to express its belief that since ICANN is of American origin, it continues to be "owned by the U.S." — and that the UN should be given a primary role in Internet policy and governance.[234]

This has not been welcomed by the Internet community, as ISOC has made clear: "Internet protocols and their architecture should continue to be developed in an open, multi-stakeholder, and bottom-up fashion — such as those led by the IETF and IEEE — and not driven by top-down processes, as in the ITU-T."[235]

230 Ibid.
231 "ETNO position paper on the New IP proposal." European Telecommunications Network Operators' Association. November 5, 2020. https://www.etno.eu/library/positionpapers/417-new-ip.html
232 Alain Durand. "New IP." ICANN. October 27, 2020. https://www.icann.org/en/system/files/files/octo-017-27oct20-en.pdf
233 Mark Montgomery and Theo Lebryk. "China's Dystopian 'New IP' Plan Shows Need for Renewed US Commitment to Internet Governance." Just Security. April 13, 2021. https://www.justsecurity.org/75741/chinas-dystopian-new-ip-plan-shows-need-for-renewed-us-commitment-to-internet-governance/
234 James Griffiths. "The Great Firewall of China." Chapter 20.
235 Elizabeth Drolet. "Proposals at ITU-T for Internet Evolution Raise Serious Concerns; According to ISOC." NANOG. August 4, 2022. https://www.nanog.org/stories/new-ip-proposals-are-a-threat-according-to-isoc/

To China, the process — to upend the existing Internet standard setting — is obviously as important as the proposal, that is, New IP. If the complete package is not accepted, they break it down into pieces to target specific alternative standards bodies and sub-bodies and alternative audiences that may be more receptive. In May 2022, China and Huawei made a newly modified resolution to introduce IPv6+ as an enhanced version of the latest version of the IP protocol, IPv6. Despite the similarity in functions and philosophies between New IP and IPv6+, Huawei claims that the two are different and that IPv6+ is exactly the kind of natural and incremental extension of IPv6 that standard makers are used to, instead of a new architecture like New IP. Strategically, Huawei made a last-minute resolution at the World Telecommunication Development Conference, the ITU's conference on telecom development, in order to avoid western scrutiny while appealing to the support of developing countries in the global south, which lag behind in IPv6 deployment and may be attracted to IPv6+, considering Huawei's investment and commitment to infrastructure projects in those countries.[236]

China's efforts to redefine the Internet will continue. If it falls short of that goal, China will aim at least to splinter off its own surveillance-state Internet with its autocratic allies, with proxies like Huawei and nation state partners such as Russia, Iran, Cuba, and North Korea. Their hidden agenda is in plain sight: After complaining that the Internet is an American invention and is still controlled by the U.S., they want to take over any role in decision making from the civil, technical, business, and user communities.

And it's not just the Internet. Back in the realm of mobile communications, with discussions over 6G already underway, China "now holds advantageous positions in many aspects of 5G wireless telecoms, providing a strong foundation for further progress," as evidenced by 6G development metrics such as "patent filings and real-world implementations of relevant enabling or precursor technologies."[237] The U.S. and Europe must catch up in the way they prioritize their resources for and focus their policy on 6G, just as they also need to do the same for the future Internet.

China might not have been ready over ten years ago with WAPI, but they believe that they are ready now. China launched its "China Standards 2035" in 2018, and its Standardization Administration and the State Administration for Market Regulation (SAMR) issued a proposal for public comment in 2022. This will cover a wide range of proposed standards that may apply even to personal computers and servers, with huge implications for the market entry of foreign technology providers.[238] It may also cover other more nascent and emerging technologies, such as quantum computing. The message sent by its efforts concerning both domestic and international standard setting is "we own our standards and we don't want you to sell us your products, and we want our standards to be global standards so that we can sell you our products, doing things our way."

6.4.2. Internet Governance and the ITU

When Russian President Vladimir Putin visited Beijing for the opening ceremony of the Beijing Winter Olympics 2022, just a few weeks before his troops brutally invaded Ukraine, he and Chinese President Xi Jinping stood together to offer limitless support to each other. Among Beijing's statements pledging economic, energy, and diplomatic cooperation between the two countries, there was also the promise to support the "internationalization of Internet governance" and "equal rights of countries to regulate the world-wide web." They pledged to "deepen bilateral cooperation in international information security," declared support for an "international convention on countering the use of information technologies for criminal purposes," and advocated greater participation in the ITU.[239]

The two countries do share common values when it comes to the Internet — surveillance, censorship, and total control.[240] At the Beijing Winter Olympics, athletes and journalists could only access the "unobstructed" Internet at designated points or hotels. The mobile app mandated for all participants to obtain event services was found by Citizen Lab researchers to contain so many security flaws that it could act as a trojan horse in everyone's pocket to secretly harness their data.[241]

236 Luca Bertuzzi. "China rebrands proposal on internet governance, targeting developing countries." Euractiv.com. June 5, 2022. https://www.euractiv.com/section/digital/news/china-rebrands-proposal-on-internet-governance-targeting-developing-countries/

237 John Lee and Meia Nouwens. "Strategic Settings for 6G: Pathways for China and the US." IISS. August 12, 2022. https://www.iiss.org/blogs/research-paper/2022/08/strategic-settings-for-6g-pathways-for-china-and-the-us

238 Shunsuke Tabeta. "China takes wider aim at foreign tech with national standards plan." Nikkei Asia. July 6, 2022. https://asia.nikkei.com/Business/Technology/China-takes-wider-aim-at-foreign-tech-with-national-standards-plan

239 "Russia and China call for internationalization of Internet governance — statement." Tass. February 4, 2022. https://tass.com/economy/1398177

240 Charles Mok. "China and Russia Want to Rule the Global Internet." The Diplomat. February 22, 2022. https://thediplomat.com/2022/02/china-and-russia-want-to-rule-the-global-internet/

241 Liza Lin. "Official Beijing 2022 Olympics Mobile App Is Marred by Security Flaws, Researchers Say." The Wall Street Journal. January 19, 2022. https://www.wsj.com/articles/official-beijing-2022-olympics-mobile-app-is-marred-by-security-flaws-researchers-say-11642511957"

But Russia's path to Internet censorship was somewhat different from China's. The country was considerably more open at first, and journalists even commented that "the Internet is the freest area of the media in Russia, where almost all television and many newspapers are under formal or unofficial government control."[242] But gradually, Russian authorities have been taking more censorship measures on the Internet as domestic political unrest has unfolded and external wars have been waged. In 2021, Russian authorities successfully got Apple and Google to remove a voting app from leading dissident Alexei Navalny from their app stores. It also doubled down on its effort to block the use of encryption through the Tor browser and VPN services. Human Rights Watch therefore called 2021 "the year of doubling down on Internet censorship" for Russia.[243]

China's CCP Central Committee and the State Council published the National Standardization Development Outline in November 2021, spelling out its plan for "China Standards 2035."[244] For that, China of course needed the support of Russia to take the "Chinese standards" global, and Russia in turn needed China's support for Rashid Ismailov,[245] Russia's Deputy Minister at the Ministry of Telecom and Mass Communications and the country's candidate at the September 2022 election for the Secretary General of the ITU, running against an American, Doreen Bogdan-Martin, director of ITU's Telecommunication Development Bureau.[246] The election was a showdown for the future governance of telecommunications and Internet standards, and eventually Bogdan-Martin was elected [247] by a wide margin of 139 to 25 votes.[248]

6.4.3. Two Futures of the Internet?

On December 9 and 10, 2021, the first Summit for Democracy was held by the White House, bringing together hundreds of governments and civil society and business leaders "to discuss the challenges and opportunities facing democracies in the 21st century." Due to the ongoing COVID-19 pandemic, the event was really a big webinar rather than a physical gathering. As the State Department was coming up with the event program in the months prior, one of the items was supposed to be the formation of a coalition of democracies around a vision for a free and open Internet. Dubbed the Alliance for the Future of the Internet, it was spearheaded by Peter Harrell, senior director for international economics and competitiveness on the National Security Council, and Tim Wu, special assistant to the president for technology and competition policy.

But the plan was met with considerable skepticism and backlash, especially from civil society and digital rights advocates. For one, the alliance was intended to commit a group of "like-minded countries" to make specific commitments in cybersecurity, privacy, data transfer, and other matters, overlapping with sensitive policy areas from national security to trade. But there were also concerns that the effort would sideline the focus on democratic values, Internet freedom, and human rights and be "reduced" to a mere "no-China club."[250] Some non-governmental groups were concerned that by consolidating the "free world," the alliance would further fragment the Internet, thereby distancing it from those Internet users in authoritarian countries rather than protecting it. At the last minute, the launch of the alliance was postponed.[251]

Four months later, the alliance was finally converted into a declaration when the White House announced a Declaration for the Future of the Internet on April 28, 2022, signed by the U.S. and 60 global partners. The signatories were labelled "partners" rather than countries, most likely in order to accommodate the important inclusion of Taiwan. The White House proclaimed the declaration a political commitment among the partners to "reaffirm and recommit" to "a single global Internet — one that is truly open and fosters competition, privacy, and respect for human rights,"[252] with principles including the protection of human rights and fundamental freedoms for all, advancing the free flow of information, inclusive and affordable connectivity for all, promoting trust in global digital ecosystems through privacy protection, and protecting and strengthening the "multi-stakeholder approach to governance."[253]

242 Russian prosecutors eye Internet censorship." Agence France-Presse. April 23, 2008. https://archive.ph/20140727020225/http://newsinfo.inquirer.net/breaking-news/infotech/view/20080423-132253/Russian-prosecutors-eye-Internet-censorship#selection-2971.0-2971.154

243 "Russia: Year of Doubling Down on Internet Censorship." Human Rights Watch. December 24, 2021. https://www.hrw.org/news/2021/12/24/russia-year-doubling-down-internet-censorship

244 Patrick Lazada, Tim Ruhlig, and Helen Toner. "Chinese Involvement in International Technical Standards: A DigiChina Forum." December 6, 2021. https://digichina.stanford.edu/work/chinese-involvement-in-international-technical-standards-a-digichina-forum/

245 Rashid Ismailov. "Bio." ITU. https://www.itu.int/en/council/2018/Pages/chairman.aspx

246 Fiona Alexander. "Behind the Race to Run the UN's Internet Agency." CEPA. July 14, 2022. https://cepa.org/behind-the-race-to-run-the-uns-internet-agency/

247 "Member states elect Doreen Bogdan-Martin as ITU Secretary General." ITU Press Release. September 29, 2022. https://www.itu.int/en/mediacentre/Pages/PR-2022-09-29-ITU-SG-elected-Doreen-Bogdan-Martin.aspx

248 ITU Election Results. https://pp22.itu.int/en/elections/elections-results/

249 "Summit for Democracy: Year of Action." Fact Sheet, U.S. Department of State. March 9, 2022. https://www.state.gov/summit-for-democracy-year-of-action-fact-sheet/

250 Issie Lapowsky. "Inside the scramble to fix Biden's plan for the future of the internet." Protocol. December 4, 2021. https://www.protocol.com/policy/white-house-alliance-future-internet

251 Issie Lapowsky. "White House delays Alliance for the Future of the Internet launch." Protocol. December 6, 2021. https://www.protocol.com/white-house-delays-alliance

252 "Fact Sheet: United States and 60 Global Partners Launch Declaration for the Future of the Internet." The White House. April 28, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/28/fact-sheet-united-states-and-60-global-partners-launch-declaration-for-the-future-of-the-internet/

253 "A Declaration for the Future of the Internet." The White House. April 28, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf

Clearly, though without explicitly mentioning China and Russia, the declaration squarely addresses the key challenges brought up by their digital authoritarian Internet model and their undermining of the multi-stakeholder Internet governance model in practice. In response to earlier criticism that it duplicates the efforts of civil society, inter-governmental, and other multi-stakeholder forums,[254] the declaration acknowledges values such as multi-stakeholderism and promises to "contribute" to efforts and organizations such as the ICANN, Internet Governance Forum (IGF), and Freedom Online Coalition (a grouping of 34 governments that "work together to support Internet freedom and protect fundamental human rights — free expression, association, assembly, and privacy online — worldwide").[255]

However, initial expectations for the declaration were uncertain. After all, what started out with the hope of a tight alliance ended up being, at least in the beginning, just a declaration. While some analysts think that this is better than nothing, with the U.S. administration showing interest in Internet governance as a part of foreign policy, the initiative must be followed through with "hard conversations" to "push back on digital transgressions." That remains to be seen. Moreover, for some signatories, which may be relatively marginal on the democratic scale, the declaration can be a diplomatic reminder to resist falling further into digital authoritarianism.[256] On the other hand, there are also notable absences among signatories for the declaration, such as important Asian Internet economies like India, Singapore, and South Korea, likely opting out due to their own tendency toward Internet control as well as geopolitical sensitivities in relation to China.

For Beijing, maybe the only logical and quickly achievable response would be to form China's own club. Since 2014, the Cyberspace Administration of China has organized its premier annual Internet event, World Internet Conference, in the eastern city of Wuzhen. In that first gathering, attendees reported receiving a draft of a manifesto from an unidentified source "slid under their hotel doors at midnight," causing many to object to the way it was handled. Eventually, the declaration was not mentioned at the close of the conference.[257] Just as the U.S.'s first attempt to form an alliance was postponed and ended up as a declaration, China's initial try at a declaration failed too.

The next year, in December 2015, in the second World Internet Conference (WIC), Xi Jinping gave a speech to outline his vision for "dialogue and cooperation on the basis of mutual respect and trust," and promoting the transformation of the global Internet governance system." Such transformation should be based on "respect for cyber sovereignty,"[258] and the new "international cyberspace governance" should not be "unilateral" or have "one party calling all the shots."[259] These visions echoed the failed declaration of a year ago.

So, what could be better now than to use the existing platform of the World Internet Conference to form an alliance to counter the American-led declaration? And if the U.S. was not able to form an alliance with its "partners" yet, why not beat them to it? China did just that. In July 2022, the World Internet Conference was "transformed" into an "international organization" made up of "founding members, including "institutions, organizations, businesses, and individuals from nearly 20 countries."[260] Xi made a video speech to an inaugural conference to congratulate the new group's formation as contributing "wisdom and power to global Internet governance development" for a "fair and reasonable, open and tolerant, safe and stable, and vibrant network space." [261]

Who are the members of the new "World Internet Conference" organization? It is said to include an unidentified list of "world-renowned leading Internet enterprises, authoritative industry organizations, and Internet Hall of Famers."[262] Whether the non-disclosure was due to secrecy or bluff, China could at least claim to have formed its club before the U.S. could. In the World Internet Conference 2022 itself, held in a rather low-profiled way in November, little updates were given about the WIC's organization. Nonetheless, democracies must remain vigilant about what the WIC will be up to next.[263]

254 "Empty Promises? Declaration for Future of the Internet is nice on paper." AccessNow. April 28, 2022. https://www.accessnow.org/declaration-for-future-internet/

255 "Aims and Priorities." Freedom Online Coalition. https://freedomonlinecoalition.com/aims-and-priorities/

256 Alex Engler. "The Declaration for the Future of the Internet is for wavering democracies, not China and Russia." May 9, 2022. https://www.accessnow.org/declaration-for-future-internet/

257 "China Delivers Midnight Internet Declaration — Offline." The Wall Street Journal. November 21, 2014. https://www.wsj.com/articles/BL-CJB-24963

258 "China internet: Xi Jinping calls for 'cyber sovereignty'." BBC. December 16, 2015. https://www.bbc.com/news/world-asia-china-35109453

259 Veni Markovski and Alexey Trepykhalin. "Country Focus Report: China Internet-Related Policy Initiatives and Laws." ICANN. January 31, 2022. https://itp.cdn.icann.org/en/files/government-engagement-ge/ge-010-31jan22-en.pdf

260 Jiaxing Li. "China's World Internet Conference goes 'international' as Beijing seeks to promote its own vision of global cyberspace." South China Morning Post. July 13, 3022. https://www.scmp.com/tech/big-tech/article/3185151/chinas-world-internet-conference-goes-international-beijing-seeks

261 "世界互聯網大會成立大會舉行." 人民網. July 13, 2022. http://cpc.people.com.cn/BIG5/n1/2022/0713/c64094-32473662.html

262 "世界互联网大会成立." 中国经济周刊. July 13, 2022. https://www.163.com/dy/article/HC587ONF0530I1ON.html

263 Justin Sherman. "China's New Organization Could Threaten the Global Internet." Slate. July 29, 2022. https://slate.com/technology/2022/07/china-world-internet-conference-organization-standards.html

7. A Call for a Competitive-Minded Response

In summary, China's Internet policy has grown from absolute internal control to the export of digital authoritarianism. This has been achieved by perfecting its legal and governance model of censorship and control and through technological competition and a renewed focus on its model of a surveillance data economy. In so doing, China is seeking global dominance over the Western model of liberal democracy that originally developed the Internet.

So, what can democracies do to compete?

Twenty years ago, democracies were overly optimistic about what the Internet would mean for society at home and abroad. We are learning, sometimes the hard way, and do not need to be overly pessimistic about the Internet and technology. But we do need to learn where we have failed, what we need to preserve, and what we need to change.

It's not that democracies have been unaware of the techno-autocratic potential of the Internet or that authoritarian governments around the world have curtailed freedom of expression and the free flow of information. In 2006, U.S. Secretary of State Condoleezza Rice established the Global Internet Freedom Task Force (GIFT) to develop a robust global Internet strategy to monitor and respond to threats to Internet freedom and to advance the frontiers of Internet freedom by expanding access to the Internet through coordination with various government agencies and the technology industry.[264]

On January 21, 2010, the then U.S. Secretary of State Hillary Rodham Clinton spoke on Internet freedom in the Newseum in Washington, D.C.,[265] right when American companies were accused of assisting censorship abroad, including in China. As part of the actions outlined in her speech, the Global Internet Freedom Task Force from the previous administration was reactivated as a forum for addressing Internet freedom around the world. There was to be more cooperation with U.S. tech players, including

264 "Global Internet Freedom Task Force." U.S. Department of State archive. https://2001-2009.state.gov/g/drl/lbr/c26696.htm#:~:text=Secretary%20of%20State%20Condoleezza%20Rice,of%20information%20on%20the%20Internet.

265 Hillary Rodham Clinton. "Remarks on Internet Freedom." U.S. Department of State archive. January 21, 2010. https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm

via non-governmental industry organizations such as the Global Network Initiative (GNI), and more government funding was proposed to help support the development of anti-circumvention tools and other Internet freedom efforts around the world.

After the Bush and Obama administrations, it wasn't until the end of the Trump administration that Internet freedom issues were back on the agenda, namely when the Clean Network was rolled out. The difference, by then, was that the Trump initiative was all about sanctions — after all these years, Chinese technological influence on the world had grown tremendously. Unlike when Secretaries Rice and Clinton were talking mostly about censorship limiting the freedom of expression for people in autocratic countries, by 2020, China and its technology companies were exporting their technology, along with their philosophy and hidden agenda of surveillance, to private and public customers around the world. Many companies, even in Europe and North America, had become highly dependent on them.

One thing that has been lacking in the last twenty years of global Internet policy has been continuity in U.S. policy. Another thing that this policy has tended to lack is action and coordination with either the private sector or other democracies. The Biden administration's Alliance for the Future of the Internet proposal should have been an attempt to address some of these issues, but it still seems difficult to make the issue of global Internet governance and leadership a diplomatic priority among the many pressing foreign policy problems facing democracies in the world today.

Meanwhile, Europe hasn't been able to take the lead in the fight for global Internet freedom and against growing techno-autocracy: The leading nations of the European Union have been more focused on combating U.S. Big Tech dominance and even on grabbing dividends from China's growing market. To its credit, Europe filled the data and privacy governance gap by taking the lead with the General Data Protection Regulation (GDPR). The GDPR has even served as a model for the Chinese government. At the same time, China has borrowed concepts and provisions from the GDPR, such as extraterritoriality, as well as from U.S. laws such as the Cloud Act, which regulates companies providing electronic communications and remote computer services in the United States, and used them in its own draconian way.

Certainly, the view of the Internet was once overly rosy and somewhat naive. But democratic governments and their lawmakers today may also be too obsessively focused on only the "dark side" of the Internet and therefore succumb to simplistic solutions that may be equally naive and unhelpful, such as regulating tech companies "just like utilities."[266] Some may even look at the tidal wave of Chinese tech crackdowns and think that maybe the Chinese are doing something right, like "balancing government control, economic growth, and innovation." Nothing could be more wrong.[267]

Precisely because the Internet is global, democracies must view a healthy Internet and its freedom as a global issue. Keeping the Internet global, as one Internet without fragmentation, is a crucial part of the fight for a better future Internet. If one part of it fails, other parts of it are at risk of becoming less free, less open, less safe, less secure, and less resilient. That is also why we must guard steadfastly against efforts to splinter the net from China and other countries that share its authoritarian values.

Laws in democratic countries can affect other countries too. Take Germany's NetzDG as an example. Fighting fake news, hate speech, disinformation, and misinformation online is the right thing to do. But by requiring platforms to quickly remove content based on government requests, it sets a precedent for censorship that autocrats will be only too happy to follow. While it may be argued that these autocratic countries can do it on their own anyway, they can now proudly justify themselves by saying that "democratic countries did it first." Democracies will lose any remaining moral high ground if they resort to the same censorship and surveillance tactics as authoritarians.

Yet we see this happening again and again in controversial laws proposed in Australia, the EU, the US, the UK, Canada, one after another, demanding backdoors for Internet companies and platforms, just as China has done. The surveillance tactics now being used in some U.S. states to track down "abortion criminals" are strikingly similar to those used in authoritarian countries. In fact, China can now confidently say, "See, we were right after all, even you have to learn to do it just like us." That is why it is so important for democracies to get their own houses in order.

266 Lauren Feiner. "Justice Thomas suggests regulating tech platforms like utilities." CNBC. https://www.cnbc.com/2021/04/05/justice-thomas-suggests-regulating-tech-platforms-like-utilities.html

267 Matt Perault. "Internet Freedom 10 Years In." Lawfare. January 21, 2020. https://www.lawfareblog.com/internet-freedom-10-years

The U.S. Congress passed the CHIPS and Science Act[268] to strengthen U.S. scientific research and advanced manufacturing capabilities to compete with China, recognizing that the country's technological lead in areas such as semiconductors, artificial intelligence, quantum computing, and robotics was shrinking and that the resilience of the chip supply chain was deteriorating. With the same mindset, a similar policy focus and priority must be placed on the Internet for the free world to compete with China and Russia.

People can argue about how many years the U.S. or Taiwan may still be ahead of China in semiconductor design, fabrication, and manufacturing. But in Internet and communications technology, China has already caught up or even taken the lead in some areas. So, the situation is arguably more dire for the Internet. The splinter Internet threat is equivalent to the semiconductor supply chain problems, or worse: Supply chain problems can sometimes be fixed and reversed by market changes, but the Internet has already been fractured for decades by efforts like China's Great Firewall, with information and services completely shut out for long periods of time. Such disruption of the Internet's "supply chain" may be much harder to reverse. And somehow, we accept China's censorship as a norm. This should not be the case.

In closing, possible components of a competitive-minded response against digital authoritarianism are proposed as follows:

1. Democratic governments should **resist the urge to pursue cyber sovereignty.** Before instituting any cyber laws, **a global impact assessment** should be conducted to consider any negative side effects of potentially fostering digital authoritarianism in other countries that would harm global Internet freedom. As is the case with climate change, a bad local law can affect the whole world.

2. Protect the lead in the data economy by urgently **establishing global privacy and data exchange rules** and regulatory norms for the Internet in the free democratic world. This can be jumpstarted by, for example, expediting negotiations between Europe and the U.S., the APEC, etc.

3. **Firmly support and adopt a multi-stakeholder model for Internet governance** while enhancing the participation of civil society globally in the current and emerging organizations and forums for policy discussion and creation.

4. **Increase participation and leadership in standard-setting and Internet governance organizations** to safeguard the values of open technology and free Internet against influences from autocratic countries attempting to take over those processes and organizations.

5. **Invest in the research and development of privacy-preserving, anti-censorship, and anti-surveillance technology** and the deployment of such technology while developing next-generation information services to overcome censorship.

6. The private sector should **adopt and commit to the principle of an open Internet and privacy by design** for all products and services, for use anywhere in the world. Tech companies should also be trained to understand the impact of their products and innovations on national security and defense.[269]

7. **Counter autocratic countries' efforts to transnationalize their digital repression** by expanding targeted sanctions and regulatory actions against surveillance platforms and technologies from authoritarian countries that effectively operate on their behalf.

8. **Empower global Internet users** through education, training, and development support, especially in underdeveloped nations and underprivileged communities by supporting digital rights and freedom of online expression.

268 "The CHIPS and Science Act." U.S. House of Representatives. https://science.house.gov/chipsandscienceact

269 Elisabeth Braw. "Tech experts need defence training for NATO's race against China." Financial Times. July 26, 2022. https://www.ft.com/content/4cc97d-cc-d02e-4ae6-a4e7-d2fafffc5d26

About the Author

Charles Mok is currently a Visiting Scholar at the Global Digital Policy Incubator, Cyber Policy Center, Stanford University, where his research focuses on digital authoritarianism and cyber policies in Asia-Pacific. He is also a member of the Board of Trustees of the Internet Society and the founder of Tech for Good Asia, a regional initiative harnessing the positive powers of digital technologies. During 2012-2020, Charles served as a member of the Legislative Council in Hong Kong, representing the Information Technology Functional Constituency, where he championed issues such as information freedom, privacy, cybersecurity, and innovation, as well as human rights and democracy.

Before his political career, Charles co-founded HKNet, one of the earliest ISPs in Hong Kong, in 1994, and also co-founded and chaired the Internet Society Hong Kong and the Hong Kong Internet Service Providers Association. He also served as President of the Hong Kong Information Technology Federation. Charles was also a former chair of the Asian, Australasian, and Pacific Islands Regional At-Large Organization (APRALO) of ICANN.

Charles holds a BS in Computer and Electrical Engineering and an MS in Electrical Engineering from Purdue University and was honored as a recipient of the 2022 Outstanding Electrical and Computer Engineer award from Purdue's Elmore Family School of Electrical and Computer Engineering.