Censorship Practices of the People’s Republic of China

Kieran Green, Andrew Sprott, Ed Francis, Dr. Brian Lafferty, Hartley Wise, Molly Henry, Grace Faerber, and Frank Miller

February 20, 2024

Disclaimer: This contracted research report was prepared by Exovera LLC at the request of the U.S.-China Economic and Security Review Commission to support its deliberations. Posting of the report to the Commission’s website is intended to promote greater public understanding of the issues addressed by the Commission in its ongoing assessment of U.S.-China economic relations and their implications for U.S. security, as mandated by Public Law 106-398 and Public Law 113-291. However, the public release of this document does not necessarily imply an endorsement by the Commission, any individual Commissioner, or the Commission’s other professional staff, of the views or conclusions expressed in this contracted research report.
About Exovera

Exovera is a leading provider of artificial intelligence and advanced technology solutions and services that enhance intelligence and law enforcement operations by generating a higher level of awareness, understanding, and strategic foresight for its customers across a wide range of complex issues and environments. Exovera is a wholly owned technology subsidiary of U.S. defense contractor SOS International (SOSi). Since 1989, SOSi has provided specialized services supporting the national security interests of the United States and the security and stability needs of its allies. SOSi advances public safety and national security through innovative research, analysis, and applied technology. SOSi conducts research and analysis in key areas of defense and intelligence work, provides high-level systems engineering services to selected national and homeland security organizations, and produces hardware and software products for government and commercial consumers.

About CIRA

Exovera’s Center for Intelligence Research and Analysis (CIRA) is a leading national security think tank serving the U.S. government, Fortune 500 companies, and the broader Washington foreign policy community. Staffed by an experienced team of analysts with both deep subject matter expertise and advanced foreign language skills, CIRA provides cutting-edge research, analysis, and operational capabilities to both government and private sector clients.

Comments may be sent to Exovera’s Vice President of Intelligence Integration, Frank Miller.

Frank Miller
Vice President, Intelligence Integration
Exovera, LLC
2650 Park Tower Drive, Suite 300
Vienna, VA 22180
Email: Frank.Miller@exovera.com or Info@exovera.com
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>APT</td>
<td>Advanced Persistent Threat</td>
</tr>
<tr>
<td>CAC</td>
<td>Cyberspace Administration of China</td>
</tr>
<tr>
<td>CCP</td>
<td>Chinese Communist Party</td>
</tr>
<tr>
<td>CGTN</td>
<td>China Global Television Network</td>
</tr>
<tr>
<td>CNNIC</td>
<td>China Internet Network Information Center</td>
</tr>
<tr>
<td>GPU</td>
<td>Graphics Processing Unit</td>
</tr>
<tr>
<td>ICANN</td>
<td>Internet Corporation for Assigned Names and Numbers</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunications Union</td>
</tr>
<tr>
<td>IXP</td>
<td>Internet Exchange Point</td>
</tr>
<tr>
<td>LSG</td>
<td>Leading Small Group</td>
</tr>
<tr>
<td>MIIT</td>
<td>Ministry of Industry and Information Technology</td>
</tr>
<tr>
<td>MLPS</td>
<td>Multi-Level Protection Scheme</td>
</tr>
<tr>
<td>MPS</td>
<td>Ministry of Public Security</td>
</tr>
<tr>
<td>PLA</td>
<td>People’s Liberation Army</td>
</tr>
<tr>
<td>PRC</td>
<td>People’s Republic of China</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

About Exovera ............................................................................................................................ i

About CIRA .................................................................................................................................... i

**Executive Summary** ................................................................................................................ 1

Key Findings ................................................................................................................................ 2

**Policy Recommendations** .................................................................................................... 4
  Undermining the CCP’s Domestic Information Monopoly ................................................................. 4
  Safeguarding the U.S. Information Space from PRC Censorship ...................................................... 5
  Protecting the International Free Flow of Information ...................................................................... 5

Report Scope, Limitations, and Methodology ............................................................................ 6

**Part 1: The Nature and Reach of China’s Censorship Apparatus** ........................................ 8

Introduction: Addressing the “How” and “Why” of PRC Censorship ............................................ 8

Evolution of PRC Censorship Practices Prior to 2013 .................................................................... 9

Censorship in the “New Era:” Information Control under Xi Jinping ........................................... 11
  Operational Reforms: Promoting a Proactive Approach to Public Opinion Guidance .................... 12
  Legal and Regulatory Reforms: Promoting an Orderly and Traceable Online Ecosystem ............ 12
  Organizational Reforms: Consolidation and Coordination ............................................................... 14

Current Challenges Facing China’s Censorship Apparatus ........................................................... 14

**Part 2: Methods and Technologies That Underpin China’s Censorship Apparatus** .......... 15

Untangling the Web of China’s Censorship Apparatus ................................................................. 15

Technical Mechanisms That Underpin PRC Censorship Practices ........................................... 18

Standard Operating Practices for Censorship .............................................................................. 21
  Public Opinion Monitoring, Analysis, and Response .................................................................... 21
  Blocking and Deleting Harmful Material ..................................................................................... 23
  Focusing on Positive Publicity ..................................................................................................... 24

**Part 3: Going Global: Chinese Censorship Practices Abroad** ............................................ 25

Strategic Background: Competing in the Global Information Environment .................................. 26

Examining China’s International Censorship Practices ................................................................. 27
  Inducing Self-Censorship among Foreign Companies and Individuals ......................................... 28
  Using Information Operations as a Mechanism for Censorship ............................................... 29

Making the World Safe for Autocracy: Exporting China’s Censorship Model ............................. 30
  Building a Parallel Media Environment ....................................................................................... 31
  Sharing Best Practices for Censorship ......................................................................................... 31
  Remaking Global Internet Governance ....................................................................................... 32

**Part 4: Case Studies** ............................................................................................................ 33

Case Study One: Censorship during the COVID-19 Pandemic ..................................................... 34
  Guidance and Policy .................................................................................................................... 34
  Covering Up the Outbreak ......................................................................................................... 35
  Disputing the Origins of COVID-19 .......................................................................................... 37
  Persisting in Zero-COVID: Lockdowns and Protests ................................................................. 38

Case Study Two: Censorship of “Historical Nihilism” ................................................................. 40
Xi Jinping’s Approach to History ...................................................................................................................... 40
Key Topics in the CCP Censorship of History.................................................................................................. 41
Measures to Combat Historical Nihilism under Xi Jinping ............................................................................. 43
Censorship of History on the Internet and in Digital Media .............................................................................. 44

Case Study Three: Censorship of the Russia-Ukraine War .............................................................................. 45
Context and China’s Official Position ............................................................................................................... 45
State Media and the Russian Perspective .......................................................................................................... 45
The Role of Social Media ................................................................................................................................ 46

Part 5: Implications of PRC Censorship for the United States ................................................................. 48
Implications of PRC Domestic Censorship ........................................................................................................ 49
Implications of PRC International Censorship .............................................................................................. 49

Addendum I: Organizational Structure of the Bureaucratic Institutions That Comprise China’s Censorship Apparatus .......................................................................................................................... 51
China’s Central Propaganda Department ........................................................................................................... 51
Cyberspace Administration of China .................................................................................................................. 52
Ministry of Public Security ................................................................................................................................ 55
Ministry of Industry and Information Technology ............................................................................................. 56

Addendum II: The Role of Five-Year Plans in Shaping PRC Censorship Practices during the Xi Jinping Era ........................................................................................................................................ 58

Addendum III: Index of Laws and Regulations Relating to Censorship in the PRC ...................................... 60
Sources Cited ........................................................................................................................................................ 72
EXECUTIVE SUMMARY

The People’s Republic of China (PRC) is home to the world’s most elaborate and pervasive censorship apparatus. This system is used by the Chinese Communist Party (CCP) to maintain its monopoly on political legitimacy and to shape the behavior of China’s citizenry through what it calls “public opinion guidance.” The CCP views information control as being its first line of defense against threats to the PRC’s one-party political system, which the Party sees as essential for ensuring China’s continued security and prosperity. Accordingly, Party censorship focuses on suppressing ideas it regards as undermining China’s political order, such as the foreign “ideological contagion” of liberal democracy, ethnic separatism, and criticisms of senior CCP leadership.

Under General Secretary of the CCP Xi Jinping’s rule, the Party has significantly expanded the scope and stringency of its censorship apparatus, with a particular focus on solidifying its control over internet content. To this end, the Party has expanded and rationalized its legal and regulatory frameworks governing internet censorship while also upgrading its technical capacity to supervise online activity. These efforts have enhanced both the Party’s ability to supervise cyberspace discourse and its control over mediums ranging from social media platforms to online gaming to private companies that develop and deploy generative artificial intelligence (AI).

Censorship in the PRC is not enacted unilaterally by any one entity but rather is coordinated among a host of Party and state institutions.* Under this framework, guidelines for ideological and thought work are drawn up by the Central Party Committee and conveyed down to the lower echelons of the CCP. Collectively, this control apparatus encompasses three broad layers: (1) the physical infrastructure used to disseminate information; (2) the regulatory measures that modulate the content of information; and (3) the normative factors that shape culture, beliefs, and cognition. The CCP has demonstrated adeptness in using this apparatus to manage acute crises such as criticisms of its response to the COVID-19 pandemic as well as endemic challenges such as combating “historical nihilism” (i.e., interpretations of history that contradict the Party’s official version of events). At the same time, the CCP allows for limited discussions of sensitive topics that do not directly threaten its hold on power, such as China’s role in the ongoing Russia-Ukraine conflict.

Although the PRC’s censorship apparatus is geared toward maintaining internal stability, its effects pose a major challenge to U.S. diplomatic, economic, and national security interests. In the past ten years, China has intensified efforts to combat the international spread of ideas and narratives it deems to threaten PRC “core interests.” This undertaking has proceeded along multiple lines of effort, including punishing U.S. private companies and individuals who express positions the CCP deems to be objectionable, restricting U.S. access to economic data, and conducting disinformation campaigns aimed at sowing division within U.S. society. Concurrently, the PRC has exported censorship tools to other authoritarian states while also advancing its preferred vision of “cyber sovereignty,” actions that undermine existing U.S.-supported norms and accords that have heretofore facilitated the global free flow of information. Lastly, the PRC uses censorship as a tool to advance its revanchist geostrategic goals, such as isolating Taiwan and laying the groundwork for eventual cross-Strait unification. These challenges necessitate that the United States takes

* This report will use the term “Party-state” to describe such institutions, as it best reflects the combined role that CCP and state bureaucratic organs play in information governance.
action to safeguard its domestic information space and to preserve a free and open internet, both of which are vital factors for continued U.S. economic prosperity and individual liberty.

**Key Findings**

*Nature and Reach of China’s Censorship Apparatus*

- Under the leadership of General Secretary Xi, the PRC has dramatically expanded its censorship apparatus. This undertaking has entailed bureaucratic reforms aimed at streamlining Party control over internet content, operational reforms to improve the technical acumen of CCP censors, and legal reforms intended to broaden state supervision over all forms of media.

- Although the CCP places severe restrictions on freedom of expression, it does not see total control over China’s information environment as being necessary or even desirable. Consequently, Party censors often allow for limited discussions of sensitive topics such as local government corruption and mismanagement. At the same time, the CCP rigorously enforces censorship on key topics, such as criticisms of senior Party leadership figures, the validity of China’s one-party political system, and select historical topics such as the 1989 Tiananmen Square protest movement.

- Despite the importance the CCP places on domestic information control, its censorship apparatus is unevenly developed and plagued by unfunded mandates. In particular, administrative authorities and institutional linkages that govern local internet censorship are organized haphazardly, with many localities having redundant or overlapping areas of responsibility and poorly delineated means of interbureaucratic coordination. In some cases, these inefficiencies lead to gaps in censorship that undermine the capacity of local Party committees to exercise information control within their area of jurisdiction and contribute to instances of social unrest.

*Methods and Technologies Underpinning China’s Censorship Apparatus*

- There is no singular Party-state entity tasked with enforcing information control within the PRC. Rather, censorship is undertaken jointly by the Central Propaganda Department (CPD), the Cyberspace Administration of China (CAC), the Ministry of Public Security (MPS), and the Ministry of Industry and Information Technology (MIIT). Collectively, these institutions wield a number of overlapping and redundant capabilities to enforce censorship both online and offline. These measures include control over information gatekeepers such as publishers, technical measures blocking Chinese citizens’ ability to access and spread forbidden content, and deterrent measures such as the threat of detention or incarceration for engaging in forbidden political speech.

- Although data restrictions and state secrecy in the PRC inhibit a comprehensive quantitative analysis of internet censorship trends, authoritative materials published by the CCP suggest that day-to-day online content management is not enacted directly by the Party-state but rather is undertaken proactively by publishers, internet service providers (ISPs), website owners, and mobile application platforms seeking to avoid incurring penalties. The PRC’s policy of assigning legal liability to ISPs and private website owners has driven these entities to self-police and censor content posted on their platforms. As a
result, many companies maintain their own network content management systems or subcontract that work to third-party moderators.

- Current Party guidance for internet content moderation stresses that deletion and blocking of posts should be a last-resort measure and that Party organs should instead focus their energy on proactive measures such as public engagement and “spreading positive propaganda.” However, in practice these directives are not always carried out, especially among local officials, who often default to using blunt-force censorship measures in order to maintain social stability and secure their own career advancement.

**China’s International Censorship Practices**

- Under General Secretary Xi, the PRC has invested heavily in its capacity to conduct “international public opinion guidance.” In pursuing this undertaking, the Party-state employs many of the same tactics it uses for domestic censorship. For instance, PRC information operations frequently “flood the zone” on foreign social media platforms with irrelevant content designed to hijack or demobilize discussions of topics the Party deems to be sensitive, such as human rights abuses in Xinjiang and Tibet.

**Lessons Gleaned from Case Studies**

- The Party’s response to the COVID-19 pandemic demonstrated the flexibility and adaptability of its censorship apparatus during crisis scenarios. For example, at the outset of the pandemic, criticisms of local officials and mentions of whistleblower Li Wenliang were initially censored but were later co-opted and amplified by Party-state outlets after public outcry in order to boost the legitimacy of the CCP.

- PRC coverage of the Russia-Ukraine War suggests the CCP uses the same approach to censoring discussions on foreign policy issues as it does for domestic affairs. For instance, Chinese netizens are permitted to discuss the conflict openly so long as those conversations avoid certain sensitive topics, such as the implications the war might have for a future dispute over Taiwan.

**Implications for the United States**

- The PRC is taking steps to curtail foreign access to information it deems to be sensitive, including corporate records, economic data, and scholarly research materials. This trend threatens to impair the ability of U.S. policymakers to accurately understand prevailing economic, political, and social trends within China.

- The CCP’s growing ability and ambition to control information beyond its borders may complicate U.S. foreign policy objectives. For instance, the PRC actively seeks to censor international acknowledgements of Taiwanese sovereignty in order to diplomatically isolate the island and lessen international willingness to intervene in a prospective cross-Strait conflict.

- The PRC is devoting considerable resources toward the development and fielding of advanced AI and big data analysis technologies for online content monitoring. This has the potential to greatly enhance the reach and targeting precision of its already vast media surveillance and censorship apparatus. Crucially, many of these AI-enabled “public opinion guidance” tools rely on off-the-shelf components imported from the United States, such as general processing units (GPUs) and cloud computing infrastructure.
Policy Recommendations

Based on these key findings, the authors of this report have formulated the following set of policy recommendations. These measures are grouped along three main themes:

Undermining the CCP’s Domestic Information Monopoly

1) Support the continued development and marketization of emerging telecommunications technologies, such as satellite-based internet constellations, to impose costs on the PRC’s censorship apparatus.

Recent advances in telecommunications technology, such as satellite internet constellations, have the potential to undermine the CCP’s stranglehold over data flows into and out of China. These constellations provide broadband services to users without the need for ground-based fiber optic cables. Widespread adoption of satellite-based internet has the potential to upend China’s current internet censorship model, which is heavily reliant on terrestrial data bottlenecks, such as internet exchange points (IXPs). It should be noted that satellite-based internet is not a panacea to internet censorship. Indeed, the PRC is already in the early stages of updating its censorship tactics and deploying its own satellite internet infrastructure to adjust to this new paradigm. Nevertheless, shifting to this model for internet dissemination would impose significant cost on the PRC’s censorship apparatus by forcing it to police a much more decentralized telecommunications infrastructure environment.

2) Instruct the U.S. Department of State to conduct a feasibility study to explore avenues to expand and improve upon U.S. public diplomacy efforts in China and provide objective reporting on misconduct and misgovernment by the Party-state.

While the United States possesses limited power to influence China’s information environment directly, public diplomacy nevertheless plays an important role in undermining its censorship apparatus. Access to objective information plays a key role in enabling China’s citizenry to hold their government accountable, especially during inflection points such as the 2019 COVID-19 pandemic outbreak and the subsequent 2022 anti-lockdown protest movements. Moreover, effective public diplomacy has the potential to expose false CCP narratives at critical junctures. For instance, in 2012, the State Department’s decision to tweet daily statistics on air quality in Beijing played a pivotal role in forcing the PRC government to revise its own pollution estimates. Additional resources for U.S. public diplomacy institutions such as Voice of America and its counterpart Radio Free Asia could enable those institutions to replicate this success by shining a spotlight on instances of misconduct and misgovernment by the Party-state.

3) Increase the budgets of federal grant-making agencies such as the National Endowment for the Humanities, National Science Foundation, and National Endowment for the Arts—which support scholars and journalists who conduct work related to China—in order to mitigate the negative impact of censorship measures, such as entry bans.

Independent journalism and scholarly research have been central to undermining PRC censorship of sensitive topics, ranging from the 2019 prodemocracy protests in Hong Kong to the CCP’s mistreatment of Uyghurs in Xinjiang. Accordingly, the United States can support these efforts by increasing funding for scholarships and grants for research related to China as well as facilitating broader access to resources such as archives. The benefits of this approach are twofold. First, it would increase both the breadth and quality of investigative research related to China. Second, it
would mitigate the negative impact of censorship measures such as entry bans by providing scholars and journalists with alternative avenues of inquiry aside from field research.

4) Support institutions that keep a public record of internet information and check the PRC censorship apparatus’s ability to reshape China’s public information environment.

The United States should promote and support projects that maintain a true historical record of information posted to public websites in China, such as the U.S. digital library service Internet Archive and its WayBack Machine. This regularly updated public record helps check the PRC censorship apparatus’s ability to reshape China’s public information environment in real time and serves as a key countermeasure to CCP attempts to obscure and rewrite history.

**Safeguarding the U.S. Information Space from PRC Censorship**

1) Strengthen information sharing and collaborative research aimed at countering disinformation on social media.

The United States should increase coordination with the private sector to combat PRC disinformation campaigns, which are often used by the CCP regime to enact de facto censorship abroad. As part of this effort, the United States should support the development and spread of tools geared toward preventing common “information saturation” techniques such as using botnets to hijack and algorithmically manipulate online conversations on sensitive topics. Moreover, elements of the U.S. intelligence community should deepen avenues for sharing information on tactics, techniques, and procedures used by state-backed advanced persistent threat (APT) groups specializing in information operations such as the PRC-linked DRAGONBRIDGE unit.³

2) Instruct the U.S. Department of Commerce to conduct a feasibility study examining best practices for supporting private firms that are subject to economic pressure by the PRC.

The threat of economic pressure and revocation of market access is a powerful tool used by the PRC to deter private companies from platforming anti-CCP voices or taking public positions that run counter to Party interests. To blunt this tool, the Department of Commerce should conduct a study examining common tactics used by China to coerce overseas companies into adhering to CCP messaging. The study should outline a set of best practices for public-private coordination that the U.S. government can use to assist private entities that face PRC economic pressure for supporting freedom of expression.

**Protecting the International Free Flow of Information**

1) Build international support for the current multistakeholder model of internet governance.

The United States should step up its efforts to counter PRC attempts to delegitimize the frameworks, norms, and organizations that enable a free and open internet. This should entail broader public diplomacy and engagement efforts through forums such as the International Telecommunications Union (ITU) aimed at demonstrating the advantages of the current system of global telecommunications governance and the pitfalls of China’s preferred “cyber sovereignty” model. Concurrently, the United States should reaffirm its commitment to the independence of organizations such as the Internet Corporation for Assigned Names and Numbers (ICANN) and take steps to ensure that the deliberations and decisions of those organizations are not subject to nation-state interference.
2) Restrict the transfer of data, hardware, software, and expertise used to support next-generation censorship tools.

The PRC is prioritizing the development of next-generation censorship and online content moderation technologies based on AI and big data analysis. Accordingly, the United States should bolster its efforts to restrict the sale of the component parts used to construct these tools as well as other inputs such as data used to train machine learning models. Concurrently, the United States should issue a public advisory list of PRC-based companies that support state censorship, including their subsidiaries or shell companies. Doing so will greatly assist due diligence by U.S.-based technology firms and will enable them to avoid inadvertently supporting China’s censorship regime.

**Report Scope, Limitations, and Methodology**

Researching China’s censorship apparatus poses a number of inherent methodological challenges. First, quantifying CCP information control is difficult because it entails proving a counterfactual: demonstrating what would have happened had censorship not occurred. This problem is exacerbated by the fact that the Party exerts tight supervision over publishers, web platforms, and media outlets that operate in China and limits access to data that could be used to prove instances of censorship. Moreover, the PRC’s omnipresent security state induces many Chinese citizens to self-censor to avoid the threat of detention or incarceration. Second, censorship in the PRC is difficult to observe and measure because the Party often favors indirect methods of information control that marginalize opposing voices rather than outright suppressing them. Conventional censorship (e.g., deletion of social media posts) comprises only a small fraction of Party censorship activities. Instead, the CCP’s information control strategy is primarily reliant on drowning out “harmful” narratives by saturating China’s information environment with content that is either apolitical or supportive of the Party. Despite these limitations, there are a number of means that can be used to gauge the nature, scope, and extent of censorship in China. These include content analysis of CCP standard operating procedures for enacting information control, structural analysis of Party organs that conduct censorship, and case study analysis of how China’s censorship system has reacted to specific challenges.*

This report seeks to outline the structure, characteristics, and impact of China’s censorship apparatus. The report is subdivided into five main parts. Part 1 will assess the nature and reach of censorship within the PRC by examining the historical, ideological, and legal basis for CCP information control. Part 2 will outline the institutions, methods, and technologies that underpin China’s censorship apparatus as well as summarize the existing challenges Party censors face in carrying out their mission. Part 3 will examine how China has sought to apply its methods of information control globally through practices such as “international public opinion guidance” as well as ongoing efforts to influence international norms pertaining to censorship. Part 4 will be composed of three case studies illustrating how the PRC has used censorship to shape domestic and international narratives on the COVID-19 pandemic, historical nihilism, and the ongoing Russia-Ukraine conflict. Lastly, Part 5 will conclude with an assessment of the impact Chinese censorship practices have on the United States. In undertaking this task, this report acknowledges that censorship is merely one aspect of information control and is used in concert with other

---

* In this report, “content analysis” refers to the textual analysis of PRC laws, regulations, and guidelines to assess how and when information control is enacted. Similarly, “structural analysis” involves examining the bureaucratic structures, mission sets, and composition of Party-state organizations responsible for censorship.
instruments of Party-state power such as propaganda, surveillance, and policing. However, for the purpose of analytical focus, the report will only examine those functions insofar as they have a demonstrated role in censorship.

To construct an accurate portrait of China’s censorship apparatus, this report chiefly draws upon authoritative Chinese-language sources to form the foundation of its analysis and conclusions. These sources include official addresses made by Party leadership, planning and guidance documents issued by the PRC central government, municipal and provincial budgetary documents, job postings, and corporate records materials. It also draws upon other primary source materials with a high degree of reliability, such as internally circulated books, technical manuals, and guidance texts published by Party-affiliated academia as well as journal articles published by core elements of the Party-state apparatus. * These ancillary sources provide a glimpse into the internal discussions and debates within the CCP pertaining to censorship and information control. Finally, this report supports its findings by drawing upon preexisting English-language scholarly literature and news reporting as well as background interviews with subject matter experts.†

* These include Qiushi (lit. “Seeking Truth” 求是), published by the Central Party School; Party Building (党建), published by the Central Propaganda Department School; and New Media (lit. “Network Broadcasting” 网络传播), published by the Cyberspace Administration of China.

† In particular, the authors would like to thank Dr. Margaret E. Roberts and Dr. Darren L. Linvill for providing their valuable insight and feedback.
PART 1: THE NATURE AND REACH OF CHINA’S CENSORSHIP APPARATUS

Introduction: Addressing the “How” and “Why” of PRC Censorship

The CCP regards its monopoly on political legitimacy as foundational to maintaining China’s continued security and development. This viewpoint stems from the Party’s long-held notion that maintaining undisputed authority is a precondition for effective governance, as encapsulated by Mao Zedong’s dictum that “to master ideological leadership is to master all forms of leadership.” Accordingly, successive generations of CCP leadership have implemented measures to maintain the Party’s firm hold over China’s information environment.*

The CCP’s censorship policy constitutes a natural outgrowth of its stated imperative of maintaining ideological primacy. China’s leadership has repeatedly made clear that it views control over information as foundational to the PRC’s overall national security. Consequently, the Party seeks to uphold domestic harmony by rectifying “erroneous trends of thought” (错误思潮) among the masses while guarding against the encroachment of Western “universal values” (普世价值), such as liberal democracy, that are antithetical to China’s one-party political system. The Party also views information control as a bulwark against nontraditional security challenges like “ethnic separatism” in Hong Kong, Tibet, and Xinjiang, which the CCP perceives as a threat to China’s territorial integrity.†

The key role of the Party’s censorship apparatus has come into particularly stark relief with the rise of the internet. As officials such as Cyberspace Administration of China (CAC) director Zhuang Rongwen have noted, platforms such as social media have upended the traditional mechanisms used by the Party to govern China’s information environment by decentralizing the mechanisms of narrative dissemination. At the same time, the Party assesses that the internet has opened new vectors for “hostile foreign forces” to spread their influence, especially among China’s youth, who are regarded as being extremely susceptible to being “bewitched” by anti-Marxist values such as excessive consumerism and historical nihilism.‡ As will be discussed later in this section, these concerns are the animating force behind current efforts to strengthen the PRC’s censorship apparatus.

Although the CCP exercises a pervasive influence on civic life within the PRC, it does not regard absolute control over China’s information environment as being practical or even desirable. Indeed, China’s leadership views a degree of civic openness as being necessary to facilitate commercial and scientific development as well as to prevent ideological rigidity and social stagnation. In practice, this results in the CCP allowing limited discussion of certain sensitive topics such as corruption and mismanagement by local officials. Doing so acts as a social safety valve through which citizens can air concerns and grievances while also enabling the Party to deflect blame to low-level administrators who “incorrectly” carry out central Party-state directives. However, in allowing these exchanges, the Party is constantly on guard against the emergence of social trends

---

* Within authoritative PRC literature there is no unified definition or descriptive term for the information environment. Hence, for the purpose of analytical clarity, this report will adhere to the definition laid out by the U.S. National Institute of Standards and Technology, which defines the information environment as “the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.”

† The CCP’s definition of “ethnic separatism” is significantly more expansive than Western interpretations, encompassing any conspicuous assertion of non-Han identity or culture alongside advocacy for political separation.

‡ Notably, these perceived ideological threat vectors are not limited to political content. Rather, they also include cultural products such as film, literature, and music.
that might threaten public order or regime stability. As a result, certain topics—such as criticisms of central Party leadership, the People’s Liberation Army (PLA), and the validity of China’s one-party state model—are subject to absolute censorship. Hence, at the most basic level, Party information control policy seeks to manage the inherent “dialectical tension” between having sufficient societal openness to promote development while also maintaining domestic security.

In order to strike a balance between these two considerations, the CCP employs a framework of “public opinion guidance” (舆论引导) that entails proactively cultivating popular support while selectively employing censorship measures against citizens who criticize the Party or its policies.* This approach places the primary onus of shaping public attitudes on China’s political and ideological work organs, which are directed to “focus on producing positive propaganda” by saturating China’s information environment with lighthearted and anodyne content.† The strategy of public opinion guidance serves the dual purposes of building trust and support for CCP governance while also drowning out voices that express discontent. Concurrently, the Party employs a flexible approach to censorship that grants citizens a degree of latitude so long as they do not violate certain precepts such as challenging the central leadership of the CCP.‡ These methods, which have been collectively dubbed “porous censorship” by the scholar Margaret Roberts, enable the PRC to reap the material benefits of societal openness while minimizing emergent threats to social stability. The result is an informational chilling effect whereby citizens self-censor to avoid running afoul of ill-defined redlines.

Evolution of PRC Censorship Practices Prior to 2013

Although the CCP’s censorship apparatus has consistently worked toward the singular end of ensuring its domestic political hegemony, the means by which the Party-state enacts information control have varied over time. During the Mao era, the Party rigorously enforced centralized management over media such as film, news, and radio as well as interpersonal speech between private citizens.‡ These strict controls over information bottlenecks, coupled with near-omnipresent state surveillance, left few avenues available for public dissent. After Mao’s death in 1976, China’s subsequent “reform and opening-up” period heralded a significant relaxation of censorship and an unprecedented degree of experimentation within civil discourse. This comparatively hands-off approach was justified by leadership figures such as Zhao Ziyang as a necessary expedient to facilitate China’s economic revitalization. However, this liberalizing trend was counterbalanced by CCP hardliners, who cautioned against Western attempts to depose

---

* Most authoritative Party sources do not directly use the term “censorship” (审查制度). Rather, CCP nomenclature tends to adopt euphemistic terms for information control such as “content management” (内容管理) and “dredging and blocking” (疏堵结合).
† For instance, the Party-state allows for criticisms of local government and even certain types of investigative journalism so long as those actions are not targeted at central leadership. Moreover, restrictions on accessing censorship evasion software such as virtual private networks (VPNs) are laxly enforced and serve more as “speed bumps” rather than outright prohibitions.
‡ Measures for enacting this control included the Nomenklatura system whereby key information gatekeepers such as editors, publishers, and film directors are centrally appointed by the CCP, as well as “neighborhood committees” tasked with surveilling and reporting the behavior of ordinary citizens.
Party rule through promoting China’s “peaceful evolution.”* 24 These intra-Party tensions resulted in a fractured approach to enforcing ideological orthodoxy within society, which in turn was a prime contributing factor enabling the 1989 Tiananmen protest movement that nearly led to the collapse of the CCP regime.† 25

The post-Tiananmen period saw a revitalization of the Party-state censorship apparatus as the CCP sought to stifle the liberalizing trends that toppled communist regimes in Europe and almost initiated its own downfall. 26 This resurgence included measures such as mandating stricter oversight over media content as well implementing a National Program for Patriotic Education (爱国主义教育) designed to instill “ideologically correct” principles among China’s youth. 27 The 1990s also saw the CCP confront a new threat to its information monopoly in the form of the emergent global internet. 28 For Party leaders, embracing the global trend of “informatization” (信息化) was deemed necessary to facilitate China’s continued economic growth. 29 However, the decentralized nature of the internet also presented a sui generis challenge that eluded preexisting mechanisms of information control. 30 Unlike traditional mediums, internet discourse is chiefly generated from the “bottom up,” creating a near-infinite array of sources of potential dissent. 31 As such, top-down censorship strategies such as oversight over information gatekeepers were rendered infeasible. To meet this challenge, the CCP sought to pioneer an entirely new censorship methodology tailored specifically for the internet. This project rested on two mutually supporting pillars. First, the Party implemented strict oversight over the physical nodes through which internet traffic flows in China, such as internet exchange points (IXPs), creating artificial bottlenecks suitable for monitoring and oversight. 32 Second, it enacted a series of policies criminalizing the use of computer networks to undermine state power or social stability.‡ 33 These twin initiatives facilitated Party-state supervision of cyberspace and have come to form the bedrock of China’s modern internet censorship apparatus.

Since the year 2000, the CCP has steadily promulgated a collection of laws aimed at codifying and refining the legal basis for internet censorship in China.§ These include the Regulation on Internet Information Services Management (互联网信息服务管理办法), which set boundaries on the types of content that internet service providers (ISPs) were permitted to host, as well as the Interim Provisions on the Administration of Internet Sites Engaged in Posting News Business (互联网站从事登载新闻业务管理暂行规定), which stipulated that only licensed publishers could distribute news online. 34 These measures were backed up by an array of supplemental regulations passed by the Party-state bureaucracy governing conduct on platforms ranging from internet

---

* CCP anxieties about the spread of malicious capitalist influence were not limited to political content. Indeed, an equally common concern was the specter of “spiritual pollution” (精神污染) caused by the proliferation of consumerism, individualism, and pornography.

† Many CCP historians use the negative example of Tiananmen to stress the paramount importance of the Party maintaining an outward appearance of ideological unity. Although internal divisions persist within the CCP, it has subsequently taken pains to ensure that censorship and propaganda efforts are undertaken in lockstep with uniform guidance handed down from Party leadership.

‡ For instance, the Ministry of Public Security’s 1997 Computer Information Network International Networking Security, Protection, and Management Regulations (计算机信息网络国际联网安全保护管理办法) outlaw online activity that “endangers national security, divulges state secrets, infringes on national or social interests, propagates superstition, or disseminates information that subverts the constitution, state power, and national unity.”

§ A full taxonomy of laws pertaining to censorship passed between 1994 and August of 2023 can be found in Addendum III of this report.
message boards to online gaming services. This period also saw the Party-state make its first forays into internet public opinion guidance as provincial and municipal Party committees established dedicated organs for online content management. Taken together, these legal and bureaucratic measures significantly bolstered CCP oversight over cyberspace. However, they also produced a bloated regulatory apparatus rife with inefficiency—one that would undergo significant evolution after Xi Jinping came to power in 2013.

Censorship in the “New Era:” Information Control under Xi Jinping

Under the leadership of General Secretary Xi, the Party has revised and expanded its censorship apparatus while adopting an increasingly draconian approach to information control. While the CCP’s core censorship targets remain the same under Xi Jinping, the severity with which the Party-state applies censorship standards has intensified. The rationale guiding this hardline approach can be glimpsed from a leaked internal directive that purportedly originated from the Central Party Committee in 2012, entitled Communiqué on the Current State of the Ideological Sphere (关于当前意识形态领域情况的通报) or, more simply, “Document No. 9.” The communiqué assessed that Western countries are actively engaged in undermining the PRC’s political system and identified a number of pervasive “ideological contagions” such as political pluralism and adversarial journalism that threatened the CCP’s grip on power. Release of the communiqué preceded an all-encompassing effort to strengthen Party oversight over all aspects of China’s information environment through measures such as purging unreliable scholars from academia and paring down the number of news services permitted to operate in the PRC.

Although General Secretary Xi has called upon the Party to step up censorship across all content mediums, he has singled out the internet as the primary area of focus. Shortly after assuming power in 2013, Xi declared that the Party should “make internet public opinion work the top priority of propaganda and ideological work.” He has frequently emphasized this theme in subsequent addresses, often framing the issue in life-or-death terms. For instance, in a 2022 speech, Xi declared that “the internet has become the main front, battlefield, and forefront of the realm of ideological struggle,” and “whether [the CCP] can fight and win the ideological battle on the internet is directly related to the political security of the country.” In order to win this ideological struggle, Xi has directed the Party to establish what he calls a “comprehensive network governance system” (网络综合治理体系). Such a system entails “Party committee leadership, government management, corporate enterprise responsibility, social supervision, and netizen self-discipline” and combines the use of “economic, legal, and technical means” to manage information content and create a “clear and bright” cyberspace environment. Xi’s drive to strengthen Party leadership within the online sphere has led to the creation and elevation of new bureaucratic organs, such as CAC, as well as the re-empowerment of legacy institutions, such as the Central Propaganda Department (CPD). These organizations have served as the Party’s chief instrument for exercising “comprehensive network governance” during Xi’s tenure.

* Specifically, the CCP has expanded its censorship bureaucracy to more rigorously enforce its longstanding prohibitions on criticisms of Party leadership, the PRC’s socialist government structure, “ethnic separatism,” “Western concepts” of individual rights, liberal cultural influences, and the spread of banned religious groups such as the Falun Gong.

† The document identifies seven problematic thought trends that must be addressed by the Party: promotion of Western-style constitutional democracy, promotion of “universal values,” promotion of notions of civil society that undermine the CCP’s political monopoly, promotion of neoliberalism or “absolute market control,” promotion of Western-style journalism practices, promotion of “historical nihilism,” and questioning the validity of China’s “reform and opening-up.”
Against a backdrop of concern at the highest levels for managing and securing China’s public information space, the CCP’s internet censorship and public opinion monitoring practices are undergoing significant evolution. Objectives for Party-state public opinion guidance have been updated across successive five-year planning cycles (detailed in Addendum II of this report) and have resulted in three main outcomes. First, organizational reforms have enhanced the CCP’s ability to coordinate censorship campaigns and public opinion emergency response measures both hierarchically and across government agencies. Second, legal and regulatory reforms have standardized and clarified the obligations and expected behaviors of online platform operators and internet users in ways that promote self-censorship and make it simpler for authorities to determine the identity of individuals influencing online public opinion. Third, operational reforms have expanded both the purview and capabilities of government organizations involved in online content work, encouraging administrators to not only monitor public opinion but also actively shape it. Although reforms in all areas remain works in progress, they constitute a concerted effort to improve the CCP’s ability to control China’s online information environment and make full use of it as a tool of governance.

Operational Reforms: Promoting a Proactive Approach to Public Opinion Guidance

Under the direction of General Secretary Xi, the Party-state is undertaking a qualitative shift in the way it conducts censorship. This change is marked by a concerted effort to move away from “blindly suppressing, blocking, or deleting content” toward an engagement-based approach that emphasizes persuasion and tutelage from Party cadres. The rationale for enacting a revitalized approach to information control was outlined by Xi at the 2018 National Propaganda and Thought Work Conference (全国宣传思想工作会议), wherein he criticized existing public opinion guidance as overly aloof.* In order to remediate these deficiencies, Xi directed the Party to make more extensive use of social media and mobile applications to educate China’s citizens and rectify so-called “incorrect thought trends.” Consequently, Party committees at all levels have been directed to revamp their propaganda and information control strategies. The degree to which the CCP has implemented these qualitative reforms is unclear. For example, during the 2023 National Propaganda and Thought Work Conference, Xi praised the CCP for making “fundamental changes” that “improved Chinese citizens’ confidence in the Party, as well as their overall spiritual outlook.” Nevertheless, he also noted that the CCP’s mission of reforming its information control apparatus is ongoing and that further action is needed to safeguard the Party’s ideological primacy.

Legal and Regulatory Reforms: Promoting an Orderly and Traceable Online Ecosystem

CCP reform efforts have focused on promulgating official sources of law and administrative measures aimed at standardizing the behavior of internet platform service providers and netizens. The centerpiece of this undertaking is the 2017 Cybersecurity Law of the People’s Republic of China (中华人民共和国网络安全法), which consolidates prior legal provisions on information and data security while providing Party-state authorities expanded oversight authority over network content. This legislation has been supplemented by a slew of companion laws and regulations that collectively form the statutory basis for China’s comprehensive network management system. These measures cover myriad topics ranging from general guidelines

* The National Propaganda and Thought Work Conference is held every five years and usually occurs shortly after the National Party Congress.
governing netizen conduct to restrictions on specific technologies such as AI-generated “deepfake” images and videos. The general trend of these measures is to promote three main aims. The first is to provide clearer enforcement mechanisms for ensuring compliance with preexisting CCP prohibitions on harmful information (this trend will be explored more fully in Section 2 of this report). The second is to make it easier for Chinese public security authorities to identify and trace sources of online information and to monitor public sentiment while fostering a climate of self-censorship by internet platform operators and individual users. The third is to implement more stringent controls over internal and outbound flows of data.

A primary focus of the PRC’s updated cyberspace legal regime is promoting accountability and eliminating avenues for anonymity among netizens. In order to achieve this end, CAC promulgated the 2017 Management Regulations for Internet Comment Services (联网跟帖评论服务管理规定) and has continually updated the framework in subsequent years. These rules expand upon preexisting legislation requiring service providers to positively identify their users, track their activity, and make such data available to the Party-state. Article 8 of the 2017 Management Regulations states that users should be denied service if they do not provide their real names when registering for online forums and message boards. Additionally, article 9 requires that users register under their real names to post or reply to comments on news websites and social media. A 2022 update to the Management Regulations adds responsibilities for Chinese operators of internet platforms such as social media and web video platforms, requiring them to approve all news-related comments and directing them to hire content moderation teams to review all comments and filter out harmful content. It further stipulates that platform users can be held liable for “liking” or circulating posts deemed to spread illegal or harmful information and mandates that network service providers report such activity to CAC.

The Party-state has shored up measures aimed at preventing domestic leakages of potentially sensitive information while also enacting tighter controls over transnational exchanges of data deemed to be of import for national security. On the domestic front, the Ministry of Public Security (MPS) Cybersecurity Multi-Level Protection Scheme 2.0 (网络安全等级保护 2.0 标准), or MLPS 2.0, expanded the definition of data deemed relevant to national security and put in place stronger enforcement measures aimed at preventing unauthorized disclosures of information.* On the international front, both the 2021 Data Security Law (中华人民共和国数据安全法) and 2021 Personal Information Protection Law (中华人民共和国个人信息保护法) empower CAC to approve or deny outbound transfers of data. Likewise, CAC’s 2022 Measures on Security Assessment of Cross-Border Data Transfer (数据出境安全评估办法) mandate security assessments for outbound transfers of data that “may endanger national security, economic operation, social stability, and public health and safety” if leaked or illegally obtained.

---

*This expanded definition includes information from “network infrastructure, critical information systems, websites, big data centers, cloud computing platforms, the Internet of Things, industrial control systems, public service platforms, mobile Internet, and other areas.”
government or large corporations such as state-owned enterprises or foreign firms), unauthorized VPN usage remains prevalent. This is particularly true among China’s youth, who tend to use VPN software much more than older age cohorts (albeit mostly for the purpose of accessing Western entertainment platforms like YouTube and Twitch rather than seeking out forbidden political information). Generally speaking, restrictions on censorship evasion software are laxly enforced and serve more as “speed bumps” rather than outright prohibitions. Nevertheless, VPN prohibitions are far from being a dead-letter law. Indeed, over the past decade there have been a small but significant number of cases wherein Chinese citizens were issued warnings, fined, or even imprisoned for VPN usage. The PRC’s sporadic and arbitrary enforcement of VPN laws is perplexing, evincing a disconnect between the CCP’s stated policy of prohibiting VPN usage and its ability or willingness to enforce those prohibitions. However, one potential explanation may be that the CCP largely tolerates “apolitical” VPN usage among the general populace, such as accessing streaming services. Conversely, members of perceived “high-risk” groups such as political dissidents and ethnic or religious minorities are singled out for heightened scrutiny and disproportionate punishment for downloading so-called “violent and terrorist software,” even in cases where VPNs are used solely for benign or innocuous purposes.

**Organizational Reforms: Consolidation and Coordination**

Under General Secretary Xi, there has been a trend toward consolidating the distribution of responsibility for establishing and implementing requirements for censorship and public opinion monitoring. Accordingly, internet content management work is now coordinated at the national level by CAC, a quasi-Party, quasi-government organization affiliated with both the CCP’s propaganda apparatus and the Chinese state government under the State Council. The scope and impact of these organizational reforms will be assessed in more detail in Addendum I of this report.

**Current Challenges Facing China’s Censorship Apparatus**

Despite CCP efforts to expand and enhance its censorship regime, internal Party assessments make clear that the system is still plagued by deficiencies. This is especially true within the lower echelons of China’s government, where some localities struggle to meet even basic objectives such as stability maintenance and preventing the occurrence of “mass incidents.” The CCP’s self-diagnosed shortcomings of its censorship apparatus can be categorized into three main themes.

First, censorship and information control efforts are inhibited by a lack of clearly defined authorities and responsibilities, especially among local governments. Many local governments in China rely on ad hoc collections of information channels to monitor and guide public opinion, which results in a fractured and ineffectual approach to public opinion management work. This dynamic is illustrated in a 2014 research report produced by the Fuzhou Municipal Propaganda

---

* “Authorized” individuals in the PRC can access VPNs through two main channels: state-owned telecoms or foreign companies operating through joint ventures with Chinese firms. Private citizens in China seeking to hop the Great Firewall are generally excluded from using these services but can still obtain and operate VPN software from popular international vendors such as ExpressVPN, Surfshark VPN, and NordVPN. However, the performance of these commercial VPNs in China has degraded significantly over the past ten years.

† Indeed, so-called mass incidents involving public demonstrations are surprisingly commonplace in China (for instance, one estimate from a Tsinghua University professor assessed that 180,000 such incidents occurred in the year 2010). To date, no qualitative study has demonstrated a correlation between lack of resourcing for CCP censorship and the frequency of mass incidents. However, self-assessments undertaken by the Party-state seem to suggest the CCP believes the two factors are closely interrelated.
Department, which noted that some localities completely lack codified interdepartmental censorship responsibilities or accountability systems for managing public opinion work.* It appears that these weaknesses remain persistent in the present day, given that as of 2023 the CCP still has not published formal guidelines for intragovernmental and intra-Party coordination on public opinion guidance work.\textsuperscript{70}

Second, institutions that conduct censorship often lack the necessary qualified staff to carry out their responsibilities effectively and are forced to rely upon part-time or volunteer workers. While the CCP’s leadership has laid out an ambitious vision for expanding its network content management capabilities, this undertaking has not been accompanied by a commensurate increase in resourcing for local-level Party committees. Consequently, China’s network content system is unevenly developed, with local governments in poor and rural areas lacking sufficient personnel to monitor and respond to trends in online public opinion.\textsuperscript{71} Moreover, even in large metropolitan areas such as Beijing, ancillary censorship functions such as internet commentary work are undertaken by volunteers or by government employees who are contractually obligated to fulfill those tasks in their spare time.\textsuperscript{72} The practice of imposing unfunded mandates on local governments has resulted in suboptimal censorship implementation, with many localities being criticized by their supervisory propaganda committees for their “careless” and “half-hearted” approaches to information control.\textsuperscript{73}

Third, CCP information control efforts are often undermined by human error and mismanagement. While Party guidelines stress that internet public opinion work should focus on identifying, engaging with, and remediating public grievances, in many cases local government officials will default to deleting posts that raise sensitive criticisms.\textsuperscript{74} The practice of “hiding, delaying, and covering up” legitimate public grievances has been harshly criticized by officials within the CPD, who characterize these methods as being overly reactive and likely to engender or exacerbate public opinion crises.\textsuperscript{75} For instance, local officials’ tone-deaf approach to citizens’ concerns is a prime contributing factor to high-profile mass incidents such as the 2011 anticorruption protests that occurred in Guangdong Province and the 2022 anti-lockdown protests during the COVID-19 pandemic.\textsuperscript{76}

**PART 2: METHODS AND TECHNOLOGIES THAT UNDERPIN CHINA’S CENSORSHIP APPARATUS**

Untangling the Web of China’s Censorship Apparatus

Within the PRC, there is no single body tasked with implementing censorship. Rather, control of China’s information environment is managed by a set of institutions that have parallel and sometimes overlapping authorities. The following section provides a top-down overview of this apparatus and its functions, starting with Party leadership and going down to the grassroots level.

CCP priorities and strategies for implementing censorship are dictated by the Central Party Committee (中国共产党中央委员会), which operates with General Secretary Xi as its decision-

* The report placed special emphasis on the joint nature of information control work in China, arguing that it is a “systemic project” (一项系统工程) that necessitates the cooperation of multiple Party-state departments and agencies.

† By way of example, internet commentary work undertaken by most Beijing universities is done by faculty supported by a much smaller number of students.
making “core” (核心).*  

CCP leadership uses two main instruments to construct policies for information control: the Central Leading Small Group (LSG) for Propaganda, Ideological, and Cultural Work (中央宣传思想领导小组) and the Central Cyberspace Affair Commission (中央网络安全和信息化委员会).†  

These organizations are respectively tasked with overseeing propaganda work and governing the internet.‡  

Both the Propaganda LSG and Cyberspace Commission formulate policies and guidelines that are then executed by central-level bureaucratic organizations as well as lower-echelon Party committees at the provincial, prefectural, county, and grassroots levels.§  

As with other Party functions, the Central Party Committee does not micromanage lower-level Party committees but rather imparts guidance for those organizations. These committees, in turn, formulate detailed action plans for Party and state institutions to enact within their areas of authority.  

In practice, daily censorship tasks are undertaken by cross-cutting bureaucratic organizations that are loosely organized as “systems” or xitong (系统).  

There are two xitong that undertake the bulk of censorship work in China: one for traditional media and one for online content. The first is the propaganda work system (宣传工作系统), which oversees content produced by legacy media such as film, radio, newspapers, and television.  

It is primarily overseen by the CCP’s CPD. The second xitong is the network information system (网信系统), which is tasked with “internet content management” (网络信息管理).  

The system is composed of a tripartite or “three-in-one” (三位一体) work system consisting of the CCP’s CAC and two ministries under the State Council—the Ministry of Industry and Information Technology (MIIT) and the MPS—as its primary component functional agencies.  

Of these three bodies, CAC has the chief role in internet censorship and is responsible for internet news management, online information coordination, network emergency management, network information services, and network information research.  

MIIT is responsible for industry management, which entails overseeing the physical infrastructure of China’s internet.  

Finally, the MPS is responsible for network policing work as well as investigating and prosecuting prohibited online speech.  

A simplified diagram illustrating this structure is laid out in Figure 1.

---

* Use of the Party nomenclature term “core” signifies that Xi wields an extremely high degree of authority over Party decision-making. The phrase has historically been used to refer to senior leaders such as Mao Zedong, Deng Xiaoping, and Jiang Zemin, who wielded a high degree of central decision-making authority.

† The LSG previously operated under the name the “Central Propaganda and Ideological Work Leading Small Group” before having its name changed in mid-2023.

‡ The high degree of importance Xi places upon Party control over China’s information environment is reflected in the composition of these leadership groups: Xi himself oversees the Central Cyberspace Affairs Commission, while one of his close affiliates, Cai Qi, oversees the Propaganda LSG.

§ The importance that Party leadership ascribes to internet governance is illustrated by CAC’s role as a combined Party-state bureaucratic body: unlike the MPS and MIIT (which are overseen by the State Council), CAC is administered directly by the Central Party Committee. Moreover, CAC offices at all levels serve as the executive wing or “functional institution” (职能机构) that directly carries out policies formulated by their overseeing Party committee.
On its surface, the CCP’s censorship bureaucracy appears uniform and highly regimented. However, in reality its structure is unevenly developed, with major disparities among various local censorship organs in terms of resourcing and capabilities. To illustrate, county-level propaganda departments (which constitute the Party’s front-line force for enacting censorship) vary significantly in terms of staffing, budget, and internal structure. Depending on locality, these departments retain between ten and 50 employees and have an annual budget of between 10 million and 50 million renminbi (RMB). Crucially, all regional propaganda departments are required by the Party to perform the same information control functions, regardless of the resources they possess. Consequently, many poorer and less populous counties that cannot retain dedicated billets for network monitoring and information control instead rely on “dual-hatted” staff to undertake censorship tasks in addition to their primary work roles. This reality results in a workforce that is spread thin and ill-equipped to fulfill its information control responsibilities. Moreover, while the PRC ostensibly possesses clearly delineated hierarchies and mission sets for Party-state institutions that manage censorship, these institutions often have redundant or overlapping areas of authority. There is a high degree of institutional variability at the local level among Party-state structures that conduct censorship, with many localities lacking codified means for interbureaucratic coordination and information sharing.

---

* Putting these departmental budgets in perspective is difficult because county governments in China generally do not publish comprehensive budgets online but rather publish budgetary statements for their individual departments. However, a good point of comparison can be gleaned from looking at personnel. For instance, while county propaganda departments maintain staffs of between ten and 50 personnel, counties in China have an average population of 500,000 people. Concurrently, provincial-level propaganda departments range in size from 200 to 500 personnel, while the average province population in China is roughly 48 million.

† The specific roles of bureaucratic institutions tasked with censorship are detailed in full in Addendum I of this report.
Technical Mechanisms That Underpin PRC Censorship Practices

Censorship of the PRC’s internet poses an enormous technical challenge. According to the China Internet Network Information Center (CNNIC), as of December 2022 China had 1.07 billion netizens who used the internet to access a broad range of services from instant messaging to online news to live streaming and online gaming. In order to monitor China’s ever-growing and ever-complexifying internet, the CCP has not been dependent on any one solution. Rather, it has relied on overlapping and redundant capabilities and the technology sector’s ability to innovate on the Party’s behalf to maintain its censorship capacity.

In its most rudimentary form, China’s internet censorship involved blocking access to objectionable websites or traffic from blacklisted domains and IP addresses by using software tools that rejected requests for access to banned sites. When this method was first deployed in the 1990s, it was initially an underpowered blunt-force instrument. The censorship software could not handle the volume of traffic coming in and out of the country, so blocking of most sites was intermittent. Moreover, blocking could be evaded with simple techniques like changing IP addresses or using proxy servers. The CCP was eventually able to expand its range of blacklisted sites as its censorship system became more mature to include the privacy protection sites and proxy servers that had been thwarting censorship efforts.

Keyword filtering was the next evolutionary step in China’s censorship toolkit. The filtering system was based on using intrusion detection system (IDS) devices to inspect web traffic at multiple levels, including international data transit gateways, domestic ISPs, and decentralized, local-level routers. The filters used deep packet inspection to look for triggering words or phrases in the destination URL or HTML. If such words or phrases were detected, the router through which the offending packet was trying to pass could issue reset packets to the source and destination IP addresses to reset the connection, effectively blocking access. The system also utilizes data traffic redirection techniques such as DNS hijacking to steer users away from censored sites and toward other IP addresses.

As technology and countermeasures to thwart Chinese censorship have advanced, so too have China’s efforts to keep up. China’s filtering capabilities now include images as well as text. Optical character recognition-based algorithms can filter images with objectionable words or phrases in a text layer, and visual algorithms can block images that match or are similar to blacklisted images. Censorship technology has also become more adept at inspecting and filtering traffic that uses the encrypted https protocol. It has even started to passively censor fully encrypted traffic based on heuristics about how fully encrypted traffic typically appears.

There is no known ubiquitous software platform used by Party-state departments tasked with censorship and public opinion monitoring. For instance, a 2014 analysis conducted by the PLA Nanjing Political College found that there were 104 online public opinion management systems from 93 different companies available in China that had passed “Double Soft” certification. However, despite being produced by different vendors, public opinion monitoring and censorship software remain highly homogenous. Most platforms offer basic functions for information acquisition, public opinion classification display, controversial topic discovery, public opinion briefing, and transmission path analysis based on common support.

* Double Soft certification is an accreditation awarded to software that meets certain requirements laid out by the State Council, such as being domestically produced and in compliance with PRC laws and regulations.
technologies such as web crawlers; metadata extraction tools; text classification, clustering, and automatic summarization tools; and tools for text similarity calculation.\textsuperscript{100}

The Party-state is currently upgrading its online censorship platforms by incorporating recent advances in generative AI, big data analysis, and imagery and voice recognition. For instance, in 2020, researchers affiliated with China’s National Radio and Television Administration filed two patents for “public opinion guidance tools” that used computer vision technology to analyze and extract data from audiovisual media.\textsuperscript{*} Concurrently, entities in China’s academic and private sectors have innovated software aimed at improving the CCP’s ability to proactively censor pockets of online discontent by singling out “clusters” of high-risk activity.\textsuperscript{102} The Party-state is also closely supervising the deployment of commercial AI systems (including large language model chatbots akin to ChatGPT) by drafting technical standards governing their construction and usage.\textsuperscript{103} Consequently, Chinese AI tools such as Baidu’s ERNIE Bot are designed from the ground up to adhere to censorship restrictions and will refuse prompts relating to sensitive topics such as Xinjiang, Tibet, and Xi Jinping’s leadership.\textsuperscript{104}

In addition to the Party organs and state-owned enterprises that enforce censorship capabilities, the CCP has used regulation to co-opt private internet companies into enacting censorship on their commercial platforms under threat of fines or closure. Tencent, for example, filters activity within China on its ubiquitous WeChat chat app from the server side, using algorithms that have been trained in part by content surveillance of non-China-registered accounts.\textsuperscript{105} Even smaller companies, like the operators of video-based social platforms YY and Sina Show, employ data security departments that maintain surveillance and perform automated reviews of content. Their capabilities include voice monitoring that can provide alerts on censored words and image processing that can capture screenshots of random chatrooms at regular intervals to detect prohibited behavior.\textsuperscript{†} \textsuperscript{106}

The decentralization of responsibility for censorship has effectively lightened the burden on the state, but it has also resulted in varying degrees of enforcement. This has long been an issue, but it has been an ongoing challenge for Chinese companies that are trying to capture market share (i.e., attract users) with innovative functionality while also clamping down on social activity to the government’s satisfaction.\textsuperscript{107} The CCP has shown a willingness to shut down services that do not effectively monitor their content, particularly in the popular livestreaming industry, which does not yet have a satisfactory technical solution for monitoring and censoring in real time.\textsuperscript{108} It has also shown no hesitance in going after major companies. For instance, ByteDance’s Neihan Duanzi (内涵段子) app, a social mobile app for jokes, comedic videos, and memes, was abruptly shuttered in 2018 and the company’s founder and CEO was forced to release a public apology in which he accepted responsibility for “not taking the proper measures to improve content supervision.”\textsuperscript{109}

\textbf{The Role of U.S. Technology Products in Constructing China’s Censorship Apparatus}

Although China retains a robust homegrown industry dedicated to producing censorship software, much of the underlying technical infrastructure used in its information control apparatus is built

\textsuperscript{*} Notably, the National Radio and Television Administration is directly subordinate to China’s Central Propaganda Department.

\textsuperscript{†} It bears noting that this vocal and text recognition software is tailored exclusively to Mandarin Chinese. Content creators who use “non-recognized languages,” such as speaking in Cantonese or Uyghur or using scripts such as Tibetan or Mongolian, often have their streams taken down, amounting to de facto censorship of non-Mandarin content within China.
upon U.S. technology and expertise. Historically, the PRC relied heavily on hardware component parts and software sourced from the United States to construct and operate its online censorship apparatus. For instance, during the 2000s, the PRC allegedly used routers, firewalls, and antivirus software from vendors such as Cisco and Symantec to conduct online censorship. During that same period, a number of U.S. technology firms actively cooperated with the Chinese government to restrict sensitive information. For example, prior to their departure from the PRC market space, both Google and Yahoo maintained specialized versions of their search engines that prevented Chinese users from accessing material forbidden by CCP authorities. However, during the 2010s, the relationship between U.S. technology firms and the Party’s censorship apparatus diminished significantly. This phenomenon is largely due to industrial policy enacted under General Secretary Xi, who has declared that key Party-state functions (such as censorship) should not be reliant on foreign-produced technologies. Consequently, many technology contracts issued by the Party-state include provisions that grant preferential treatment to bidders who employ domestically sourced hardware and software. At the same, increased public scrutiny during this period likely played a role in inducing U.S. tech giants to distance themselves from the Chinese government in order to avoid the appearance of complicity with CCP human rights abuses.

At present there is limited evidence to suggest that major U.S. technology companies knowingly aid and abet China’s information control regime by directly providing the Party-state with specialized hardware. Nevertheless, although U.S.-based firms do not manufacture bespoke censorship products for use by the Party-state, many “off-the-shelf” products that are not subject to export restrictions (such as servers, processors, and motherboards) are still widely used by CCP censors. For example, one 2021 study from researchers affiliated with the German Council on Foreign Relations alleges that component parts from Cisco, Dell, HP, IBM, Microsoft, and Oracle are presently used in the MPS’s Golden Shield Project. Additionally, it is likely that the PRC’s censorship apparatus inadvertently benefits from U.S. vendors operating in China, such as Amazon Web Services and Microsoft Azure. While neither company is known to market directly to the CCP, their engagement enables the PRC to build capacity and expertise in fields such as cloud computing, which can be used to store, retrieve, and analyze vast quantities of text, audio and image data and is therefore a crucial input for the Party’s “public opinion guidance” tools.

Despite the PRC’s ongoing drive for industrial self-sufficiency, its censorship apparatus is still reliant on U.S. imports, especially those used in emerging technologies such as AI, machine learning, and big data applications. For instance, many of the platforms that comprise China’s “next generation” of AI-enabled public opinion guidance systems rely on imported hardware such as graphics processing units (GPUs) to provide their computing power. Concurrently, PRC firms that produce censorship and surveillance technology have allegedly instrumentalized partnerships with companies such as Google and IBM to refine and improve their products. In many cases, foreign companies working in China deliberately conceal their connections to China’s

---

* The opaque nature of the CCP’s censorship bureaucracy makes it difficult to determine the exact extent to which U.S. products are still used in PRC censorship systems. However, it is probable that the proportion is significant, given that many Party-state systems still rely on legacy information technology systems that use Western component parts.

† Although originally designed as a component for video game systems, GPUs also provide an effective solution for powering AI systems. Their design is optimized for conducting parallel computation, which is necessary to effectively train machine learning models.
security services, which complicates due diligence to avoid contributing to the PRC’s censorship apparatus.

**Standard Operating Practices for Censorship**

On paper, the PRC boasts a formidable array of bureaucratic, legal, and technical tools it can use for the purpose of internet censorship. However, these tools are not employed uniformly within China due to resourcing and structural discrepancies between different local governments. The vast majority of day-to-day censorship and public opinion work is overseen by lower-level Party-state bureaucracies that have their own distinct standard operating procedures, normative regulations, and technology platforms. Consequently, priorities for censorship and the stringency with which content control measures are enforced varies depending on locality. Despite this variability, there are a few core mission sets shared among Party-state institutions at all levels that collectively illustrate the standard operating procedures the CCP uses to control China’s information environment.

**Public Opinion Monitoring, Analysis, and Response**

Public opinion monitoring capabilities form the bedrock for China’s censorship regime, enabling the CCP to preemptively identify and suppress potentially harmful information. Across all levels of government, Party-state institutions of all stripes maintain their own internal public opinion monitoring capabilities as well as access to shared databases of local public opinion information. Collection of this material appears to be primarily aimed at controlling “online public opinion incidents,” managing online discussion hot spots, and identifying “black swans and gray rhinos” that have the potential to undermine regime stability or precipitate real-world “mass incidents.”

Public opinion monitoring within China is undertaken by a patchwork system of CAC branch offices, propaganda department branch offices, miscellaneous other bureaucratic offices, news organizations, universities, and for-profit companies. Given the varied nature of these entities, there is no unified methodology or toolset used to conduct public opinion monitoring. However, in general, these institutions use a combination of web scraping, advanced search engine analysis, data mining, and human assessments to forecast trends in public opinion. Public opinion monitoring is generally carried out 24 hours a day by tracking relevant microblogging platforms, forum communities, industry portals, local sites, and news sites. After collection, these data are structured, categorized, and stored for usage (see Figure 2).
After public opinion data are processed, they are then assessed by human analysts tasked with flagging emergent negative trends. Depending on locality, this work is overseen by either full-time professional public opinion analysts or by dual-hatted department employees.* These analysts work collectively to assess the severity of emerging public opinion trends and classify them according to a predetermined framework.† In cases where public opinion trends are deemed to pose imminent danger to social stability, the monitoring entity relays its findings to its supervising work unit, which will coordinate with other relevant departments such as the MPS to implement a response.‡ A diagram depicting how various Party-state organs coordinate censorship messaging and response during these “public opinion emergencies” can be found in Figure 3.

* Job requirements for public opinion analysts tend to vary, but in general they prioritize high degrees of education, political reliability, and technical acumen. For instance, one job posting for a public opinion analyst job listed conditions for employment as including being a member of the CCP, having a graduate degree from an accredited college or university, and having extensive familiarity with computers and network applications. The job posting went on to stipulate that ideal applicants would be under 35 years old and should be willing to work night shifts.

† By way of example, the Fuzhou Municipal Propaganda Department classifies public opinion incidents according to a four-tiered system: “mild crises” (轻度危机) which can be remediated using standard warning measures (一般警示措施); “moderate crises” (中度危机), which require special warning measures (特别警示措施); “high-level crises” (高度危机), which require extreme warning measures (危险警示措施); and “deep crises” (深度危机), which require emergency action (紧急行动措施).

‡ Response measures include punishments ranging from warnings from law enforcement to detention and incarceration by the MPS. Notably, the threshold for speech and behaviors deemed harmful to public order is often arbitrary and poorly defined. For instance, Chinese citizens have been detained for seemingly minor infractions such as insulting police officers and members of the PLA.
## Blocking and Deleting Harmful Material

The most direct instrument the Party-state uses to censor online material consists of directly deleting or restricting objectionable information, a process known in Party nomenclature as “dredging and blocking” (疏堵结合). This aspect of network supervision and management work is done directly by local CAC and propaganda branch offices via takedown requests to web service providers or, more commonly, enacted preemptively by internet platforms seeking to avoid legal censure. In some cases, these platforms subcontract moderation efforts to third parties who monitor and delete harmful materials on their behalf. In the past, network supervisory tasks were undertaken primarily by human moderators who would monitor their platform for forbidden content. However, recent advances in computer vision, natural language processing, and AI have enabled much of this work to be automated by network monitoring technology platforms.

While post deletion is certainly the most visible part of China’s online censorship apparatus, it constitutes only a fraction of Party censorship efforts. Indeed, while many Party scholars acknowledge that directly censoring harmful information is an indispensable function of information control, some caution against the overzealous employment of dredging and blocking measures. According to this line of thinking, post deletion is a blunt instrument that should be used sparingly to avoid inciting public opinion backlash or allowing legitimate grievances to fester. However, recent scholarship has demonstrated that many local Party-state leaders still heavily

---

* The lack of transparency exhibited by both Party-state censorship institutions and Chinese social media companies makes it difficult to quantitatively assess the percentage of content moderation that uses “dredging and blocking” methods compared to other methods, such as positive publicity. However, guidance issued by Party-state censorship authorities and data analysis conducted by Western scholars both suggest that content deletion is used sparingly and constitutes only a small proportion of the CCP’s overall information control mission.
employ dredging and blocking content moderation methods due to their belief that suppressing
dissent will facilitate faster promotion or additional resourcing from the Party center.\textsuperscript{138}

**Focusing on Positive Publicity**

As discussed in Section 1, the main instrument the PRC uses to aid censorship efforts is the
employment of public opinion guidance. This entails saturating China’s information space with
material that “promotes positive energy and suppresses negative factors” as well as conducting
online outreach and engagement with ordinary netizens.\textsuperscript{139} Accordingly, Party propaganda organs
at all levels are involved in producing content that encourages the “consolidation of the shared
ideological foundation of the CCP and Chinese people.”\textsuperscript{140} The need for this mission set is
especially acute during times of crisis or upheaval, with Party commentators noting that having a
prompt, unified, and omnipresent response to “hot topics” is necessary to forestall “false or
distorted information” from gaining purchase among China’s citizens.\textsuperscript{141} As a result, the Party has
undertaken a concerted effort to focus its propaganda work on platforms with the highest degree
of reach among China’s citizens, such as microblogging and video hosting services.\textsuperscript{142}

In addition to producing content for consumption by Chinese netizens, Party organizations at all
levels also employ online commentators to engage directly with Chinese netizens.\textsuperscript{143} These
practices have been characterized by Party officials as an updated version of Party “mass line” (群
众路线) work and are established by local government departments or by grassroots institutions
such as private companies and news organizations.\textsuperscript{144} Universities tend to be especially active in
organizing online commentary teams, which are composed of school teaching and administrative
staff as well as student volunteers. For instance, a 2016 survey conducted by members of the
Propaganda Department of the China Youth University of Political Science (中国青年政治学院
党委宣传部) found that 67 percent of universities in Beijing had established teams of online
commentators who conducted public opinion work online.\textsuperscript{145} In other cases, public opinion teams
are formed on an ad hoc basis, with teams from multiple work units grouped together by their
supervising propaganda committee aided by “grassroots public opinion leaders” (草根意见领
袖).\textsuperscript{146} Notably, responsibility for managing these teams seems to be fractured and irregular. While
the preponderance of internet commentary teams appear to be overseen by their affiliate Party
propaganda department, some are supervised directly by their own work unit or university
department, with no standardized reporting or oversight mechanisms.\textsuperscript{147}

While there is a high degree of variability in the composition and reporting structure of network
commentary teams, there is near-uniformity in how these groups operate on a day-to-day basis.\textsuperscript{†}
Team members are selected for their ideological and political reliability, acumen with computer
technology, strong writing and reasoning skills, and familiarity with their work unit’s relevant
bylaws and regulations.\textsuperscript{148} In most cases, CCP membership is desired but is not a requirement for
joining these teams.\textsuperscript{149} Daily responsibilities for team members include:\textsuperscript{150}

- Monitoring popular internet platforms and web forums for content and trends relevant to
  their area of responsibility.

\textsuperscript{*} Notably, network commentary groups are also organized by a range of local Party-state institutions that are not directly involved
in propaganda work, such as veterans’ associations and housing authorities.

\textsuperscript{†} Specifically, multiple job postings from institutions such as universities, social service institutions, and regional Party committees
all include the exact same language describing the roles and responsibilities of internet commentary teams.
• Reposting positive news and content related to their parent work unit.
• Participating in online discussions related to their work unit, with a special focus on guiding public opinion on “hot-button issues and thorny discussions, resolving grievances, and correcting ideological misunderstandings.”
• Upholding “online ideological security” (网络意识形态安全) by “refuting erroneous views” and “exposing false information.”

Moreover, in addition to these day-to-day tasks, these groups are also responsible for promptly reporting to their overseeing propaganda department or work unit to provide information support in the event of emergencies or mass incidents.151

China’s Censorship Apparatus in Action: The Qinglang Campaign

An illustrative example of the Party-state’s approach to managing online public opinion can be observed in the “Qinglang” (清朗) campaign that has been ongoing since 2021. The campaign was launched by CAC with the initial purpose of “rectifying the chaos” caused by overactive online celebrity fan communities but has since expanded in scope to include more generalized measures aimed at dictating the behavior of Chinese netizens. As such, its stated purpose of “fostering a positive online environment” does not merely apply to suppressing platforms and accounts that spread illegal information but also extends to policing behaviors deemed to have a “harmful social impact.”152 It has focused particularly on media consumed by China’s youth, such as video games, livestreaming services, and short video platforms like Douyin (the PRC’s domestic version of TikTok).153 This has led CAC to release stricter guidelines governing the content displayed online, limiting the amount of time minors can spend on gaming platforms and livestreaming services, and “rectifying” the algorithms used to suggest content to users.154 Although the Qinglang campaign’s notional goal is to crack down on antisocial online behaviors, in practice it has been used to severely limit the freedom of expression of many Chinese netizens.155 The Party’s definition of “harmful behavior” is such that it extends to suppressing behavior deemed deviant or harmful to public morality. For instance, the campaign has targeted LGBTQI+ groups for suppression on the basis that they promote social behaviors and attitudes that are harmful to the “national spirit.”156 Moreover, the campaign has also sought to suppress content and commentary that foster negative attitudes about prevailing social issues such as poverty and social inequity.157

PART 3: GOING GLOBAL: CHINESE CENSORSHIP PRACTICES ABROAD

Although the CCP’s censorship apparatus is primarily domestically focused, its influence extends far beyond China’s borders. Indeed, the principles and techniques used by the PRC for internal information control directly inform its approaches to shaping the thought processes of foreign audiences. As China has risen to become a central player within global economic and diplomatic affairs, it has increasingly sought to stifle the spread of information abroad that is deemed harmful to the Party and the PRC’s national interests, such as portrayals of CCP human rights abuses and narratives that challenge China’s claimed sovereignty over Taiwan. These efforts have reached new heights under General Secretary Xi, who has directed the Party-state to expand its capacity to

* Antisocial behaviors defined by CAC include cyberbullying, rumor-spreading, trolling, and “doxxing” of third parties. In internet parlance, the term “doxxing” refers to the unauthorized disclosure of personal information such as a real name, address, or phone number.
conduct “international public opinion guidance” (国际舆论引导力) and to more aggressively combat “anti-China” narratives abroad.* 158 Concurrently, China has intensified its longstanding campaign to reshape the norms, regulations, and platforms that govern and facilitate transnational information exchanges, with the goal of creating an international communications system more attuned to the preferences of PRC leadership.

Strategic Background: Competing in the Global Information Environment

The strategic rationales that motivate China’s foreign censorship efforts share many commonalities with those that guide the domestic information control regime. In both cases, the Party’s information control strategy is premised on the notion that the PRC is under ideological siege from abroad and that steps must be taken to counter “hostile foreign forces” that seek to undermine China’s political system and curtail its development. These concerns have taken on a new imperative with the rise of networked communications systems, such as the internet, that enable the spread of information unconstrained by national boundaries. 159 Under this now global communications paradigm, even information circulated on foreign information platforms has the potential to adversely affect domestic stability within the PRC.† 160 However, while the Party is acutely aware of the potential harms posed by unrestricted global information flows, it also recognizes that these technologies have the potential to greatly benefit China. For instance, the communicative potential of the internet better enables China to raise its soft power profile by winning over foreign audiences, and it brings material benefits such as increased access to international commercial and scientific information exchanges. 161 Consequently, the PRC’s international communications strategy seeks to maximize the economic and diplomatic benefits of global engagement while also placing an a priori emphasis on safeguarding the domestic interests of the Party.

PRC leadership regards international public opinion guidance as a “non-traditional national security” (非传统国家安全) mission that is vital for ensuring China’s continued prosperity and social stability.162 According to this line of thinking, maintaining a positive image among foreign audiences enables the PRC to maximize its freedom of action in pursuing its diplomatic objectives, and it blunts rhetorical attacks that “slander China and undermine its continued development.”163 As such, the Party under Xi Jinping has invested extensively in cultivating China’s international “discourse power” (话语权), which is broadly defined as the ability to build global support for the CCP’s political and normative preferences.‡ 164 To this end, the Party has built up an extensive institutional apparatus devoted to influencing foreign audiences. This bureaucratic network includes institutions that conduct overt messaging such as the Propaganda Department’s State Council Information Office, elements that conduct semi-covert influence cultivation such as the United Front Work Department, and parts of the PLA and Ministry of State Security that conduct

---

* The PRC’s ongoing drive to expand international censorship has had a particularly severe impact on freedom of expression among members of the Chinese diaspora community. Within the past ten years, the Party-state has taken steps to more heavily monitor and police posts made by Chinese expatriates on social media apps such as WeChat and Weibo. This undertaking has coincided with expanded PRC extraterritorial surveillance and intimidation of its citizens living abroad, such as monitoring of Chinese international students, to ensure that they do not fall prey to “ideological contagions.”
† For example, several Party sources pointed to the 2015 Tianjin chemical explosion as a key example of international news coverage undermining CCP-approved narratives, which served as a catalyst for domestic civil unrest.
‡ The term can also be translated as “right to speak.”
covert information campaigns. Collectively, these groups have a broad mandate to pursue activities that advance pro-China narratives, including censorship tasks such as information suppression.

China’s international public opinion guidance strategy is colored by the notion that it is inherently disadvantaged by the structure of the global information space. According to this view, the United States was the primary architect of the platforms and forums that facilitate global communications and maintains a monopoly on the mainstream media platforms and information sources that shape public opinion. Correspondingly, the PRC is dismissive of U.S. claims to be a neutral steward of the global communications order, believing instead that the West uses its hold over shared network infrastructure to foment unrest in rival regimes through occurrences such as “color revolutions.” Although Party leadership believes it insulated itself from this threat by pursuing policies such as an autarkic approach to internet development, it regards the current configuration of the global information space as being a long-term threat to its own development and security.

While the PRC views itself as disadvantaged in current global information competition, it believes it has a unique opportunity to reverse its current position. This notion is born from the assessment that the international order is in the midst of “great changes unseen in a century” that present China with a “rare opportunity to catch up with established powers.” These changes are driven by emergent “Fourth Industrial Revolution” technologies such as AI and machine learning that will upend existing means of production and communication. In the information sphere, these changes are expected to obviate traditional mediums of news distribution and cultural consumption, as emerging communications mechanisms such as mobile platforms, augmented reality, and algorithmically driven content consumption become more pervasive. This period of strategic opening is further widened by what the PRC perceives to be deepening internal contradictions within the international order of Western liberalism. Accordingly, China has implemented a multipronged strategy to wrest control of the global communications commons and increase its own degree of agenda-setting power. Broadly speaking, this undertaking has proceeded along two main lines of effort. First, the PRC is challenging the United States’ messaging on existing platforms by engaging in international public opinion guidance under the aegis of “strategic communications” (战略传播). Second, China has sought to build out a parallel infrastructure of social media platforms and global internet norms that will produce a more friendly international environment for China in the long run.

Examining China’s International Censorship Practices

Implementing international public opinion guidance poses a unique challenge for the CCP. This challenge results from the fact that the PRC cannot rely on the broad-reaching legal and regulatory authorities that form the backbone of its internal censorship apparatus. Moreover, the bureaucratic apparatus that China uses for international public opinion guidance is less pervasive and less well-developed than its domestic counterpart. As such, Chinese foreign public opinion guidance work is often hampered by a lack of resourcing and insufficient understanding of its target audience.

---

* In many cases, these accusations verge on being outright conspiratorial. For instance, a common thread of thought among Party academicians posits that the content of U.S. and Western media is dictated by the “hidden agenda of specific interest groups,” such as major holders of capital.

† According to General Secretary Xi, the five core objectives for strategic communications work are: strengthening China’s communications influence internationally, increasing China’s cultural appeal, improving China’s image abroad, raising China’s level of discourse and persuasive power, and providing the capability for China to guide international public opinion.
To compensate for these shortcomings, the PRC employs a number of “quasi-censorship” tactics that mimic those used for internal censorship. These efforts are guided by the assessment that public dynamics are broadly similar worldwide regardless of culture or locality.\(^1\)

Hence, China’s foreign propaganda work system employs domestic information control tactics, such as enacting punitive measures to deter the circulation of certain types of speech, as well as saturation tactics aimed at drowning out narratives the CCP deems to be objectionable. Concurrently, the Party undertakes a triage approach to censorship abroad, focusing on combating narratives that directly threaten the CCP or core PRC national interests.\(^1\)

### Inducing Self-Censorship among Foreign Companies and Individuals

One key tool China employs for external information control is economic coercion. As the world’s second-largest economy, the PRC enjoys significant leverage over entities seeking to trade with or do business in China. It uses this power to withhold market access and exert economic pressure on companies and individuals that transgress Beijing’s redlines. In this respect, economic retaliation is a disciplinary measure the Party-state uses in lieu of de jure legal authority to police speech abroad and induce foreign entities to self-censor.\(^1\) While economic coercion has long been a mainstay of the PRC’s information control toolkit, the practice has been used with increasing regularity under General Secretary Xi’s leadership.\(^1\) Over the past decade, China has levied economic punishments against more than 120 individual companies deemed to support speech that violates Beijing’s “core interests.”\(^1\) In some cases, economic pressure serves as a punitive measure against companies for their official statements or to coerce them into pulling products from the market.\(^1\) For instance, in 2018, CAC ordered the Marriott hotel chain’s website to be blocked for a week in response to the company publishing a customer survey that listed Taiwan, Hong Kong, and Macau as countries distinct from the PRC.\(^1\) That same year, the Gap clothing company was forced to issue an apology for selling clothing featuring a map of China that omitted Taiwan and southern Tibet.\(^1\) At other times, PRC economic pressure has aimed to discipline firms for opinions expressed by individual employees. Many of these cases have targeted high-profile figures in the sports and entertainment industry, such as in 2019, when China suspended broadcasts of NBA games involving the Houston Rockets after the team’s manager made comments supporting the prodemocracy movement in Hong Kong.\(^1\) These information control efforts have also extended into comparatively niche subcultures such as e-sports and virtual content creation, where distributor companies have faced economic repercussions due to individual streamers and competitors making comments deemed harmful by Beijing.\(^1\)

Another core mechanism China uses to enact censorship abroad is by restricting in-country access to scholars and journalists who make statements or conduct research the Party deems problematic. The PRC has long made use of travel bans to punish individuals who “hurt the feelings of the Chinese people, which have been meted out with varying degrees of regularity depending on China’s internal political environment.”\(^1\) However, under General Secretary Xi, the PRC has broadened the parameters of topics it deems to be politically sensitive and has more stringently enforced punishments on researchers who cover “harmful” topics.\(^1\) As a result, foreign

---

* To illustrate, survey studies conducted by institutions such as the China Institute of International Studies (a think tank affiliated with the PRC’s Ministry of Foreign Affairs) note that Chinese foreign influence organs are frequently undermined by budgetary shortfalls and a lack of subject matter experts.

† In particular, sources assess that the group psychological dynamics that drive the formation of public opinion remain the same regardless of circumstance. These dynamics include the propensity for information to spread via “group contagion” as well as collective dynamics within public opinion that render populations vulnerable to being “controlled, exploited, and manipulated.”
journalists and scholars working in China have been forced to navigate an increasingly hostile bureaucratic environment and have been more frequently subjected to retaliatory measures ranging from harassment to deportation.\textsuperscript{188} Party-state intimidation has driven a significant decline in foreign journalists operating in China, fueled by additional hurdles imposed by the COVID-19 pandemic. For instance, a 2023 survey conducted by the Foreign Correspondents’ Club of China found that 56 percent of journalists working in China had their work “obstructed at least once” by government officials, while 38 percent reported having their sources harassed or detained.\textsuperscript{189} Looming threats of expulsion or visa denial are especially acute for academics whose professional livelihoods are dependent on the ability to conduct in-country research.\textsuperscript{190} The resulting chilling effect has had deleterious consequences for the field of China studies, with many researchers being pressured to either self-censor and restrict their focus to inoffensive subject areas or to forgo conducting field work entirely.\textsuperscript{* 191}

Using Information Operations as a Mechanism for Censorship

In addition to enacting censorship through deterrence, the PRC is also pursuing measures to directly shape the prevailing content and narratives espoused by foreign audiences. This practice, which is often referred to by PRC scholars as “borrowing a boat to go out to sea,” entails using foreign platforms to spread narratives sympathetic to China while also drowning out voices that spread “harmful information.”\textsuperscript{192} Crucially, the PRC regards these measures as being inherently defensive in nature and necessary to combat the spread of Western “computational propaganda” (计算宣传) that seeks to poison foreign audiences against China.\textsuperscript{† 193} In undertaking this mission, PRC tactics closely mirror those used for domestic information control, focusing on both spreading “positive publicity” on topics related to China and using information saturation tactics to obscure narratives deemed to be harmful to PRC core interests.

The PRC’s direct international public guidance methods can be grouped into two broad categories: overt and covert. Overt work entails the production and distribution of content that is “legitimate” in the sense that it is produced by real people, distributed legally, and attributable to the PRC or its proxies.\textsuperscript{‡ 194} This material is spread on popular platforms such as X (formerly Twitter), YouTube, and Facebook and seeks to directly engage foreign audiences with the goal of spreading positive sentiment and countering narratives that “maliciously slander” (恶意诋毁) China.\textsuperscript{195} As such, these channels conduct both “day-to-day” work, such as promoting sympathetic narratives about sensitive topics like China’s governance practice in Xinjiang, as well as “emergency response” work that seeks to proactively manage international public opinion during times of crisis.\textsuperscript{196} Generally speaking, overt international public opinion guidance work is conducted by central Party-state organs such as state-run media and the Propaganda Department’s State Council

---

\textsuperscript{*} To illustrate, a 2018 study published in \textit{China Quarterly} found that 70 percent of China-focused scholars agreed with the statement that “self-censorship is a problem in the field of academic China studies.” The same study found that concerns over political sensitivity induced 48 percent of respondents to adapt their project description, 25 percent to change their research focus, and 15 percent to discontinue their research altogether.

\textsuperscript{†} Indeed, a common notion shared by many Party and scholarly sources is that international popular opposition to China’s policies on issues such as Taiwan independence and its governance of Xinjiang and Tibet do not arise organically but rather are fomented by algorithmic manipulation and botnets established by hostile Western governments like the United States.

\textsuperscript{‡} Notably, the sourcing of certain types of overt propaganda is not immediately clear. For instance, China’s Propaganda Department bankrolls the production of content from online “influencers” who do not disclose their connections to the Party-state.
Information Office.* In recent years, however, PRC-based private companies have also begun to run reputation laundering campaigns that use similar messaging and tactics to those employed by their state counterparts.† For instance, companies such as fashion retailer Shein and technology conglomerate Huawei have sought to diffuse international criticism by inviting Western influencers on all-expense-paid trips to China, with the understanding that those individuals will make content that is sympathetic to their hosts.‡

Covert international public opinion guidance work refers to the use of surreptitious measures designed to create artificial social consensus and drown out certain types of information. This entails using tactics such as targeted harassment, algorithmic manipulation, and botnet accounts to obfuscate or muddle discussions on Western social media platforms about issues the PRC government deems sensitive. Given the secretive and politically sensitive nature of this work, covert public opinion manipulation is undertaken either by China’s Ministry of State Security or by elements of the PLA that specialize in information operation. In some cases, these tactics are used to supplement the persuasive potential of overt propaganda efforts, such as in 2019, when China used botnet accounts to attack prodemocracy protestors in Hong Kong and give the false impression of widespread support for the government. However, these measures appear to be principally aimed at disrupting the coalescence of online narratives that are harmful to China through tactics such as hijacking popular hashtags and impersonating public figures who are critical of the PRC.§ Notably, China’s intelligence services are also investing heavily in improving their technological capacity to “guide” international public opinion by leveraging emergent technologies such as generative AI. Consequently, China’s ability to manipulate foreign audiences may pose an increasingly acute threat to the global information commons.

Making the World Safe for Autocracy: Exporting China’s Censorship Model

Concurrent to its international public opinion guidance efforts, China is also engaged in a project of reshaping the norms, platforms, and regulations that facilitate international communication. It seeks to create an “ideologically multi-polar world” that denies the United States’ and its allies’ agenda-setting powers within the realm of international public opinion. This undertaking has proceeded along three lines of effort. First, the PRC is fostering the development of state-owned and private communications platforms to compete with those operated by the West. Second, the PRC government is expanding bilateral engagements with other authoritarian regimes to share best practices for censorship and information control. Finally, China is seeking to upend the current model of internet governance through intergovernmental organizations such as the International Telecommunications Union (ITU).

* Additionally, provincial and prefectural city propaganda offices also undertake foreign propaganda work, as do some state-owned enterprises such as China Ocean Shipping Company (COSCO).
† In particular, these campaigns focus on courting “big-V” influencers who are known to have wide audiences outside of China.
‡ The degree to which these efforts are coordinated with China’s propaganda organs is unclear. However, at the very least it seems likely that the Party-state is aware of and approves of these undertakings, given the high international profile of the companies and the fact that entry visas were granted to the influencers in question.
§ To give a recent example, in 2022, PRC influence operators undertook a campaign to impersonate the popular “Intrusion Truth” cyber threat intelligence blog on social media. The operation appears to have had the goal of deflecting scrutiny away from China’s alleged hacking campaigns by implicating the United States. Moreover, as the first case study of this report will demonstrate, hashtag hijacking and information saturation were both tools the CCP relied upon heavily to disrupt criticism of its handling of the COVID-19 pandemic.
Building a Parallel Media Environment

The PRC has invested heavily in building up news and content dissemination platforms in order to combat U.S. “cultural imperialism and expand its available avenues for conducting international public opinion struggle.” To support this effort, China has increased resourcing for “flagship international propaganda” media institutions such as Xinhua, China Global Television Network (CGTN), and Phoenix TV. To maximize the global market share of these platforms, China has focused the bulk of its attention on cultivating audiences in the “global information periphery” such as Africa and Southeast Asia through programs like the Belt and Road Initiative. This strategy rests on the notion that public attitudes on China within these areas are more malleable and thus more likely to accept PRC narratives. Accordingly, providing easily accessible news platforms (often free of charge) is regarded by the CCP as a low-cost and effective means of winning over foreign audiences who do not currently hold strong views toward China.

In addition to expanding its legacy media offerings, the PRC has also promoted the spread of homegrown internet and social media platforms. Foremost among these is the short video app TikTok, which is owned and operated by the company ByteDance Ltd. Although TikTok is not the only Chinese-developed app to attain widespread usage in the West, it is the first social media platform to gain widespread adherence among non-Chinese-speaking audiences. As such, its success has been celebrated by the Party-state as heralding the end of the United States’ monopoly over global digital culture. However, while many within the Party are sanguine about the geopolitical implications of TikTok’s success, there are disagreements about the degree to which the app should be instrumentalized to further CCP political aims. For instance, within intra-Party literature, some voices advocate for mandating the implementation of content screening and algorithmic optimization in order to promote content that evangelizes China’s culture as well as its economic and political systems. Other voices caution that taking such heavy-handed measures is liable to result in backlash and that the Party should instead endorse a laissez-faire approach designed to passively improve China’s global image. This latter strategy appears to guide TikTok’s current content moderation strategy, which adheres to a strategy of “depolarization” and “localization” that seeks to downplay politically controversial speech and demobilize populist sentiment.

Sharing Best Practices for Censorship

The PRC plays a pivotal role in enabling autocratic regimes worldwide to conduct their own forms of censorship by promoting the spread of technologies and governance practices used to enact censorship. Although the Party does not espouse a specific “China model” of information governance that it seeks to export abroad, it nevertheless looks to normalize authoritarian

---

* Notably, the PRC’s expansion of its foreign-language media offerings has been accompanied by an ongoing drive by its United Front Work Department to acquire, co-opt, or subvert diaspora Chinese-language media outlets, with the goal of aligning their messaging with the preferences of the CCP.

† TikTok serves as the international counterpart of the Douyin (抖音) short video app. While the two versions share the same interface, there are important distinctions between the two. For instance, content on Douyin is more heavily regulated, and the app places special usage restrictions on users, such as minors.

‡ Unlike state media organizations, ByteDance is a private company and thus does not operate as a formal extension of the Chinese government. Nevertheless, the Party-state holds a great deal of sway over its behavior by virtue of the fact that it holds “golden shares” that grant the CCP representation on the company’s board of directors. Moreover, despite being legally incorporated in the Cayman Islands, the majority of ByteDance’s day-to-day operations take place in China, thus rendering it subject to PRC internet laws and regulations.
approaches to government in order to legitimize its own political system. As a result, it is actively engaged in providing other authoritarian governments with the tools and expertise necessary to conduct more effective state repression.

The first way China exports censorship is by sponsoring and promoting the commercial sale of technologies that facilitate state repression. Generally, censorship platforms are not sold as standalone tools but rather as part of a broader suite of surveillance technologies such as video monitoring and facial recognition software. For instance, firms like Hikvision, Yitu, and CloudWalk produce hardware and software components that comprise internal control mechanisms such as “comprehensive information management platforms” (综治信息平台) used by provincial and local governments in China.† These firms collectively hold a dominant global market share in the field of surveillance applications, including cloud computing and AI-enabled platforms that aid state censorship.‡ As a result, they play a key role in fulfilling market demand posed by authoritarian regimes that have aspirations for more internal control but lack the strong homegrown technology sectors necessary to realize their vision.

In addition to facilitating the global spread of censorship technologies, the PRC also provides support and advice to authoritarian regimes on how best to implement stability maintenance and information control. These exchanges are undertaken bilaterally and through development programs such as the Digital Silk Road. For example, Chinese network infrastructure investments in countries like Laos, Pakistan, and Sri Lanka have been accompanied by cooperative ventures aimed at sharing best practices for information control in cyberspace such as intergovernmental dialogs and joint police training. There is also strong circumstantial evidence indicating that PRC-backed consultation was instrumental in shaping network content laws issued by countries such as Vietnam, Tanzania, and Uganda.‡ Moreover, China’s Belt and Road Initiative has also served as a vector for China to evangelize its model of internet content management to multilateral institutions such as ASEAN. Specifically, the PRC uses its dialogues with these groups to tout the developmental benefits of its information control apparatus and to encourage other governments to adopt similar measures.

Remaking Global Internet Governance

The PRC’s most ambitious project for normalizing censorship abroad is its campaign to realign and restructure the institutions that administer the underlying architecture of the global internet. China’s leadership has long expressed dissatisfaction with the present “multistakeholder” model for internet governance, asserting that it grants disproportionate agenda-setting power to the United

---

* Indeed, the PRC’s censorship model is reliant on a number of factors that are not easily replicable by other states, such as its unique IXP management system, the high degree of penetration the Party enjoys within civil society, and the presence of a robust science and technology sector to support the development of censorship platforms.

† Comprehensive information management platforms appear to be used most pervasively in “high-risk” areas in the PRC such as Tibet and Xinjiang, although they are also employed across many other localities. The platforms are operated by local governments and incorporate data inputs from civilian bureaucratic institutions as well as elements of the MPS and People’s Armed Police. They also feature mechanisms to collect voluntary data submissions from citizens through the use of mobile applications such as the “Peaceful Tibet” (平安西藏) app.

‡ The exact proceedings of these meetings are not publicly available, making it impossible to conclusively draw a direct causal connection between these engagements and the content of the enacted legislation. However, in all three cases, the structure and purview of the laws that were passed closely align with China’s own guidelines, such as the 2017 Cybersecurity Law.
Accordingly, the PRC is actively promoting an alternative multilateral internet governance model based on the concept of “cyber sovereignty” (网络主权). Such a model would privilege the role of nation-states in formulating policy while shutting out nongovernmental organizations, private companies, and civil society advocates. It would also internationally codify Beijing’s preferred definitions of “information security” (信息安全) and “mutual non-interference in internal affairs,” which would inhibit the free movement of information and data across borders and allow authoritarian states to more easily conduct censorship.

The PRC’s strategy for shaping cyberspace governance—premised on controlling the evolution of the internet’s physical infrastructure—is key to cultivating diplomatic and political influence. As such, China has partnered with like-minded authoritarian states such as Russia and Iran in order to achieve institutional capture within the intergovernmental organizations that regulate the global internet, such as the ITU. China made considerable inroads toward achieving this goal throughout the 2010s. During this period, Beijing was able to secure a number of key appointments for its preferred candidates within the ITU, culminating with the election of Houlin Zhao to leadership of the organization in 2015. The PRC leveraged this representation to realize a number of objectives, such as shepherding through the adoption of regulatory standards for emergent technologies like 5G, smart cities, and the Internet of Things. However, China’s domineering approach to ITU governance engendered significant pushback, resulting in an erosion of its representation in the body during its most recent election in 2022.

Although China has recently suffered setbacks within the ITU, it remains deeply committed to using that body as an instrument to promote its preferred models of information control. This drive is presently manifesting in the PRC’s ongoing efforts to influence standards governing emergent information technologies it deems to be particularly destabilizing, such as generative AI. Moreover, China is continuing to pursue its long-term project of diminishing the legitimacy of the current multistakeholder approach to cyberspace governance through proposed measures such as divesting the Internet Corporation for Assigned Domain Names and Numbers (ICANN) of its internet oversight authorities and transferring those powers to the ITU.

**PART 4: CASE STUDIES**

To illustrate the strengths and limitations of China’s information control apparatus, this section presents three case studies that examine the CCP’s censorship bureaucracy in action. Case study one focuses on the Party-state’s response to the COVID-19 pandemic, demonstrating how the PRC utilizes censorship as an emergency response tool. The study reveals the flexibility and adaptability of Party-state censorship, as evidenced by its evolving messaging strategy and combined use of

---

* The “multistakeholder” model refers to a bottom-up approach for internet governance in which subject matter experts from governments, the private sector, academia, and nongovernmental organizations collaborate to enact internet regulations.

† China supplements these procedural efforts with soft power initiatives to promote its model of cyber sovereignty, such as sponsoring exhibitions and international forums. For instance, since 2014, CAC has organized the annual World Internet Conference (世界互联网大会), which showcases the PRC’s approaches to internet governance.

‡ The ITU is an agency subordinate to the UN that is responsible for formulating the regulations and guidelines that govern international communications technology, such as technical standards for emergent technologies.

§ ICANN is a nonprofit organization that administers key parts of the global internet’s underlying infrastructure, such as root servers, domain name systems, and IP address allocation mechanisms. The group was directly overseen by the Department of Commerce from its founding in 1998 until 2016, when it became an independent organization.
Case Study One: Censorship during the COVID-19 Pandemic

The COVID-19 pandemic has been a real-time stress test for China’s censorship apparatus and public opinion management capabilities. From an information control perspective, COVID-19 posed an acute and multifaceted challenge for the PRC’s leadership. On the domestic front, the CCP assessed that cultivating popular confidence in its response to the pandemic was key to demonstrating its legitimacy and ability to maintain social stability. Internationally, the PRC regarded questions over the origins of COVID-19 and criticisms of its initial response to the crisis as being harmful to its prestige and image as a responsible global stakeholder. As a result, throughout the course of the pandemic, the CCP has used all available means to promote its preferred narratives relating to COVID-19 and to stifle information that contradicts Party-approved positions. From the earliest days of the crisis, when information about an outbreak of mysterious “pneumonia” cases first became public, through more recent events, such as the lockdowns in Shanghai and Urumqi, Chinese national and local authorities have sought to control the narrative and guide public opinion through a variety of censorship techniques, including online content deletion, propaganda dissemination, and the arrest and intimidation of dissidents. The employment of these censorship techniques has been flexible and dynamic, varying over time and adapting to changing domestic and international circumstances.

Guidance and Policy

When news of the emergent coronavirus first appeared on social media, CAC sought to limit discourse on it through directives to remove posts and promote alternative content. CAC’s involvement in censorship of information on COVID-19 began in the first week of January 2020, when it issued a directive to news websites ordering them to use only government-published material. In February, directives were issued to CAC workers, specifying which articles were to be promoted on local news aggregators and social media, how many hours they should be featured on their home screens, and even the typeface that headlines should use. According to the directives, “negative” news and words such as “incurable,” “fatal,” and “lockdown” were not to be used “to avoid causing societal panic.” CAC instructed its local offices to “seriously deal with” reports of “harmful” content and “spreading panic” about COVID-19 on social media platforms. It also criticized “the lax management of illegal information released by users” on Baidu and singled out platforms such as Weibo, Tencent, and ByteDance for “special supervision.”

General Secretary Xi has himself openly acknowledged the importance of influencing and managing public opinion during this crisis. Starting in early February 2020, Xi began publicly and
frequently emphasizing the importance of “propaganda education” and “public opinion guidance” in controlling the narrative on COVID-19.\(^{238}\) In official public remarks on February 15 of that year, Xi spoke of “taking the lead and expanding positive energy online” by “strengthening the tracking and analysis of public opinion,” “proactively speaking out and providing positive guidance,” and “letting positive energy always fill cyberspace” while “controlling overall public opinion” by “strengthening control of online media” and “cracking down on those who spread rumors and cause trouble.”\(^{239}\)

These calls gradually formalized into official policy. On February 6, 2020, the Supreme People’s Court, Supreme People’s Procuratorate, Ministry of Public Security, and Ministry of Justice jointly issued legal guidance for “severely punishing” those who “maliciously fabricate false epidemic information, create social panic, stir up social emotions, and disrupt public order.”\(^{240}\) Later that month, the Chinese Center for Disease Control and Prevention instituted reporting requirements for publication of information related to COVID-19 and imposed restrictions on sharing that information without authorization.\(^{241}\) This was followed on March 3 by an official internal notice mandating that all publication work on COVID-19 information be managed by a new special task force under the State Council.* According to this directive, a “special team on public opinion” would work with the “propaganda group,” consider “public opinion trends and social concerns,” and guide the publication of scientific research and information.\(^{242}\) One week later, the Ministry of Education circulated a directive to universities containing this guidance, which some universities posted to their websites without proper authorization.\(^{243}\)

Covering Up the Outbreak

In the initial weeks of the outbreak, fear played an instrumental role in delaying the reporting of critical information to authorities. In December 2019, hospitals and commercial labs had detected a SARS-like coronavirus in patients but did not report their findings publicly for fear of political repercussions.\(^{244}\) This self-censorship resulted in the withholding of critical information and a delayed coordinated response to the crisis.\(^{245}\) When unauthorized information about the virus did appear on Chinese social media, the initial response by local authorities was to exert pressure on the individuals responsible. On December 30, 2019, Li Wenliang, an ophthalmologist, shared information in a WeChat group about confirmed cases of “SARS” (severe acute respiratory syndrome),† which was subsequently leaked to Chinese social media platforms. The next day, hospital authorities made Dr. Li write a formal apology for spreading “false information” and “causing public terror.”\(^{246}\) A few days later, police from the Wuhan Public Security Bureau made Dr. Li sign a statement acknowledging that he had violated the law by spreading “false information” that “seriously disturbed the social order” and that he would heed the warning and cease “illegal activities.”\(^{247}\)

Party-state authorities soon changed tactics when intimidation failed. After officials in Wuhan admitted that the epidemic was worse than they had anticipated or portrayed, there followed a brief period of relaxed censorship during which social media users discussed the pandemic more freely and castigated local government officials; criticism of the central government, however, remained

---

* This task force was dubbed the Scientific Research Group of the State Council’s Joint Prevention and Control Mechanism in Response to the COVID-19 Pandemic.

† The SARS epidemic began in southern China in November 2002 and spread globally in 2003. China was criticized for withholding information during the crisis.
That respite ended with the outpouring of grief and anger that accompanied news of Dr. Li’s death from the virus on February 6–7. Immediately following the news of Dr. Li’s death, the top two trending hashtags on China’s most popular social media platform, Sina Weibo, were “The Wuhan government owes Li Wenliang an apology” and “We want freedom of speech,” each of which were viewed millions of times before being censored within a few hours.

The response to Li Wenliang’s death demonstrates both shortcomings of China’s local censorship authorities as well as the resiliency of the CCP’s censorship regime at the national level. Shortly after Dr. Li’s passing, CAC immediately realized the elevated risks the public outcry following his death posed to its efforts to manage public opinion. CAC sent out directives to local propaganda workers and news outlets warning of the “butterfly effect, broken windows effect, [and] snowball effect” triggered by Dr. Li’s death and the “unprecedented challenge” it posed to online management and control work. It ordered news websites not to issue push notifications alerting readers to his death and to remove his name from trending topics pages. Online media outlets were permitted to report but not to “comment or speculate” on Dr. Li’s death, and they were instructed not to “hashtag and [to] let the topic gradually die out from the hot search list, and guard against harmful information.” Aside from these directives, CAC also resorted to public intimidation. To foster a “good online atmosphere” and control “harmful information and rumor,” CAC announced that it had punished website owners, mobile application developers, and social media users for publishing illicit content on COVID-19, sending a warning to others who might post content deemed sensitive by authorities. At the same time, CAC activated legions of fake online commenters to flood social sites with distracting chatter.

To carry out these activities, government departments in China use specialized software procured from private companies. According to leaked documents, the Chinese technology company Urun Big Data Services developed software that allows government workers to track online trends, coordinate censorship activity, and manage fake social media accounts. One of its products allows operators to quickly add likes to posts, assign specific tasks to commenters, and track their completion. Other software monitors social media for “harmful information” on sensitive topics, such as “incidents involving leadership” or “national political affairs.” Officials in Hangzhou apparently used Urun software to scan social media for keywords like “virus” and “pneumonia” in conjunction with place names. Social media platforms aided in the censorship effort by blacklisting keywords so that messages containing those terms would be automatically filtered out and never reach their intended recipient.

Social media users in China have pushed back against state-imposed censorship through a variety of creative ways. One widely shared post mocked the prevalence of blocked webpages that showed a “404” or “page not found” error by commenting “404+404+404+404+404=2020.” When an article was published in People magazine containing an interview with Ai Fen, a doctor at a major hospital in Wuhan who claims to have ultimately been responsible for sharing the patient medical report that eventually made its way to Dr. Li, it was quickly censored. Social media users reacted by writing the story backward, translating it into English and German, and using “Martian” language (a coded language based on ancient Chinese characters), emojis, and braille symbols to bypass the censors, with mixed success. Other methods to evade censors included posting photographs of text, using encrypted platforms such as Telegram and Signal, and archiving content.
Disputing the Origins of COVID-19

One issue of political sensitivity to China’s leaders, and thus subject to increased scrutiny by China’s censorship regime, has been the origins of COVID-19. For instance, in March 2020, Fudan University posted a notice from the Ministry of Education on its website (later removed) stating that “papers tracing the origins of [COVID-19] should be strictly managed.” Any documents on the topic slated for publication would need to go through a multistep process, starting with review and approval by academic committees at the universities, after which they would be sent to the Ministry of Education’s science and technology department, which would then forward them to a “special team on source-tracing” under the State Council’s special task force for final review and approval. Other papers related to COVID-19 would be evaluated by the academic committees based on factors such as their “academic value” and “proper timing.” Such deliberately convoluted procedures create friction that effectively obstructs information from becoming public, particularly that which contradicts the Chinese government’s preferred narrative of how effectively it initially responded to the crisis. Likely as a result of these policies, Chinese researchers then began censoring themselves, requesting that their work on the origins and spread of COVID-19 as well as conditions for medical workers be withdrawn from international scientific journals. Journal editors often enabled these efforts by obliging the requests. In one case, Wuhan researchers successfully requested that gene sequences be removed from a database managed by the U.S. government’s National Library of Medicine.

While China was restricting the public discourse space domestically, it was also engaged in externally facing operations to influence the international conversation. Responding to U.S. accusations that the virus may have leaked from a lab in Wuhan, China engaged in a disinformation campaign to flood the internet with alternative narratives. According to a report by the investigative site ProPublica, a Chinese company operated thousands of fake and hijacked Twitter accounts to flood the platform with disinformation and “positive energy” about China’s handling of COVID-19 and to suggest the virus originated in the United States or Europe.† While these efforts may have proven ineffective internationally, state media and government accounts have amplified these alternative narratives of COVID-19’s origins to shore up domestic support on popular social media sites like Weibo and elsewhere.

---

* GitHub is periodically a target of censorship by the Party-state due to its position as one of the few foreign-owned internet platforms operating in China. The site remains accessible because it is a key resource for Chinese-based computer programmers and web developers. However, GitHub’s status as an open forum for information exchange has led to it being targeted by the PRC, such as in 2013 when its service was interrupted by a cyber attack originating from China.

† For the sake of clarity, this section will use the term “Twitter” to refer to the website now known as X, because the events described in this case study occurred prior to the website changing its name in 2023. In the year prior to the pandemic, Beijing-based internet marketing company OneSight Technology, Ltd. had won a contract to boost the Twitter following of China News Service, the news agency of the United Front Work Department, which is responsible for influence operations in foreign countries; in the same year, other Chinese government agencies, including CAC, had offered similar bids. These accounts were then activated to promote Beijing’s preferred messaging on Twitter.
Persisting in Zero-COVID: Lockdowns and Protests

China’s censorship of COVID-19 faced mounting pressures in 2022 when its stringent and inflexible “Zero-COVID” policy brought about a wave of discontent. The first major test that year for China’s Zero-COVID policy was the Shanghai lockdown, which was enacted in response to an outbreak of the highly transmissible Omicron variant of COVID-19. After that lockdown was extended on April 1, residents began to voice complaints publicly about their conditions, including food and medical shortages. Some even recorded conversations with officials and posted them online. Eventually, someone compiled several of these recordings into a six-minute video montage titled *Voices of April*, which was released on April 22 and quickly went viral on Weibo and WeChat. The central government in Beijing immediately recognized the video’s potential to incite collective action and the risk it consequently posed to regime stability. Leaked directives from Beijing and the Guangdong CAC offices, which appear to have ultimately originated from the national CAC, ordered media platforms to “comprehensively clean up” all content related to *Voices of April*.† When authorities in Shanghai ultimately announced at the end of May that the restrictions would be lifted, they were careful to send out preemptive guidance to media outlets. Leaked directives from an unspecified government agency advised the media to “take care to keep a firm grip on messaging; titles and content must be precise to avoid ambiguity or misunderstanding” and to “actively carry out online guidance through such methods as following and replying to comments to secure the understanding, cooperation, and support of citizens.”‡

The same dynamic resurfaced in September 2022 with the lockdown of Ili Kazakh prefecture in the Xinjiang Uyghur Autonomous Region, but this time the evidence illustrates a different tactic employed by local authorities to censor discussions of sensitive topics: flooding. While there had been no official announcement of a lockdown in Ili prefecture, an area of Xinjiang with 4.5 million residents, comments and videos surfaced on Weibo and other social media of food and supply shortages following an extended period of COVID-19 restrictions. Local directives to internet commenters sought to drown out discussion of the deprivations in Ili prefecture with irrelevant content such as stories related to “domestic life, daily parenting, cooking, or personal moods” as well as “movies, games, making friends, studies, postgraduate entrance examinations, and idle chat.”

Another challenge to China’s censorship regime came in November 2022 when protests erupted in several Chinese cities. These protests are sometimes colloquially referred to as the “White Paper Movement,” named after the blank pieces of paper demonstrators carried as a symbolic challenge to CCP censorship.

* The Chinese term for this policy has been variously translated into English as “dynamic clearing,” “dynamic clearance,” and “dynamic zero.”
† Social media users attempted to circumvent these restrictions and evade censors through a variety of means: altering the title, embedding the video or overlaying its audio onto other video clips, rotating the video, posting mosaics comprised of individual frames, or disguising QR codes in movie posters.
‡ These protests are sometimes colloquially referred to as the “White Paper Movement,” named after the blank pieces of paper demonstrators carried as a symbolic challenge to CCP censorship.
of which had been dormant or were recently created.\textsuperscript{277} The activity levels of these accounts spiked during the protests and then immediately tapered off in December. Subsequent analysis from U.S.-based cyber threat intelligence firms strongly indicates this activity was carried out by organs of the Chinese Party-state.\textsuperscript{278} Crucially, the Party-state’s response to the protests was not limited to cyberspace. For instance, dozens of anti-lockdown protesters were detained and interrogated by the Ministry of Public Security, with a small number being imprisoned for expressing support for the movement.\textsuperscript{279}

Leaked internal Party-state directives demonstrate the perceived threat posed by the protests to public opinion management. Chinese internet users had preserved and spread information about the protests by circumventing the Great Firewall and accessing foreign websites like Twitter.\textsuperscript{280} Sensing the challenge this trend posed to content management in the wake of widespread protests, CAC issued a directive to “initiate a Level I Internet Emergency Response, the highest level of content management” in the wake of public outcry expressed over the Urumqi fire.\textsuperscript{281} It urged “key managers [to] take a hands-on approach and strengthen content management.”\textsuperscript{282} At around the same time, CAC issued a notice on the Thorough Clean-up and Regulation of Firewall-Circumvention Tools, Goods, and Services, prompting “all platforms” to “continue their concerted efforts to clean up online sales of goods and services used to circumvent the Firewall, including Firewall-circumvention routers, VPNs, web accelerators, VPS [virtual private servers], overseas Apple accounts, etc.”\textsuperscript{283} Given the timing of these directives and their oblique references to the widespread protests at the time, these directives must be seen as a direct reaction to Chinese internet users circumventing censorship by posting content to foreign websites like Twitter and Facebook to preserve and share records of the protests.

As the heavy-handed crackdown continued on the streets and in cyberspace, General Secretary Xi responded to the underlying cause of the protests and abruptly reversed his uncompromising Zero-COVID policy, which had been in place for roughly three years. On December 7, 2022, less than two weeks after protests broke out, the State Council issued the Notice on Further Optimizing and Implementing Prevention and Control Measures for the New Coronavirus Epidemic, which put forth “ten new measures” for the “further optimization and implementation of epidemic prevention and control.”\textsuperscript{284} While terms like “further optimization” suggested a continuation of existing policy, in truth the new measures represented a complete reversal of Zero-COVID.\textsuperscript{285} Authoritative commentaries in the \textit{People’s Daily} and other state media sought to rationalize the dramatic reversal by emphasizing that the new policy direction was a continuation and optimization of existing policy while “taking into account the current situation.”\textsuperscript{286} The policy shift and the lack of accompanying coherent censorship guidance reportedly caused confusion among censors and consequently resulted in delayed censorship of remarks implicitly critical of the abrupt policy shift, although general censorship in the form of deleting obviously negative expressions and promoting “positive energy” continued as before.\textsuperscript{287} Nevertheless, while the end of the PRC’s Zero-COVID policy resulted in a cessation of lockdowns, topics relating to the pandemic remain subject to strict censorship. For instance, the Party-state has prohibited the sharing of crowdfunded online databases aimed at calculating the number of deaths caused by COVID-19 in China, and it continues to disallow foreign researchers from accessing data relating to the origins of the virus.\textsuperscript{288}

The example of COVID-19 demonstrates that the Party-state censorship apparatus has a wide range of online and offline tools that can be deployed depending on varying circumstances. In the
case of Dr. Li, Chinese authorities first sought to instill fear among whistleblowers. When that did not work, they tried to create friction by censoring information about him. Ultimately, they tried to co-opt the narrative by portraying Dr. Li as a martyr of the CCP. With the sensitive question of the origins of COVID-19, China stifled researchers by restricting what could be published, and then it flooded domestic and international media platforms with disinformation. Finally, with public challenges to the Zero-COVID policy in the form of mass protests, Chinese authorities opted to perpetrate physical intimidation, remove online posts, increase barriers to circumvention tools, and flood platforms with distracting, irrelevant content.

Case Study Two: Censorship of “Historical Nihilism”

One major target of censorship under General Secretary Xi is what CCP sources call “historical nihilism” (历史虚无主义): information and commentary on history that complicates, contradicts, or reinterprets the Party’s official ideological narrative of China’s history.* The Party’s approach to politically fraught historical events ranges from the near-total obliteration of events from the public record, as with the 1989 Tiananmen Square massacre, to allowing for limited public discussion and even critical analysis of some events, such as the Cultural Revolution. While Xi Jinping is not the first CCP leader to emphasize combatting historical nihilism, he has elevated that struggle as a core goal for the Party. Since assuming power in 2012, Xi has spoken on multiple occasions about the political importance of historical issues, used historical narratives to bolster the Party’s reputation and his own authority, enacted policies to increase the reach of historical propaganda, and enacted laws to censor and publish alternate perspectives on history in academia, the arts, digital spaces, and popular media. This section will briefly discuss the CCP’s censorship of several key events in its history: the Great Leap Forward, the Cultural Revolution, and the 1989 crackdown on mass protests in Tiananmen Square. It will also analyze the theory and practice of Xi’s censorship of history and use of historical propaganda.

Xi Jinping’s Approach to History

Since assuming leadership of the Party, General Secretary Xi has emphasized the importance of history, an issue he believes concerns the very survival of the CCP and his own grasp on power. Xi has fiercely condemned both definitions of “historical nihilism:” first, rejecting or ignoring lessons and cultural legacies from pre-Communist Chinese history, and second, challenging or failing to conform to the Party’s version of historical events. Xi spoke about “historical nihilism” in a January 2013 speech to the Central Party Committee, soon after his selection as general secretary. In the speech, Xi portrayed “socialism with Chinese characteristics” as the historical destiny and only correct ideology for China, and he condemned domestic and international critics who cast doubt upon official CCP interpretations of history. He concluded this address by asserting that the CCP must retain ideological control, including control of its history, if it wants

---

* The term “historical nihilism” attained common usage among the CCP during the 1980s. At that time, amid internal debates about Mao’s legacy, senior Party leaders who were aligned with Deng Xiaoping condemned Party members who would either totally valorize or totally refute Mao. They called these perspectives “historical nihilism,” contrasting them with Deng Xiaoping’s position (eventually made the official Party verdict) that Mao should be remembered as a great leader who nonetheless made grave mistakes. Subsequent commentaries, such as a 2017 article by a scholar affiliated with the Central Party School, emphasize that the Deng-era definition of historical nihilism is “basically equivalent” to the CCP’s modern definition, which they give as “an attitude towards the Party’s history and leaders that is not fair, objective, and scientific.” Then, as now, allegations of “historical nihilism” are particularly sensitive to criticisms of past CCP leaders and highly dependent on what modern CCP leaders define as the “fair, objective, and scientific” version of past events.
to maintain its grasp on power. These articulated principles form the basis of Xi’s goal of attaining the “great rejuvenation of the Chinese nation” (中华民族伟大复兴), a concept that emphasizes the vital role the CCP has played in enabling China to reclaim its central status on the world stage. Over the past ten years, the Party has invoked this triumphalist view of Chinese history and culture in order to justify a wide range of policies, including elevating Xi’s status as paramount leader, further centralizing the CCP within daily civic life, and pursuing assimilationist policies targeting China’s non-Han ethnic minorities.

**Key Topics in the CCP Censorship of History**

To understand what is censored as “historical nihilism,” it is necessary to understand what the Party upholds as the correct historical narrative. The Party’s narrative of history centers the CCP as the savior of the Chinese people and indispensable architect of the PRC’s past and future success. It describes China as suffering a “century of humiliation” at the hands of Western powers and Japan, which ended with liberation from colonial and capitalist exploitation through the establishment of the PRC by the CCP. It then characterizes the Mao era as a time of continual positive economic development, albeit marred by some mistaken policies for which Mao himself bears only a fraction of blame. The Party praises the “reform and opening-up” (改革开放) policies of Deng Xiaoping and his successors as a necessary step in the continued adaptation of socialism’s “Chinese characteristics” rather than a repudiation or rupture with the socialist past. Under Xi, the Party now claims to have entered a “new era of socialism with Chinese characteristics,” a term that was introduced at the start of Xi’s second term in 2017 and later backdated to coincide with his initial ascension to leadership in November 2012.

The Party’s narrative of the Maoist years minimizes the famine caused by the Great Leap Forward and the Party’s responsibility for it. Official sources refer to the 1959–1961 famine with euphemisms such as “three years of hardship” or the “three years of natural disasters.” However, in 2012, a People’s Daily editor’s Weibo post denying the famine sparked widespread backlash on the social media platform and even several articles in print media discussing the famine, such as a detailed feature article in Southern People Weekly (南方人物周刊) that called for this history to be remembered and for China to never return to an “extreme planned economy.” This degree of relatively free public discussion on the topic was still subject to censorship and did not presage a broader reckoning or relaxation of censorship on the topic. Social media posts and essays related to the topic are still regularly censored, and scholarly research and publications on the era are sharply restricted or banned. The Party’s official narrative on the famine remains unchanged: a 2014 article from the website of the Chinese Academy of Social Sciences claimed the famine was an error of the Party’s “exploration of the road of socialist construction,” that the policies of the Great Leap Forward could not have been predicted to fail at the time, and that “Western hostile forces” exaggerate the death toll. The November 2021 Historical Resolution briefly referred to the Great Leap Forward and people’s commune movement as mistakes departing from the “correct line” (正确路线) without discussing the consequences of those mistakes or how they emerged within the Party. Moreover, the Central Propaganda Department’s (CPD) 2021 Brief History of the Communist Party (中国共产党简史) included a condensed discussion of the Great Leap Forward and softened language from previous editions critical of Mao’s handling of the resulting famine.
In contrast, the Party allows for explicit criticisms of the Cultural Revolution, though these criticisms are not allowed to indict the Party as a whole, Mao’s positive legacy, or modern leaders and policies. The Party formally acknowledges the Cultural Revolution as a grave and destructive error that it must be vigilant not to repeat. Under Deng Xiaoping, the CCP officially repudiated the Cultural Revolution in its 1981 Resolution on Certain Questions in the History of Our Party since the Founding of the People’s Republic of China (关于建国以来党的若干历史问题的决议), the second such “Historical Resolution” in the Party’s history.\(^{307}\) In that document, the Party concluded that Mao and his policies were largely correct and a net positive for China’s development. It also condemned “errors” of early economic policy (implicitly, the Great Leap Forward) and the Cultural Revolution, but only as matters of secondary importance.\(^{308}\) Beyond this official verdict, Chinese authors began to explore the tragedies of the era through fiction and autobiography.\(^{309}\) However, commemoration and discussion of the era are increasingly rare due to a mix of self-censorship, state-driven censorship, and the psychological burden of the trauma individuals suffered (and in some cases, actively or complicitly perpetrated) in the era.\(^{310}\)

Although Xi personally suffered under the Cultural Revolution, under his administration the Party’s official negative verdict on the era seems to have become less pointed in public-facing materials. The aforementioned 2021 revisions of the *Brief History of the Communist Party* replaced a sharply critical chapter on the Cultural Revolution with a less detailed version, omitting the text of the Party’s 1981 Resolution and Deng’s remarks warning against individuals holding too much power.\(^{311}\) The November 2021 Historical Resolution sharply criticized the Cultural Revolution and Mao’s “completely erroneous” judgment when launching it, though it omitted the 1981 Resolution’s condemnation of cults of personality.\(^{312}\) To be clear, Xi has not reversed the Deng-era verdict on the Cultural Revolution. More limited official acknowledgments of the era under Xi could be motivated by increasing historical distance, making the need for some form of reconciliation less immediate and staving off negative comparisons between Xi and Mao. Under Xi, censors and propaganda authorities continue the past practice of allowing and even encouraging some nostalgia for cultural aspects of the era. However, such official nostalgia remains carefully limited, as cultural events like music concerts and art from the era have occasionally provoked public backlash.\(^{313}\)

The 1989 Tiananmen student and worker protests and the Party’s brutal military response (in Chinese, the June 4th Incident, 六四事件) are more heavily censored than other controversial historical events, with almost no permissible public discourse on the subject. When rarely discussed in internal documents or official media, the protests are characterized as “counterrevolutionary riots” (反革命暴乱) and referred to with euphemisms such as “the political turmoil between the spring and summer of 1989” (1989年春夏之交的政治风波).\(^{314}\) To the Party, the protests also indicated a need for enhanced censorship to limit dissent and prevent collective action: immediately following the massacre, the Party cracked down on media, activists, and academia.\(^{315}\) Over the 1990s, the Party strengthened ideological control of newspapers and education, increasing the school system’s focus on “patriotic education,” particularly for subjects of political and historical importance.\(^{316}\) In the internet age, authorities impose blanket censorship of even coded online references to the massacre at Tiananmen Square. Offline, police work to prevent protests and commemorations through actions like the preemptive detention of known activists prior to the anniversary of the event.\(^{317}\)
Measures to Combat Historical Nihilism under Xi Jinping

Under General Secretary Xi, new laws and central guidance on historical nihilism have been put forth that are broad enough in scope to be flexibly interpreted and applied. In 2018, the National People’s Congress passed the Law for the Protection of Heroes and Martyrs (英雄烈士保护法), which forbids “distorting, vilifying, blaspheming, or denying the deeds and spirit of heroes and martyrs” such as by “slandering” their reputations or using their images and names for commercial purposes.* The law stipulates that such content on internet platforms will be prevented from being shared and taken offline and offenders will be punished in accordance with the nation’s Cybersecurity Law. It allows a martyr’s relatives to sue over such speech, and even if such relatives do not exist or wish to sue, it allows government procuratorates (检察机关) to do so in their stead in a civil case. CAC’s 2019 Provisions on the Governance of the Online Information Content Ecosystem (网络信息内容生态治理规定) do not explicitly refer to censorship of historical issues or historical nihilism beyond reiterating the prohibitions of the Martyrs’ Law, but it bans a wide range of content, including material that “hypes up gossip, scandal, and misdeeds” or “harms national glory and interests.” Further regulations include a 2021 CAC notice on live streaming that bans live streamers from “disseminating historical nihilism” and a 2023 notice on increased censorship of social media posts that “invent harmful information damaging to the Party and government’s image.”

The Party-state has wielded these expanded authorities to further tighten control of academic research and publication. For instance, the Martyrs’ Law was preceded by a controversy over the historian Hong Zhenkuai’s 2013 article challenging the facts of a popular story of several PLA soldiers’ heroic sacrifice against Japanese soldiers at Langya Mountain. Defamation cases by the soldiers’ descendants against Hong were all settled against him, forcing him to issue a public apology. Both the initial Hong Zhenkuai precedent and the Martyrs’ Law serve as a warning to historians that China’s civil courts view scholarship that challenges popular myths of CCP history as an attack on national honor, leaving academics and their publishers liable to lawsuits. An anonymous historian interviewed by the Washington Post in 2018, following the law’s passage, said historians felt increased pressure not to write anything critical about “any aspect” of PRC history and are even directly threatened by public security officials with the loss of jobs, pensions, or social services. Editors of academic publications are increasingly concerned by the possibility of violating unclear boundaries of censorship, leading to proactive self-censorship in academia.

The Party has also increased censorship of unapproved or potentially subversive artistic portrayals of history, instead promoting propagandistic media.† For example, under Xi, the already limited tolerance for artistic depictions of the Cultural Revolution era has almost completely vanished. China’s censors have allowed very few books and films set during the Cultural Revolution to be released. Sometimes, censors have allowed works on the era to be published, only for theaters to

---

* The term “martyr” is used to refer to both historical and modern individuals who died in the service of the Chinese public, CCP, and/or PRC.
† While their work is rare and heavily censored, amateur and professional scholars, journalists, artists, and historians do still conduct research, compile primary source archives, and even publish writings and films on historical topics heavily censored by the Party. Though these historians and artists are almost totally censored and subjected to state surveillance and harassment, their work still circulates to a limited extent in international and underground communities through the internet and other digital technologies. Their work is notable as a demonstration that while censorship of history under Xi has dramatically increased, it is not so absolute that no dissenting voices exist.
refuse to screen a movie or for censors to change course and retroactively ban a book’s
distribution. In contrast, cultural and propaganda authorities work to create and promote
historical films and television shows on patriotic themes, attempting to make Party history more
appealing than past propaganda in a society where citizens have much greater choice in media
consumption. These typically depict the era from the Party’s founding to the Korean War, allowing
them to focus on the most dramatic narratives of Party heroism against internal and external
enemies while avoiding controversies of the Maoist era, including the Great Leap Forward and
Cultural Revolution.

Censorship of History on the Internet and in Digital Media

As with other issues, social media companies are liable for censoring sensitive historical topics on
their own platforms, incentivizing excess caution. Forbidden topics are identified with a mix of
algorithmic detection of relevant keywords and human censors who can interpret users’ creative
attempts to bypass keyword detection. These coded references often involve historical events and
allusions. In 2021, CAC also established a hotline specifically for reporting cases of historical
nihilism online, thereby making use of nationalist internet users to identify and report history-
related content for censorship. In 2022, after the CAC Party secretary published an essay stating
it was necessary to “dare to brandish the sword, dare to struggle, and forcefully refute mistaken
views like historical nihilism” on the internet, several large social media companies—including
Douban, Douyin, Toutiao, and Weibo—issued warnings to users not to post historical nihilism and
to report such content through the platforms’ content reporting channels.

Digital censorship of the Tiananmen protests and massacre is particularly strict. A 2016 study of
the widely used messaging and social media app WeChat determined that the keywords “six-four”
were automatically blocked from chats if combined in a phrase or sentence with terms like
“democracy movement” or “memorial.” The study’s research on keywords censored from chats
found that 55 percent of keywords or phrases automatically blocked from chats referred to the
massacre. Content monitoring and censorship on social media platforms intensifies even further
around the anniversary of the event. Leaked censorship directives from recent years not only target
content that could reference Tiananmen (such as candle emoticons, images of tanks, or numbers
referencing the anniversary date) but also strictly limit all posting capabilities. These include
restricting official and popular accounts from posting on Douyin, requiring user-posted content to
undergo inspection before publication, or preventing users from editing their display names or
statuses under the excuse of technical maintenance.

General Secretary Xi did not begin the CCP’s campaign to censor historical nihilism, but he has
taken it to new heights through the stricter surveillance and censorship of traditional and digital
media. By passing censorship laws and regulations with broad and subjective application,
signaling a crackdown on historical topics through both public and internal remarks and campaigns,
and harassing or punishing the most prominent dissident voices, Xi and the Party have created a
climate hostile to any critical portrayals of China’s history. In creating such a climate, the Party
both raises the costs of dissent and harshly limits the scope of topics that are clearly safe for public
discussion, incentivizing rigid censorship by authors (or posters) themselves, their peers, and their
publishers (or digital platforms). Not only has Xi targeted negative or even objectively neutral
portrayals of Party history as “nihilism,” he has also emphasized and promoted the Party’s version
of that history to support the legitimacy of its governance and his own centralization of power.
Case Study Three: Censorship of the Russia-Ukraine War

The CCP’s approach toward handling the Russia-Ukraine War provides an instructive case study demonstrating how the Party manages discussions of foreign events that do not directly involve China. While the CCP tightly controls domestic narratives, it adopts a more nuanced approach toward certain international events. The Party has allowed limited discussions of the war but has carefully managed to avoid sparking social discord or drawing comparisons to sensitive issues like the status of Taiwan. Furthermore, the Party has applied the same adaptive approach to censoring foreign events as it does to censoring domestic ones, with tactics like information saturation being deployed strategically to allow controlled discourse within predefined boundaries.

Context and China’s Official Position

The Russia-Ukraine War poses an ongoing and unique challenge to PRC domestic and international prerogatives, even as it has created an opportunity to deepen the prevalent anti-West discourse that dominates Chinese social media. The Party-state’s handling of the situation reflects its dual objectives: to maintain positive relations with Russia and to uphold its longstanding principle of national sovereignty and territorial integrity. Chinese censorship techniques reflect these contradictory aims, limiting the coverage and conversation around the war through social media censorship and minimal coverage in the media while ensuring that the message received by the public remains wholly pro-Russian. To strike a balance between these aims, the Party-state’s approach to managing online discourse about the Russia-Ukraine War has shifted since the beginning of the conflict. It has gone from initially promoting a maximalist position in favor of Russia toward advocating for a more nuanced position that more carefully enunciates the differences between Chinese and Russian prerogatives.

State Media and the Russian Perspective

As made clear by official directives, Chinese censorship has ensured a pro-Russian slant since the early days of the conflict. Russia generally tends to be a censored topic, with acts of resistance or negative stories about Russia generally not covered in Chinese media. Concurrently, perpetration of falsehoods regarding the Russia-Ukraine War is a key pillar of China’s strategy, serving to keep the public behind the Sino-Russian partnership even as the Russian military falters. These falsehoods paint the picture of a weak Ukraine, with the implication being that a Russian victory is all but assured.* While state media coverage of the war tends to be minimal, stories that do air tend to rely heavily on pro-Russian sources.† For example, in Xinhua broadcasts, Russian military officials and spokespeople are disproportionately used, and CCTV’s nightly news program often relies on Russian media footage or the reporting of CCTV correspondents in Russia.340

Efforts to counter the overwhelmingly pro-Russian narrative have been largely disrupted and minimized. A few days after the start of the war, five renowned Chinese historians wrote an open letter denouncing Russia’s action on its neighbor and calling for peace. The letter was only online

---

* These included CCTV’s early claim that Ukrainian President Volodymyr Zelenskyy had fled Kyiv in the wake of the first wave of Russian attacks, that Ukrainian soldiers surrendered their weapons to advancing Russian forces, and that Russian forces are precise enough to have only struck military targets.
† A Financial Times analysis also found that CCTV has consistently relegated brief reports about the Ukraine crisis to the final minutes of its main evening broadcast, even as stories highlighting Putin or the Putin-Xi relationship received primetime coverage.
for two hours and 40 minutes before being removed by Chinese censors, with prowar commentators denouncing the authors as “shameful” and “traitorous.” Another notable initiative was the creation of an “alternative news agency” named *Yuci Tongshi*(与此同时) by anti-war Chinese citizens. It published articles demonstrating solidarity with Ukraine on WeChat, until it too was deleted by censors. It is no surprise that both of these developments occurred on WeChat—even as things are swiftly censored, analysts consider it the closest to a space for dissent available in China. High-profile social media accounts have also been targeted; in at least two cases, celebrities who called Putin “crazy,” urged followers to pray for peace, or posted photos of antiwar protests in Russia had their Weibo accounts suspended or restricted.†

Even as China has carried Russia’s perspective, it has noticeably sought to minimize the war’s overall coverage. For example, an analysis by the University of Glasgow published in July 2022 compared online news media framing of the Russia-Ukraine War and analyzed 24,422 stories obtained from Ukraine, Russia, the United States, and China. Chinese news sites only accounted for 3.23 percent of the total, with 2.15 percent of the total having been published in Mandarin. China has little to gain from an excess of coverage and discussion of the war, as any coverage threatens to dampen overall positive perceptions of the Sino-Russian strategic partnership. In a telling example, at the extensively covered Two Sessions of the National People’s Congress in 2022, Minister of Foreign Affairs Wang Yi only mentioned Ukraine at one press conference. Russian weakness has already become a talking point on Chinese social media; by some accounts, Chinese censors have relaxed their previously more exacting policing of Russian criticism.

**The Role of Social Media**

The interactions between traditional state media and social media have supercharged the messaging potential on the Chinese side, transforming what in earlier times would have remained merely turgid headlines in the *People’s Daily* into viral content. One technique often used is state media’s creation of certain hashtags, which are often parroted by downstream media. In the early days of the war, CCTV created a hashtag asserting that President Zelenskyy had fled Kyiv, which was reportedly viewed 510 million times. CCTV’s coverage of a Russian “antifascism” conference, accompanied by a hashtag on Weibo, had within 24 hours of posting garnered 650 million views and 90 media citations. The *Global Times* also disseminated the hashtag #UkraineCrisisInstigator, a dubious accusation alleging that the United States is responsible for the Russia-Ukraine War. A CNN analysis of nearly 5,000 Weibo posts from 14 Chinese state media outlets during the first eight days of Russia’s invasion found that of the more than 300 most-shared posts about the events in Ukraine, almost half could be classified as distinctly pro-Russian. Moreover, Russia’s mouthpieces RT and Sputnik both have official accounts on Weibo, with tens of millions of followers collectively. They are two of the main providers of pro-Russia narratives on Weibo, which also amplifies their voice through algorithmic recommendation.

Chinese social media accounts affiliated with the state work directly to explain the Russian perspective. On Weibo, the term “Azov Battalion” rose to popularity following a March 3 post by the Communist Youth League account. The post introduced the group as a Nazi organization affiliated with the state work directly to explain the Russian perspective. On Weibo, the term “Azov Battalion” rose to popularity following a March 3 post by the Communist Youth League account.

---

* The name can be literally translated as “Meanwhile” or “At the Same Time.”
† The two individuals, former talk show host Jin Xing and actress Ke Lan, consequently lost their ability to reach 13.6 million and 2.9 million followers, respectively.
and linked it with the Anti-Extradition Bill Movement in Hong Kong. The Taiwan-based Doublethink Lab has reported on how the Chinese public was not familiar with the discourse surrounding “Ukrainian Nazis” prior to the war, and it was Russian media in collaboration with Chinese media that rapidly built up the narrative following the outbreak of hostilities. Even as NATO remains a focal point for popular anger, Chinese media also carries many of the more specific accusations lobbied by Russia against Ukraine.

As the war has gone on, Chinese censors have allowed a wider range of opinions on the Russia-Ukraine conflict to be aired, reflecting the earlier directive on cooling public sentiment. In the early days of the war, on February 27, 2022, Weibo announced that it had suspended 10,000 accounts and removed more than 4,000 posts that “ ridiculed war” and mocked the situation in Ukraine. Besides misinformation, Weibo said offending posts include “vulgar content” related to jokes about Ukrainian women. On March 5, Weibo released another announcement stating that it had suspended more than 1,000 accounts that published “vulgar jokes” and “content that is overly insulting and warmongering.” The social media platform also began censoring searches for “Ukraine” and “pretty women,” the latter being another reference to the joke that Ukrainian refugees would become wives to Chinese men. Douyin, too, has been active, reporting in the first month of the conflict that it had removed 6,400 videos that violated its rules, cut more than 1,600 live feeds, and deleted more than 12,000 comments. Even without many further announcements, this kind of constant culling has very likely continued at the same or even a higher rate, targeting not only peace advocates but also those whose are too craven in their support of Russia.

The Party-state has sought to diminish some of the more aggressively prowar sentiments while keeping a focus on criticizing the United States and NATO. For instance, Xinhua and other government organs use social media to “discuss and present in a reasonable way” opinions of the war and criticize those who “spoke inappropriately.” Topics about “Ukrainian Nazis” and the need to “de-Nazify Ukraine” or blaming Ukrainians for war crimes and atrocities such as those in Bucha go largely uncovered within Chinese media. Instead, Chinese social media has removed exceedingly partisan views from both sides of the discussion.

There has also been consistent pushback against any suggestions or implications that liken the situation in Taiwan to that of Ukraine. Even a day after the start of the war, China’s ambassador to Cuba was already declaring online that “Taiwan is not Ukraine.” Russia’s decision in September 2022 to hold referendums in four occupied territories of Ukraine was rebuked by Chinese officials, who reiterated their commitment to maintaining “sovereignty and territorial integrity.” Chinese media contains no references to Taiwan being the next Ukraine, and commentary on social media attempting to compare Taiwan and Ukraine—even commentary justifying a future invasion of Taiwan—is rapidly censored. Even where it might serve Chinese prerogatives by deepening popular support for an invasion of Taiwan, China, implicitly recognizing the illegality of Russia’s invasion of Ukraine, seeks to hem the discussion.

Chinese social media also allows individuals who are producing a message aligned with that of the state to play an outsize role in the debate, an example of China’s system of participatory censorship. On Bilibili, one of the first independent videos describing the Russia-Ukraine War to rocket to popularity was titled “What kind of big power game is hidden behind the strange Russia-
Ukraine conflict?" The video argues that Ukraine was a puppet of the United States and that the war was the result of U.S. provocation and the aggressive eastward expansion of NATO. It was the top trending video on the site the day after its publication on February 24, 2022, and had accrued over ten million views by September 2023. Top search results for “Ukraine War” (Украинская война) on Bilibili still return results with a Russian perspective, with the vast majority being either interviews with Putin and other Russian officials or serving as analyses of Russian military tactics. Other popular videos peddle Russian conspiracy theories, such as a video titled “Emergency deletion, mysterious virus, biochemical experiments... What exactly did the U.S. do in Ukraine?” which promotes the unfounded U.S. biolab in Ukraine theory. These types of creators, who peddle in nationalist messaging and promote the Party line, are rewarded by the secretive algorithms of Chinese social media websites, leading to boosted view counts and greater income for their creators. In doing so, they serve as mouthpieces for the regime and key assets of the censorship system, despite being nominally independent and unaffiliated with the CCP.

Online searches for information, too, face a high level of censorship in China. In an April 2023 report from researchers at the University of Toronto’s Citizen Lab, 60,000 unique censorship rules used to partially or totally censor search results were uncovered across Baidu, Baidu Zhidao, Bilibili, Microsoft Bing, Douyin, Jingdong, Sogou, and Weibo. While some combinations returned no matches, such as a Baidu search for “Arrest Warrant + Putin + Xi Jinping,” others, such as Sogou searches for “be the next Ukraine + Taiwan” were allowed but only gave results from authorized sources. Other Ukraine combinations with authorized results were related to the military, including references to Chinese company “DJI, drones, and Ukraine,” “Elon Musk, Ukraine, and the Starlink,” and “A Year After Invading Ukraine + Russia Depends on China.” These “soft censors” for very specific combinations of words appear to be deployed rapidly in response to changing events and news developments. Even relatively minor figures or events are removed from search results, such as Wang Jixian, a Ukraine-based Chinese programmer who shares videos of the conflict, with his content often presenting a view of Ukraine that diverges from the official narrative in a way that could be hard to dispute.

China’s response to the Russia-Ukraine War sheds light on the nuances of its geopolitical, media, and public opinion control strategies. The convergence of media censorship, social media narrative control, and promotion of pro-Russian sentiment reflects a desire to maintain a balance between a desire to shape international relations and internal public perception. The extensive and adaptive censorship efforts—ranging from flooding the airwaves with Russian talking points and engaging in keyword suppression to the deletion of dissenting and aberrant views—illustrate an intricate web aimed at shaping domestic and international narratives to align with China’s geopolitical and ideological objectives. While maintaining an ostensibly neutral stance on the Russia-Ukraine War, China has actively facilitated the propagation of pro-Russian content while subtly highlighting its sovereign prerogatives and maintaining a distinction between inward- and outward-facing media. The implicit collaboration between Russian and Chinese media outlets and the perpetuation of anti-Western discourse are indicative of a larger strategic alignment aimed at fostering a multipolar world while reinforcing their respective national interests.

**PART 5: IMPLICATIONS OF PRC CENSORSHIP FOR THE UNITED STATES**

The ongoing expansion and strengthening of the PRC’s censorship apparatus poses a number of key diplomatic, economic, and security challenges for the United States. These risks stem from
spillover caused by the CCP’s domestic information control apparatus as well as the direct effects of China’s efforts to extend its censorship model internationally. This section will assess the impact of PRC censorship on U.S. interests at home and abroad and will conclude by outlining a set of policy recommendations for remediating those effects.

**Implications of PRC Domestic Censorship**

Increased domestic censorship has amplified the risk of local incidents within China spilling over to become global crises. Under Xi Jinping, the PRC has diminished or closed off many of the academic, journalistic, and private channels that facilitated information exchanges between the United States and China. Consequently, accurate data on internal trends and conditions within China are increasingly obscured from outside observers. The adverse effects of this dynamic are embodied in China’s botched early response to COVID-19, wherein state censorship exacerbated the virus’s initial spread and prevented a timely international response. Moreover, the Party’s information control regime will likely inhibit joint Sino-U.S. efforts to redress future emergencies such as economic instability. For example, China’s decision to restrict access to key data such as corporate records and youth unemployment statistics has impeded U.S. companies’ ability to conduct adequate due diligence and reduce their exposure to market downturns in the PRC. *378 The resulting uncertainty exacerbates the risk that economic instability within China spreads to precipitate a generalized global financial crisis.

The CCP public opinion guidance policies enflame domestic sentiment against the United States and its partner nations. As demonstrated in the case studies section of this report, the Party frequently draws upon a mix of patriotic sentiment and historical grievances to rally its citizens against “hostile foreign forces.” The Party pairs this narrative strategy with censorship of pro-Western sentiment to dial up and dial down negative sentiment directed abroad, depending on the objectives of CCP leadership. In the past, Beijing has used this approach to build support for discreet policy objectives. For instance, in order to drum up domestic support for hardline foreign policy measures in China’s near abroad, the Party frequently invokes historical memory of the Second World War and Korean War to inspire popular antagonism against Japan and South Korea, respectively. †379 However, a concerning emergent trend is the Party’s increasing propensity for attributing domestic failings, such as slowing economic performance, to U.S. machinations aimed at “containing” China and curtailing its development. This dynamic may increase risks of future regional conflict as the CCP sublimes internal discontent into support of a more aggressive foreign policy.380

**Implications of PRC International Censorship**

The PRC’s growing capacity to police information beyond its borders complicates U.S. foreign policy both in peacetime and in a future potential crisis. From an ethical perspective, China’s efforts to restrict discussions on sensitive issues like the status of Taiwan, Hong Kong, and Xinjiang are antithetical to core U.S. values such as freedom of expression and association. These

---

* Moreover, corporate records information also plays a key role in enabling Western researchers to uncover instances of corporate malfeasance by Chinese companies, such as sanctions evasion and enabling state repression in Xinjiang.

† CCP censorship strategy generally does not make sharp distinctions between treatments of the United States and its allies, portraying the latter as proxies for advancing U.S. interests. For example, contemporary PRC portrayals of the Korean War emphasize cultivating a “patriotic spirit of uniting against an enemy” and inspiring citizens to oppose “U.S. aggression,” and they mostly ignore the historical role of South Korea.
practices are also problematic at a practical level in the sense that they enable China to shape global public opinion in a manner that undermines U.S. national security interests. As the previous sections have demonstrated, China’s drive for “international public opinion guidance” is a mechanism for “operational preparation of the environment” designed to maximize its available diplomatic options during times of crisis while constraining its adversaries’ options. Consequently, what may seem like minor concessions to PRC sensibilities (such as mandating companies to refer to Taiwan as “Chinese Taipei”) are designed to have a cumulative effect, eroding the United States’ internal political will and external moral authority to oppose cross-Strait coercion.  

Concurrently, although the PRC still lacks soft power and broad-based political appeal, it possesses a growing capacity to achieve its foreign policy objectives by weakening or drowning out anti-CCP narratives. For example, Chinese information operations aimed at influencing foreign perceptions on the COVID-19 pandemic evinced a capability to spread doubt and confusion about topics deemed sensitive by the Party, such as the origins of the virus and the effectiveness of the PRC’s response. Although PRC messaging efforts are often rudimentary, its influence organs rapidly seek to incorporate new technologies, such as generative AI, to boost their effectiveness. Indeed, the PRC has already used early versions of these platforms to create fake images and disinformation pertaining to topics such as the 2023 Hawaii wildfires. These capabilities are likely to grow in sophistication and effectiveness as China both cultivates its own home-grown AI industry and continues to benefit from knowledge and expertise imported from the United States. As the PRC incorporates these emergent technologies into its “international public opinion guidance” operations, it is likely that the Party’s ability to shape global attitudes and narratives will become increasingly potent.

Finally, China’s stated ambitions to reshape global telecommunications governance pose a dire threat to the viability of the internet as a means of global information exchange. At a basic level, adoption of the PRC’s “cyber sovereignty” framework would have the effect of balkanizing the internet along national boundaries, stifling the free flow of information that has made that platform an engine for global economic and scientific development. As ICANN CEO Göran Marby has noted, such a move would jeopardize internet interoperability, leading to a fragmentation of the global internet along national lines. Moreover, on a practical level, moving from a multistakeholder to a multilateral model of telecommunications governance would place responsibility for technical administration of the internet in the hands of government officials who lack industry expertise. This would ultimately diminish the quality and competency of global internet governance. Finally, the international normalization of censorship measures, coupled with the increased availability of information control tools, will amplify global trends of rising authoritarianism and democratic backsliding.

* For leadership within the Party, the necessity of this strategy has come into particularly stark relief in light of the ongoing Russian war in Ukraine. The conflict demonstrated the power that international narratives play in producing real-world effects such as facilitating sanctions imposition against Russia and arms shipments to support Ukraine.
ADDENDUM I: ORGANIZATIONAL STRUCTURE OF THE BUREAUCRATIC INSTITUTIONS THAT COM普ICE CHINA’S CENSORSHIP APPARATUS

China’s Central Propaganda Department

As the manager of China’s propaganda work xitong, the Central Propaganda Department (中国共产党中央委员会宣传部), or CPD, is a key node in China’s censorship apparatus. The CPD serves as the “mouthpiece” (喉舌) for the Party as well as the chief custodian for news and cultural content produced in the PRC. It is China’s oldest and most venerable instrument used for information control, having been founded in 1924. As such, it exercises direct oversight over content produced by legacy media institutions in China. Additionally, it plays a key role in internet censorship through its role as the CCP’s principal institution that determines the “main line” (主线) of online public opinion guidance and propaganda work.

Structure

The CPD serves as the CCP’s main mechanism for controlling and shaping China’s information environment. Accordingly, it bears responsibility for ensuring that media produced in China aligns with “core socialist values.” The CPD operates a number of internal offices that manage portfolios related to censorship, such as its Media Oversight Bureaus (传媒监管局), Illegal Activity Prevention Bureau (反非法反违禁局), and Public Opinion and Information Bureau (舆情信息局). Moreover, the department directly manages the output of state media institutions through its subordinate body, the National Radio and Television Administration (国家广播电视总). It also maintains strict oversight of nonstate media outlets by requiring news organizations to meet certain ideological and organizational requirements in order to receive operating licenses. As a result, all media in China is subject to guidance and review by CPD officials, who ensure that all distributed content aligns with official “narratives” (提法) that are determined by Party central leadership. This control scheme extends down to local governance structures in China where each province, prefecture-level city, and county Party committee possesses its own department that implements the directives of its supervisory Party propaganda organization and oversees content from local news, radio, and television producers.

Crucially, the CPD and its subordinate branches are also in charge of “online public opinion information work,” which entails “integrating and guiding” (综合和引导) the work of other departments that support that mission. As such, the CPD appears to work closely with, and at times directly oversees, parts of the Cybersecurity Administration of China’s (CAC) missions, especially those related to online sentiment and public opinion. This partial oversight role over the internet is reflected in the composition of China’s central leadership. For instance, CAC’s current director, Zhong Rongwen (庄荣文), serves concurrently as a deputy director (副部长) within the CPD. This dual-hat arrangement extends to subordinate branches of those departments. It appears standard practice for each province and prefecture-level city to have its deputy chief of the propaganda department (委宣传部部长) serve concurrently as the director of the local CAC.

* In official English translations, the PRC refers to this institution as the “Central Publicity Department.” This is likely done as an expedient measure, given the negative connotation the word “propaganda” has in many Western countries.
† It also coordinates this mission with other bureaucratic offices such as the Ministry of Culture and Tourism, Ministry of Education, and the People’s Liberation Army’s (PLA) General Political Department.
Moreover, local propaganda departments will often finance the operational and personnel expenses for their corresponding CAC offices and in some cases will directly oversee their operations.*

**Oversight Tasks**

Propaganda departments at all levels act as the Party’s first line of defense for preventing and dispelling potentially deleterious information. They closely monitor the media environments within their areas of jurisdiction and act as a coordinative body to develop responses to potentially adverse public opinion trends. To this end, these departments maintain sub-bureaus that “monitor and guide internet public opinion.”† Each provincial, prefecture-level city, and county-level propaganda department is in charge of its area’s internet propaganda management system (互联 网宣传管理) and online public opinion guidance capabilities (网上舆论引导能力). These units are also responsible for coordinating with their corresponding CAC offices to exercise oversight over online communities, Weibo accounts, WeChat accounts, blogs, and websites that are registered within their areas of jurisdiction.

In addition to these surveillance responsibilities, propaganda departments are in charge of “strengthening the Party’s position online” and “spreading positive energy” on the internet. In recent years, this task has placed particular emphasis on conducting propaganda work using mobile platforms and social media. For instance, internal propaganda department guidelines mandate that all work units (单位) under the relevant Party committee’s jurisdiction maintain official microblogs and WeChat platforms to carry out propaganda work. They also maintain “online commentary teams” (网络评论员队伍) tasked with interacting with netizens within the jurisdiction by “guiding online comments” as determined by supervisory departments.‡

**Cyberspace Administration of China**

The Cyberspace Administration of China (国家互联网信息办), or CAC, is the CCP’s chief bureaucratic organ tasked with managing online content in the PRC. It assumed its current form as an independent Party-state bureaucratic organization in 2014, combining the regulatory powers of more than 15 bureaucratic internet regulators under a single unified entity.

**Structure**

CAC is administered directly by the Central Party Committee through the Central Cyberspace Affairs Commission (中央网络和信息化委员会). While information on the central structure of CAC is scarce, it appears to comprise one main office, 14 sub-bureaus, and nine affiliate research institutions that are in charge of tasks ranging from coordinating cybersecurity

---

* For instance, while the Shanghai branch of the CAC General Office is subordinate to Shanghai Party Cyberspace Affairs, the office itself is managed and funded by the municipal Party Committee’s Propaganda Department.
† Depending on locality, these public opinion monitoring responsibilities are either managed in house or contracted out to third parties such as universities, news media organizations, or private companies. In some cases, propaganda departments will receive multiple public opinion information feeds from a combination of these sources.
‡ These teams are often colloquially referred to as the “Fifty Cent Party” (五毛党).
§ The Commission was initially established in 2014 as the Central Leading Group for Cybersecurity and Informatization (中央网络安全和信息化领导小组) before being elevated to the level of Commission in 2018. This organizational change likely reflects the importance that Party leadership attaches to the role of internet content oversight work.
work to promoting mobile internet infrastructure development. A few of these departments have portfolios that deal directly with censorship. These include:

- The Bureau of Network Commentary (中央网信办网评局), which is in charge of directing website owners to issue warnings for and delete harmful posts.409
- The Bureau of Internet Community Work (中央网信办网络社会工作局), which is in charge of managing and engaging with “national-level online communities.”* 410
- The Bureau of Comprehensive Management and Law Enforcement Supervision (综合管理执法督查局), which is tasked with coordinating with elements of China’s security state to punish internet crimes.411
- The Bureau of International Cooperation (国际合作局), which is tasked with managing communication and engagement with foreign online communities.412

Lastly, CAC coordinates with other key institutions, such as the Ministry of Industry and Information Technology (MIIT), to jointly oversee industry regulatory and licensing authorities, like the China Internet Network Information Center (中国互联网络信息中心 or CNNIC), the National Information Security Standardization Technical Committee (全国信息安全标准化技术委员会 or TC260), and the Cybersecurity Review Technology and Certification Center (网络安全审查技术与认证中心 or CCRC).413

Since 2018, CAC has dramatically expanded its authority over local internet governance. At present, CAC maintains branch offices at every provincial and prefectural city level and is currently in the process of establishing offices at the county level.414 Generally, each CAC branch department (网信办) oversees a Network Propaganda Office (网络宣传办公室 or 网宣办) and a Network Management Office (网络管理办公室).415 These institutions are tasked with both “vertical management,” which entails carrying out instructions laid out by their supervisory institutions, as well as “horizontal management,” which entails formulating internet content policies that are specific to their areas of jurisdiction.416 Many branch offices also feature additional subunits, such as network management and law enforcement sections (网络管理执法科), network propaganda and commentary sections (网络宣传评论科), and network public opinion monitoring and assessment centers (网络舆情监测研判中心).417 These offices operate under a principle of “unified standards and different characteristics,” meaning they all follow the same regulations set out by CAC, although means of implementation may vary from locality to locality.418

Oversight Tasks

CAC functions as a “supra-ministerial regulator” that oversees China’s digital ecosystem.419 Its main focus is ensuring that online activity aligns with the preferences of the Party, with day-to-day technical management of the internet being delegated to other ministries such as MIIT. Accordingly, CAC’s mission set comprises these tasks:420

* These include social media platforms such as WeChat and Weibo as well as popular websites that have a national reach, such as the Zhihu information exchange forum.
1) Implementing internet information dissemination guidelines and policies (互联网信息传播方针政策) and promoting the establishment of a legal system for governing online information dissemination.

2) Guiding (指导), supervising (督促), and coordinating (协调) relevant departments in order to strengthen online information content management.

3) Approving and conducting daily supervision of online news companies and related businesses.

4) Guiding relevant departments to construct commercial oversight plans for online gaming platforms, online audiovisual content, online publishing, and other online publishing fields.

5) Coordinating with relevant departments to plan and implement the establishment of “network cultural fronts” (网络文化阵地).* 421

6) Planning, constructing, and maintaining key news websites.

7) Organizing (组织) and coordinating online propaganda work.

8) Investigating and punishing (查处违) illegal websites in accordance with the law.

9) Guiding relevant departments in their work of supervising telecommunications companies, internet service providers (ISPs), and other businesses that handle basic internet management tasks such as domain name registration, IP address allocation, and website registration.

10) Guiding local CAC branch offices to carry out work within the scope of their duties.

CAC also plays a leading role in drafting regulations and using its supervisory authorities to enact punitive measures against internet companies that do not comport with established guidelines. These punishments can range from issuing warnings to imposing fines to revoking licenses and permanently shutting down websites.† 422 In addition to this domestic censorship portfolio, CAC determines which foreign websites and applications to block within China and coordinates with MIIT to make forbidden material inaccessible.423 It also closely regulates the sale and circulation of censorship evasion software, such as virtual private networks (VPNs), and coordinates with the Ministry of Public Security (MPS) to punish the unauthorized usage and distribution of those tools.‡ 424 Finally, CAC is tasked with managing transnational data transfers and uses this authority to restrict foreign entities from accessing information deemed to be sensitive, such as corporate records information and scholarly articles hosted on the China National Knowledge Infrastructure (中国知网 or CNKI) database.425

The organizational structure and censorship duties of CAC branch offices mirror that of their parent institution. Party committees at the provincial and prefectural levels maintain their own Cyber Security and Informatization Committees (网络安全和信息化委员会), which oversee a

---

* The word “front” (阵地) is used in a martial context. It refers to the notion of waging “cultural warfare” in online battlefields.
† For instance, in 2022, CAC conducted disciplinary interviews with 8,608 website platforms, issued warnings to 6,767 companies, issued fines to 512 companies, suspended the licenses of 621 companies, removed 420 mobile applications from circulation, closed down 25,233 “illegal” websites, and referred 11,229 criminal cases to law enforcement.
‡ While businesses and academic institutions are permitted to use government-approved VPNs, their use by private citizens is outlawed in China. Until recently, this prohibition was only sporadically enforced. However, since 2020 the Party-state has more vigorously implemented its ban on censorship-evasion software.
corresponding CAC department (网信部) and are responsible for the network ideology work responsibility system within their area of jurisdiction.\textsuperscript{426} This entails tasks such as tracking, analyzing, and sharing information on online public sentiment, ensuring that local companies are in compliance with Party guidelines on online content, coordinating incident responses to online public sentiment emergencies, and training nontechnical cadres in best practices for carrying out online public opinion work.\textsuperscript{427} CAC branch offices are also tasked with taking a hands-on approach toward engaging netizens with the purpose of fostering “healthy and progressive online public opinion.”\textsuperscript{428} This work parallels that undertaken by local propaganda departments, with CAC branch offices conducting online public opinion guidance work via paid parttime commentators as well as “grassroots network information personnel” recruited from the local community.\textsuperscript{429}

Finally, CAC offices are deeply enmeshed with other bureaucratic elements in their jurisdictions, and they use these connections to assess, manage, and direct public sentiment. For instance, many localities maintain Joint Cyber Security Response Small Groups (网络安全联合处置小组), which comprise elements of local CAC, MPS, administrative, propaganda, and emergency response departments.\textsuperscript{430} These groups facilitate the sharing of public opinion intelligence, materials relevant for ongoing criminal investigations, and other information pertinent to social stability.\textsuperscript{431} These groups also serve as an ad hoc coordinative mechanism for conducting crisis control and emergency response during public disturbances such as “mass incidents.”\textsuperscript{432}

Ministry of Public Security

The Ministry of Public Security (中华人民共和国公安部), or MPS, plays a key role in China’s censorship apparatus by investigating and punishing Chinese netizens who post or share information deemed harmful by the Party-state. Similar to its counterparts in CAC and the CPD, the MPS operates an extensive network surveillance architecture used to monitor the online behavior of ordinary Chinese citizens. This work is primarily undertaken via the Golden Shield Project (金盾工程), which is a program designed to facilitate intelligence gathering and information sharing among MPS departments at the central, provincial, prefectural city, and county levels.\textsuperscript{*} These surveillance capabilities in turn empower the MPS to investigate and prosecute crimes that involve forbidden forms of expression. Concurrently, MPS departments at all levels maintain sub-bureaus dedicated to online policing.\textsuperscript{†} These bureaus have a broad mandate to investigate online speech that spreads rumors, harms the Party-state, or promotes unsanctioned religious activity.\textsuperscript{‡}

While the MPS plays an integral role in policing online speech, it generally does not have a direct hand in censoring online material. Rather, the threat of investigation and punishment serves as a

---

* Contrary to popular belief, the Golden Shield Project is not solely composed of internet censorship infrastructure, nor is the term synonymous with the Great Firewall. Rather, Golden Shield comprises a set of generalized law enforcement tools, such as the MPS intranet platform, that enable information control, sharing, and surveillance. While Golden Shield has, at times, been used to aid censorship efforts, these tasks appear to have been assumed by CAC and the Ministry of Information and Technology (MIIT) after 2014.

† Naming conventions for these institutions vary, but they are usually rendered either as “network security departments” (网安部) or “internet police departments” (网络警察分局).

‡ According to existing regulations, the MPS is empowered to prosecute online speech that “spreads rumors, defamation or harmful material, incites subversion of state power, undermines the socialist system, incites separatism, undermines national unity, undermines ethnic unity, or which organizes and facilitates cult activity.”

---
deterrent mechanism, inducing netizens to self-censor for fear of the ill-defined boundaries of acceptable online speech. As such, the bulk of the MPS’s online policing efforts focus on cybercrimes such as online fraud and extortion, leaking state secrets, and speech that engenders social mobilization or directly threatens the Party-state. Online activity deemed harmful but not outright criminal is handled by local CAC branch offices, which are empowered to refer more serious cases to the MPS or local law enforcement entities.

**Ministry of Industry and Information Technology**

China’s Ministry of Industry and Information Technology (国工业和信息化部), or MIIT, is a state institution that oversees the core linkages of China’s telecommunications infrastructure. It instrumentalizes this authority to support the Party-state’s censorship efforts by overseeing the day-to-day operation of China’s “Great Firewall” and using its oversight authority to enforce private companies’ compliance with online content regulations. At present, MIIT oversees all internet traffic coming into and out of China through three national-level internet exchange points (IXPs) located in Beijing, Shanghai, and Guangzhou. Data transiting through these nodes are automatically inspected, and traffic that contains suspicious data or that is sent from blacklisted foreign IP addresses is blocked. These filtering mechanisms are also used to uphold CAC restrictions barring foreign users with non-mainland IP addresses from accessing certain sites such as the corporate records repository Tianyancha. In addition to blocking foreigners from accessing content hosted in China, the Great Firewall also prevents Chinese netizens from accessing foreign sites, either by denying access outright or “throttling” requests by restricting bandwidth to those sources. Concurrently, MIIT and its subordinate institutions are also engaged in an ongoing effort to disrupt unapproved censorship-evasion tools and VPNs such as Tor.

MIIT also uses its regulatory and licensing authority to ensure that Chinese internet firms adhere to laws and regulations governing network content. This work is principally done through the China Internet Network Information Center (中国互联网络信息中心), or CNNIC. CNNIC is currently China’s sole domain name registry service and root server operator and is responsible for the allocation of all national-level (.cn) domain names. It uses this authority to ensure that ISPs and internet data centers adhere to Party-state licensing and regulatory requirements under penalty of being deprived of access to key network resources and infrastructure. This oversight capacity in turn extends to govern the behavior of downstream information services providers such as social media platforms and website owners. As part of their licensing agreement, these companies are required to implement government guidelines, such as real-name registration for users, and also assume legal liability for content posted on their platforms. This constitutes a powerful incentive for network companies to self-regulate, lest their parent ISP throttle their internet bandwidth or shut down their websites entirely. Accordingly, the vast majority of internet companies in China opt to self-police content on their platforms as a proactive measure against drawing the ire of Party-state regulators.

---

* The phrase “Great Firewall” is a colloquial term used by Western sources to describe China’s internet censorship architecture. However, the term is not employed by official PRC sources.

† Between 2014 and 2021, CNNIC was overseen by CAC before authority was transferred to MIIT in 2021. This decision seems perplexing, as it runs contrary to CAC’s purpose of having oversight authority over online issues vested in a single institution. Nevertheless, this change in ownership does not appear to have disrupted Party-state oversight over Chinese ISPs, with both CAC and MIIT coordinating closely to enforce compliance with existing internet content laws and regulations.
ADDENDUM II: THE ROLE OF FIVE-YEAR PLANS IN SHAPING PRC CENSORSHIP PRACTICES DURING THE XI JINPING ERA

Although the CCP’s exact censorship priorities are often shrouded in secrecy, the broad contours of its evolving objectives can be gleaned from top-line guidance such as its national five-year plans. Xi Jinping has overseen three of these five-year planning cycles, each of which has resulted in new innovations in CCP political and ideological work.

China’s 12th Five-Year Plan for National Economic and Social Development (中华人民共和国国民经济和社会发展第十二个五年规划纲要), covering the period from 2011 to 2015, calls for “creating a good social and cultural environment” online. In order to accomplish this, it directs Party-state organs at all levels to “effectively strengthen cultural market supervision and effectively curb the spread of illegal and harmful information” and “comprehensively use economic, educational, legal, administrative, and public opinion means to guide the people to understand honor and disgrace, to be upright, and to fulfill their obligations, so as to form a social atmosphere that supports righteousness and eliminates evil, and promotes the good and punishes the bad.” The plan also emphasized using new and emerging media such as the internet to understand and shape public opinion.*

China’s 13th Five-Year Plan (2016–2020), calls for using public opinion propaganda and cultural influence to cultivate “core socialist values” (社会主义核心价值) and leveraging mainstream and emerging media to “improve the level of public opinion guidance and enhance communication, credibility, and influence.” With regard to the online environment specifically, the plan states that China should “develop a positive Internet culture” (发展积极向上的网络文化), “develop innovative online propaganda methods that conform to the laws of online communication, and improve online public opinion analysis and guidance capabilities.” The 13th Five-Year Plan also uses the phrase “cyberspace governance” (网络空间治理), not found in previous iterations, to describe China’s efforts to regulate the online media environment through legal and administrative means. It furthermore links governance of cyberspace to concepts of national security and ideological security, advocating for “strengthening the struggle against enemies in online sovereign space and the management and control of online public opinion.”

The 14th Five-Year Plan (2021–2025) likewise links cybersecurity to political security, stating that the PRC should “strengthen the protection of data resources” and “upgrade capabilities for security protection and maintaining political security.” The plan also stipulates that the CCP should further improve its ability to exert control over the network space and online public opinion. This entails strengthening the hierarchy and classification apparatuses for network platforms, improving the laws and regulations that regulate enterprise data collection and usage and those that dictate news dissemination and reprinting, and improving oversight over “new network technologies and applications which have a great influence and large numbers of users.” The 14th Five-Year Plan also echoed previous priorities for network content policing such as cracking

* Specifically, the plan called for the Party to “strengthen the construction of important news media, pay attention to the construction, use and management of emerging media such as the Internet, grasp the correct direction of public opinion, and improve communication capabilities” (加强重要新闻媒体建设，重视互联网等新兴媒体建设、运用、管理，把握正确舆论导向，提高传播能力).
down on illegal activities like online rumors (网络谣言), harmful information (有害信息), fake news (虚假新闻), online extortion (网络敲诈), online trolling (网络水军), and paid deletion of posts (有偿删帖).\textsuperscript{460}
ADDENDUM III: INDEX OF LAWS AND REGULATIONS RELATING TO CENSORSHIP IN THE PRC

<table>
<thead>
<tr>
<th>Law or Regulation</th>
<th>Rules Issued/Purpose</th>
<th>Issuing Agency</th>
<th>Release Date</th>
<th>Effective Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criminal Law (刑法)</td>
<td>Adds the crimes of illegal hacking into computer information systems and destroying computer information systems to the Criminal Law code.</td>
<td>National People’s Congress</td>
<td>14 March 1997 (revised) (Amended 29 August 2015)</td>
<td>1 October 1997</td>
</tr>
<tr>
<td>Interim Measure on the Management of Internet Domain Name Registration</td>
<td>Establishes a domain name management system, and a registration, approval, change, and cancelation process.</td>
<td>State Council Informatization Leading Small Group</td>
<td>30 May 1997</td>
<td>30 May 1997</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>Ministry/Department</td>
<td>Date Range</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Administrative Measure for Public Multimedia Communications in China</td>
<td>Clarifies the rules for the access of service operators and information source providers and implemented a business licensing system and application approval system.</td>
<td>Ministry of Posts and Telecommunications</td>
<td>10 September 1997 to 1 December 1997</td>
<td></td>
</tr>
<tr>
<td>Interim Regulation on the Administration of the Secrecy of Computer Information Systems</td>
<td>Stipulates the confidential management of secret-related systems, information, places, and media.</td>
<td>National Administration of State Secrets Protection</td>
<td>26 February 1998 to 26 February 1998</td>
<td></td>
</tr>
<tr>
<td>Administrative Measure for China Jinqiao Information Network Public Multimedia Information Services</td>
<td>Implements a business licensing system for the provision of multimedia information access services on China Jinqiao Information Network.</td>
<td>Ministry of Electronics Industry</td>
<td>1 March 1998 to 1 March 1998</td>
<td></td>
</tr>
<tr>
<td>Interim Regulation on the Management of Telecommunications Internet</td>
<td>Includes mobile phone communications networks and data communications networks under the Ministry of Industry and Information Technology’s supervision.</td>
<td>Ministry of Industry and Information Technology</td>
<td>7 September 1999 to 7 September 1999</td>
<td></td>
</tr>
<tr>
<td>Trial Measure on the Management of Computer Information System Integration Qualifications</td>
<td>Stipulates computer information system integration qualifications, application requirements, evaluation standards, supervision, and management requirements.</td>
<td>Ministry of Industry and Information Technology</td>
<td>7 December 1999 to 1 January 2000</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
| Administrative Measure on the Dissemination of Audiovisual Programs on the Internet and Other Information Networks (互联网等信息网络传播视听节目管理办法) | Establishes a business licensing and supervision system. | 2003 edition: State Administration of Radio, Film, and Television  
<p>| Interim Provision on Internet Culture Management (互联网文化管理暂行规定) | Establishes a business licensing system for internet cultural activities and products as well as a self-examination and self-assessment system. | Ministry of Culture | 10 May 2003 (revised 15 December 2017) | 15 December 2017 |
| Opinions on Strengthening Information Security (关于加强信息安全保障工作的意见) | Establishes a protection system based on security level, sets a path for the improvement of encryption technology, the improvement of security monitoring systems, emergency response systems, etc. | National Informatization Leading Group | 26 August 2003 | 26 August 2003 |</p>
<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Issuing Body</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice Prohibiting the Broadcasting of Computer Online Game Programs</td>
<td>Institutes a “minor protection system” for underage users accessing online content.</td>
<td>State Administration of Radio, Film, and Television</td>
<td>12 April 2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>12 April 2004</td>
</tr>
<tr>
<td>Opinions of the National Copyright Administration on Whether Internet</td>
<td>Establishes rules on internet copyright protection as well as mechanisms to promote understanding of its attendant rules and prohibitions against deleting information.</td>
<td>National Copyright Administration</td>
<td>16 April 2004</td>
</tr>
<tr>
<td>Cafés Should Bear Legal Responsibility for Downloading and Supporting</td>
<td></td>
<td></td>
<td>16 April 2004</td>
</tr>
<tr>
<td>“Cheating” (国家版权局关于网吧下载提供“外挂”是否承担法律责任的意见)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notice on Strengthening the Content Review of Online Game Products</td>
<td>Establishes a system for internet cultural business licensing applications, review, importation, etc.</td>
<td>Ministry of Culture</td>
<td>14 May 2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>14 May 2004</td>
</tr>
<tr>
<td>Suggestions on Further Strengthening and Improving Minors’ Ideologies</td>
<td>Suggests ways to guide public opinion, purify the online environment, and strengthen management.</td>
<td>National Press and Publication Administration</td>
<td>31 May 2004</td>
</tr>
<tr>
<td>and Morals (关于进一步加强和改进未成年人思想道德建设的若干意见)</td>
<td></td>
<td></td>
<td>31 May 2004</td>
</tr>
<tr>
<td>Electronic Signature Act</td>
<td>Validates the authenticity of messages and establishes an electronic signature and authentication system.</td>
<td>National People’s Congress Standing Committee</td>
<td>28 August 2004 (revised 23 April 2019)</td>
</tr>
<tr>
<td>(电子签名法)</td>
<td></td>
<td></td>
<td>23 April 2019</td>
</tr>
<tr>
<td>Interpretation of Several Issues Concerning the Specific Application</td>
<td>Includes the protection of minors’ online information in the scope of legal management.</td>
<td>Supreme People’s Court</td>
<td>3 September 2004</td>
</tr>
<tr>
<td>of Law in Criminal Cases Using the Internet, Mobile Communication,</td>
<td></td>
<td></td>
<td>3 September 2004</td>
</tr>
<tr>
<td>and Audio Channels to Produce, Duplicate, Publish, Sell, and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disseminate Obscene Digital Information (关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notice on the Purification of Online Games (关于净化网络游戏工作的通知)</td>
<td>Establishes rules to unify ideological work and “purify” the online games market.</td>
<td>Ministry of Culture, Ministry of Industry and Information Technology.</td>
<td>9 June 2005</td>
</tr>
<tr>
<td>Internet Email Service Management Measure (互联网电子邮件服务管理办法)</td>
<td>Regulates the behaviors of internet email service providers.</td>
<td>Ministry of Industry and Information Technology</td>
<td>30 March 2006</td>
</tr>
<tr>
<td>Minor Protection Law (中华人民共和国未成年人保护法)</td>
<td>Stipulates the protection of minors in online activities.</td>
<td>National People’s Congress Standing Committee</td>
<td>29 December 2006</td>
</tr>
<tr>
<td>Regulation on the Administration of Internet Audio-Video Program Services (互联网视听节目服务管理规定)</td>
<td>Clarifies the responsibilities of national social organizations, establishes a business licensing system and copyright protection system for online audiovisual programs, clarifies the responsibilities of main funders and operators of business units, etc.</td>
<td>State Administration of Radio, Film, and Television, Ministry of Industry and Information Technology</td>
<td>20 December 2007 (revised 28 August 2015)</td>
</tr>
<tr>
<td>Announcement on Regulating the Content Review and Declaration of Imported Online Game Products (关于规范进口网络游戏产品内容审查申报工作的公告)</td>
<td>Requires applications for licenses, review, termination, and change of operating systems.</td>
<td>Ministry of Culture [文化部]</td>
<td>24 April 2009</td>
</tr>
<tr>
<td>Notice on Strengthening the Management of Online Currencies in Online Games</td>
<td>Establishes strict market access rules, conducts risk prevention, and strengthens supervision.</td>
<td>Ministry of Culture, Ministry of Commerce</td>
<td>4 June 2009</td>
</tr>
<tr>
<td>(关于加强网络游戏虚拟货币管理工作的通知)</td>
<td>Reporting Guidelines for Online Game Virtual Currency Issuing Companies and Online Game Virtual Currency Trading Companies (网络游戏虚拟货币发行企业，网络游戏虚拟货币交易企业申报指南)</td>
<td>Establishes reporting and processing rules for virtual currency in online games.</td>
<td>Ministry of Culture</td>
</tr>
<tr>
<td>Notice on Improving and Strengthening the Management of Online Game Content (关于改进和加强网络游戏内容管理工作的通知)</td>
<td>Establishes a business work unit self-regulation, game content supervision, and social supervision system.</td>
<td>Ministry of Culture</td>
<td>13 November 2009</td>
</tr>
<tr>
<td>Law on the Conservation of State Secrets (保守国家秘密法)</td>
<td>Incorporated classified information systems into confidentiality management and implemented a hierarchical protection system.</td>
<td>National People’s Congress Standing Committee</td>
<td>29 April 2010</td>
</tr>
<tr>
<td>Interim Measures for the Management of Online Games (网络游戏管理暂行办法)</td>
<td>Establishes a business licensing, content review, self-examination, virtual currency circulation prohibition system, and game operator corporate responsibility system.</td>
<td>Ministry of Culture</td>
<td>3 June 2010 (revised 15 December 2017)</td>
</tr>
<tr>
<td>Decision of the Standing Committee of the National People’s Congress on Strengthening Network Information Protection (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)</td>
<td>Establishes rules to protect the privacy of personal information and ensure the responsibility of internet service providers.</td>
<td>National People’s Congress Standing Committee</td>
<td>28 December 2012</td>
</tr>
<tr>
<td>Interim Provisions on the Development and Management of Instant Messaging Tools Public Information Services (即时通信工具公众信息服务发展管理暂行规定)</td>
<td>Places CAC in charge of coordinating and guiding the development and management of public information services for instant messaging. Requires instant messaging tool service providers to implement their security management responsibilities. Requires users to register for accounts after passing real identity information authentication.</td>
<td>Cyberspace Administration of China</td>
<td>7 August 2014</td>
</tr>
<tr>
<td>Notice of the State Council on Authorizing the Cyberspace Administration of China Responsibility for Managing Internet Information Content (国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知)</td>
<td>Grants CAC responsibility for the management of internet information content nationwide and makes it responsible for the supervision, management, and law enforcement of internet information content.</td>
<td>State Council</td>
<td>28 August 2014</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Provision on the Management of Internet User Account Names (互联网用户账号名称管理规定)</td>
<td>Places CAC in charge of the registration of internet user account names nationwide and requires service providers to supervise and manage the registration and use of internet user account names.</td>
<td>Cyberspace Administration of China</td>
<td>4 February 2015</td>
</tr>
<tr>
<td>Regulations on the Management of the Release of Information on Online Dangerous Goods (互联网危险物品信息发布管理规定)</td>
<td>Prohibits users from publishing information about “dangerous goods” (危险物品) online and mandates that businesses that operate internet information services must apply for a business license.</td>
<td>Cyberspace Administration of China</td>
<td>16 February 2015</td>
</tr>
<tr>
<td>Internet News Information Service Unit Interviews Regulation (互联网新闻信息服务单位约谈工作规定)</td>
<td>CAC is required to establish an interview system for internet news information service units.</td>
<td>Cyberspace Administration of China</td>
<td>28 April 2015</td>
</tr>
<tr>
<td>National Security Law (国家安全法)</td>
<td>Stipulates that the country should build a network and information security system to safeguard national cyberspace sovereignty, security, and development interests.</td>
<td>National People’s Congress Standing Committee</td>
<td>1 July 2015</td>
</tr>
<tr>
<td>Decision on Amending Some Regulations and Regulatory Documents (关于修订部分规章和规范性文件的决定)</td>
<td>Clarifies various regulations pertaining to network content.</td>
<td>State Administration of Press, Publication, Radio, Film, and Television</td>
<td>28 August 2015</td>
</tr>
<tr>
<td>Internet Information Search Service Management Regulation (互联网信息搜索服务管理规定)</td>
<td>Implements rules on the responsibilities of information security management systems, including information review, public information real-time inspection, emergency response, and personal information protection.</td>
<td>Cyberspace Administration of China</td>
<td>25 June 2016</td>
</tr>
<tr>
<td>Mobile Internet Application Program Information Service Management</td>
<td>Improves information content audit management of internet app store service providers.</td>
<td>Cyberspace Administration of China</td>
<td>28 June 2016</td>
</tr>
<tr>
<td><strong>Regulation (移动互联网应用程序信息服务管理规定)</strong></td>
<td><strong>Internet Live Streaming Services Management Regulations (互联网直播服务管理规定)</strong></td>
<td><strong>Cyberspace Administration of China</strong></td>
<td>4 November 2016</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>---------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Distinguishes between live streaming and reposting responsibilities; establishes a credit rating management system for internet live streamers and responsibilities for live streaming service providers.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cybersecurity Law (网络安全法)</strong></td>
<td>Establishes rules for the security of key information infrastructure operators, internet information security detection, early warning, and emergency response systems.</td>
<td><strong>National People’s Congress Standing Committee</strong></td>
<td>7 November 2016</td>
</tr>
<tr>
<td><strong>General Principles of Civil Law (民法总则)</strong></td>
<td>Clarifies that data and virtual property are civil objects and are transferable and inheritable.</td>
<td><strong>National People’s Congress</strong></td>
<td>15 March 2017</td>
</tr>
<tr>
<td><strong>Regulation on the Administration of Internet News Information Services (互联网新闻信息服务管理规定)</strong></td>
<td>Grants CAC responsibility for the supervision, management, and law enforcement of internet news information services nationwide. It also stipulates that internet news information services must “serve the people, socialism, adhere to the correct direction of public opinion, and promote the formation of a positive, healthy, and positive network culture, safeguarding national interests and public interests.”</td>
<td><strong>Cyberspace Administration of China</strong></td>
<td>2 May 2017</td>
</tr>
<tr>
<td>Mandates the establishment of an administrative law enforcement supervision system for internet content.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Internet News Information Services Licensing Management Implementation Rules (互联网新闻信息服务许可管理实施细则)</strong></td>
<td>Requires a news information service license to provide internet news information services to the public through websites, apps, forums, blogs, etc.</td>
<td><strong>Cyberspace Administration of China</strong></td>
<td>22 May 2017</td>
</tr>
<tr>
<td><strong>Measures for the Administration of Internet Domain Names (互联网域名管理办法)</strong></td>
<td>Establishes a system on domain name services, operations, maintenance, supervision, and management.</td>
<td><strong>Ministry of Industry and Information Technology</strong></td>
<td>24 August 2017</td>
</tr>
<tr>
<td><strong>Internet Forum Community Services Management Regulations (互联网论坛社区服务管理规定)</strong></td>
<td>Grants CAC responsibility for the supervision, management, and law enforcement of internet forum community services nationwide.</td>
<td><strong>Cyberspace Administration of China</strong></td>
<td>25 August 2017</td>
</tr>
<tr>
<td>Internet Forum Comment Services Management Regulations (互联网跟帖评论服务管理规定)</td>
<td>Grants CAC supervisory, management, and enforcement power over comments services nationwide and mandates that real identity registration information for users should be authenticated.</td>
<td>Cyberspace Administration of China</td>
<td>25 August 2017</td>
</tr>
<tr>
<td>Internet User Public Account Information Service Management Regulations (互联网用户公众账号信息服务管理规定)</td>
<td>Grants CAC responsibility for the supervision, management, and law enforcement of public account information services for internet users nationwide and stipulates that public account information service platforms and public account producers and operators shall “adhere to correct public opinion guidance and value orientation.”</td>
<td>Cyberspace Administration of China</td>
<td>7 September 2017 (updated 22 January 2021)</td>
</tr>
<tr>
<td>Internet Group Information Service Management Regulations (互联网群组信息服务管理规定)</td>
<td>Grants CAC responsibility for the supervision, management, and law enforcement of internet group information services nationwide and stipulates that internet group information service providers and users should “adhere to the correct orientation, promote socialist core values, cultivate a positive and healthy internet culture, and maintain a good internet ecology.”</td>
<td>Cyberspace Administration of China</td>
<td>7 September 2017</td>
</tr>
<tr>
<td>Management Measures for Content Management Practitioners of Internet News Information Service Units (互联网新闻信息服务单位内容管理从业人员管理办法)</td>
<td>Stipulates that CAC is responsible for the planning and guidance of the education and training of employees of internet news information service units nationwide and the supervision and inspection of their employment.</td>
<td>Cyberspace Administration of China [国家互联网信息办公室]</td>
<td>30 October 2017</td>
</tr>
<tr>
<td>Regulations on the Management of Security Assessments for New Technologies and New Applications of Internet News Information Services (互联网新闻信息服务新技术新应用安全评估管理规定)</td>
<td>Stipulates that CAC shall organize and carry out security assessments of new technologies and new applications of internet news information services.</td>
<td>Cyberspace Administration of China</td>
<td>30 October 2017</td>
</tr>
<tr>
<td>Decision of the Ministry of Culture on Abolishing and Amending Some Departmental Regulations (文化部关于废止和修改部分部门规章的决定)</td>
<td>Clarifies existing intradepartmental network content regulations.</td>
<td>Ministry of Culture</td>
<td>15 December 2017</td>
</tr>
<tr>
<td>Regulation Title</td>
<td>Description</td>
<td>Enforcing Agency</td>
<td>Start Date</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Weibo Information Service Management Regulation (微博客信息服务管理规定)</td>
<td>Mandates that Weibo service providers should establish and improve a rumor-refuting mechanism and should proactively take measures to refute rumors if they find that microblog service users publish or spread rumors or false information.</td>
<td>Cyberspace Administration of China</td>
<td>2 February 2018</td>
</tr>
<tr>
<td>Law on the Protection of Heroes and Martyrs (英雄烈士保护法)</td>
<td>Mandates CAC shall encourage and support the creation, production, and publicity of the deeds of heroes and martyrs and declares that it is prohibited to distort, vilify, blaspheme, or deny the deeds and spirit of heroes and martyrs.</td>
<td>National People’s Congress Standing Committee</td>
<td>27 April 2018</td>
</tr>
<tr>
<td>Regulation on the Security Assessment of Internet Information Services with Public Opinion Attributes or Social Mobilization Capability (具有舆论属性或社会动员能力的互联网信息服务安全管理规定)</td>
<td>Mandates that Internet information service providers with public opinion attributes or social mobilization capabilities are required to conduct security assessments.</td>
<td>Cyberspace Administration of China</td>
<td>15 November 2018</td>
</tr>
<tr>
<td>Counterterrorism Law (反恐怖主义法)</td>
<td>CAC is required to carry out targeted antiterrorism propaganda and education; telecom operators and ISPs must provide technical support and assistance to public security and national security agencies to prevent and investigate terrorist activities.</td>
<td>National People’s Congress Standing Committee</td>
<td>27 April 2018 (Revised)</td>
</tr>
<tr>
<td>Regulation on the Administration of Blockchain Information Services (区块链信息服务管理规定)</td>
<td>Stipulates that CAC is responsible for the supervision, management, and law enforcement of blockchain information services nationwide. It further stipulates that blockchain information service providers should implement information content security.</td>
<td>Cyberspace Administration of China</td>
<td>10 January 2019</td>
</tr>
<tr>
<td>Regulation on the Management of Internet Audio and Video Information Services (网络音视频信息服务管理规定)</td>
<td>Stipulates that CAC, culture and tourism, and radio and television departments at all levels shall carry out the supervision and management of online audio and video information services, and that providers and users shall “adhere to the correct political direction, public opinion guidance and value orientation, promote socialist core values, and promote the formation of a positive, healthy, upward, and good internet culture.”</td>
<td>Cyberspace Administration of China [国家互联网信息办公室]</td>
<td>18 November 2019</td>
</tr>
<tr>
<td>Regulation on the Ecological Governance of Internet Information Content (网络信息内容生态治理规定)</td>
<td>Encourages producers of online information content to publish information that promotes Xi Jinping Thought and Party line policies and forbids the publication of illegal information that endangers national security.</td>
<td>Cyberspace Administration of China</td>
<td>15 December 2019</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>Agency</td>
<td>Date</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Internet Information Service Algorithm Recommendation Management Regulations</td>
<td>Grants CAC responsibility for governance, supervision, and management of national algorithm recommendation services. Stipulates that algorithm recommendation service providers shall “not use algorithm recommendation services to endanger national security and social public interests, disrupt economic and social order, or spread bad information.”</td>
<td>Cyberspace Administration of China</td>
<td>31 December 2021</td>
</tr>
<tr>
<td>Provisions on the In-Depth Synthesis Management of Internet Information Services (互联网信息服务深度合成管理规定)</td>
<td>Grants CAC responsibility for coordinating the governance, supervision, and management of deep synthetic services across the country. It also bans the use of deep synthesis services (deepfakes) to engage in activities that damage the country’s image or infringe on social and public interests.</td>
<td>Cyberspace Administration of China</td>
<td>25 November 2022</td>
</tr>
<tr>
<td>18 March 2023 - 10 January 2023</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provisions on Administrative Law Enforcement Procedures of Cyberspace Affairs Departments (网信部门行政执法程序规定)</td>
<td>Mandates that CAC shall establish an administrative law enforcement supervision system and strengthen law enforcement capabilities.</td>
<td>Cyberspace Administration of China</td>
<td>18 March 2023</td>
</tr>
<tr>
<td>Provision on the Management of Information Services in Short-Range Ad Hoc Networks (近距离自组网信息服务管理规定)</td>
<td>Mandates that ISPs of short-range ad hoc networks must improve risk prevention capabilities, prevent and resist the spread of bad information, and report to CAC.</td>
<td>Cyberspace Administration of China</td>
<td>6 June 2023</td>
</tr>
<tr>
<td>Provision on the Governance of Internet Violent Information (Draft for Comments) (网络暴力信息治理规定 征求意见稿)</td>
<td>Mandates that ISPs are required to strengthen the management of internet user account and delete, block, disconnect, and restrict the dissemination of online violent information.</td>
<td>Cyberspace Administration of China</td>
<td>7 July 2023</td>
</tr>
<tr>
<td>Interim Measures for the Management of Generative Artificial Intelligence Services (生成式人工智能服务管理暂行办法)</td>
<td>Regulates the use of generative artificial intelligence technology to provide services that generate text, pictures, audio, video, and other content to the public within the territory of the People’s Republic of China.</td>
<td>Cyberspace Administration of China</td>
<td>13 July 2023</td>
</tr>
<tr>
<td>Specifications for the Website Platform to Accept and Handle Reports of Enterprise-Related Online Infringement Information</td>
<td>Requires domestic website platforms to accept and handle counterfeit information, misleading information that affects the public’s fair judgment,</td>
<td>Cyberspace Administration of China</td>
<td>10 August 2023</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10 August 2023</td>
</tr>
<tr>
<td>Rumored information, insulting information, and leaked information.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SOURCES CITED


Xie Xinzhou [谢新洲] and Li Jialun [李佳伦], “A Brief History of Macro Policy and Basic System Development of Internet Content Management in China” [中国互联网内容管理宏观政策与基本制度发展简史], Journal of Information Resources Management [信息资源管理学报] 3 (2019).


Xie Xinzhou [谢新洲] and Li Jialun [李佳伦], “A Brief History of Macro Policy and Basic System Development of Internet Content Management in China” [中国互联网内容管理宏观政策与基本制度发展简史], Journal of Information Resources Management [信息资源管理学报] 3 (2019).


Xie Xinzhou [谢新洲] and Li Jialun [李佳伦], “A Brief History of Macro Policy and Basic System Development of Internet Content Management in China” [中国互联网内容管理宏观政策与基本制度发展简史], Journal of Information Resources Management [信息资源管理学报] 3 (2019).


133 Shi Haijun [史海军], “Discussion on How the Government Should Deal with Internet Rumors — Taking the ‘Qin Huohuo’ Incident as an Example” [刍议政府如何应对网络谣言—以“秦火火”事件为例], Jiamusi Municipal Party Committee Propaganda Department News Center [佳木斯市委宣传部新闻中心], News Dissemination [新闻传播], 2015, 2.


135 Shi Haijun [史海军], “Discussion on How the Government Should Deal with Internet Rumors — Taking the ‘Qin Huohuo’ Incident as an Example” [刍议政府如何应对网络谣言—以“秦火火”事件为例], Jiamusi Municipal Party Committee Propaganda Department News Center [佳木斯市委宣传部新闻中心], News Dissemination [新闻传播], 2015, 2; Xie Xinzhou, “Promote Media Integration toward In-Depth Development” (推动媒体融合向纵深发展), People’s Daily, March 26, 2019. Translation.


140 Xie Xinzhou, “Promote Media Integration toward In-Depth Development” (推动媒体融合向纵深发展), People’s Daily, March 26, 2019. Translation.

141 Xie Xinzhou, “Promote Media Integration toward In-Depth Development” (推动媒体融合向纵深发展), People’s Daily, March 26, 2019. Translation.

142 Cyberspace Administration of China, Focus on Dual Bases and Dual Responsibilities, Adhere to Overall Planning and Hardening, and Advance with the Times to Promote the Healthy and Orderly Development of Guizhou’s Cyberspace Industry (着力双基双责 坚持统筹硬化 与时俱进推动贵州网信事业健康有序发展), March 9, 2017. Translation.


Economic Tactics
China’s Search for Security
Andrew Scobell,
Foreign-Journalists-Crackdown-Transparency/
2019.

China Is Getting Harder Every Month,”
Foreign Policy
May 27, 2021.
https://foreignpolicy.com/2021/05/27/china-expels-foreign-journalists-crackdown-transparency/.

Victor Cha, oral testimony for the House Committee on Rules,

Laura He, “China Suspends Business Ties with NBA’s Houston Rockets over Hong Kong Tweet,”

Jane Li, “Even Japanese Anime Celebrities Can’t Escape China’s Campaign over Taiwan,”
Quartz, October 1, 2020.
https://www.animenewsnetwork.com/interest/2020-10-28/virtual-youtuber-agency-hololive-to-disband-hololive-cn-group/165640; Peter Allen Clark, “What to Know about Blizzard, Hong Kong and the Controversy over Politics in Esports,”
Time, October 21, 2019.

Amy King, “Hurtind the Feelings of the Chinese People,”

Human Rights Watch, “China: Government Threats to Academic Freedom Abroad,”
March 21, 2019.
Foreign Policy, May 27, 2021.
https://foreignpolicy.com/2021/05/27/china-expels-foreign-journalists-crackdown-transparency/.

Ned Price, “Harassment of Foreign Journalists in the People’s Republic of China,”
Guardian, November 15, 2016.


231 Cyberspace Administration of China, The State Cyberspace Administration of China Instructs Relevant Local Cyberspace Offices to Investigate and Deal with Illegal Website Platforms and Accounts in Accordance with the Law (国家网信


protests.


99


371 Bilibili, “Ukraine War” (乌克兰战争). Translation. https://search.bilibili.com/all?vt=36128500&keyword=%E4%B9%8C%E5%85%B0%E6%88%98%E4%BA%89&from_source=weibtop_search&xspm_id_from=333.788&search_source=5&order=click.


102


2020 Departmental Budget and Related Information


Dong Shaopeng and Sun Dengfa, “Innovate the Internet Publicity Management Model and Strive to Improve the Ability to Guide Online Public Opinion —— Enlightenment from Nenjiang County to Strengthen the Construction of Online Public Opinion Guidance Ability” [创新互联网宣传管理理念着力提高网上舆论引导能力—嫩江县加强网上舆论引导能力建设的启示], Work Exchange 2013:8. Translation.


Dong Shaopeng and Sun Dengfa, “Innovate the Internet Publicity Management Model and Strive to Improve the Ability to Guide Online Public Opinion —— Enlightenment from Nenjiang County to Strengthen the Construction of Online Public Opinion Guidance Ability” [创新互联网宣传管理理念着力提高网上舆论引导能力—嫩江县加强网上舆论引导能力建设的启示], Work Exchange 2013:8. Translation.


410 Nan Ting, “For the First Time, the Cyberspace Administration of China to Publicly Select 9 Cadres” (中央网信办首次面向社会公开选拔 9 名处级干部), Xinhua, October 27, 2014. Translation.

411 Nan Ting, “For the First Time, the Cyberspace Administration of China to Publicly Select 9 Cadres” (中央网信办首次面向社会公开选拔 9 名处级干部), Xinhua, October 27, 2014. Translation.

412 Nan Ting, “For the First Time, the Cyberspace Administration of China to Publicly Select 9 Cadres” (中央网信办首次面向社会公开选拔 9 名处级干部), Xinhua, October 27, 2014. Translation.
107


110


