Stanford University

DIGICHINA

Behind the Facade of China's Cyber Super-Regulator

What we think we know—and what we don't—about the Cyberspace Administration of China

by:
Jamie P. Horsley

Published
August 8, 2022

This article is a preview of DigiChina's forthcoming in-depth report on the Cyberspace Administration of China.

On July 2, 2021, the Cyberspace Administration of China (**CAC**) abruptly launched its first ever cybersecurity review, targeting ride-hailing juggernaut DiDi Global just two days after it raised US$4.4 billion in a New York initial public offering, citing unspecified potential data and national security risks. The CAC also suspended new user registrations during the review, to prevent any expansion of risks. It then quickly issued additional orders to remove DiDi's apps from Chinese stores for illegally collecting personal information.

The CAC's actions caught markets by surprise. Under existing law and practice, DiDi's U.S. share sale did not require Chinese government approval, nor did it appear to involve the purchase or installation of goods and services that might endanger cybersecurity, which was the standard at the time to trigger a cybersecurity review per then-current legislation. Indeed, the CAC on July 10, 2021, published a proposed revision of applicable rules to require a cybersecurity review in advance of foreign listings by companies that qualify as critical information infrastructure operators and hold personal information of more than one million people.

After more than a year, during which DiDi's share price and market value halved since its New York listing, the CAC released a short statement on its decision to impose a US$1.2 billion fine on the company for unspecified violations of the cybersecurity, data security, and personal information protection laws. A more detailed question and answer between an unnamed CAC official and journalists listed many unlawful behaviors by DiDi but failed to explain what factors prompted the cybersecurity review. The full decision document for the review was withheld on national security grounds, obscuring the precise legal basis for the fine, and thus raising many questions and leaving other market participants without guidance on how to navigate China's complex and ever-evolving regulatory ecosystem for cybersecurity.

The CAC's surprise crackdown on DiDi, while not entirely unexpected, and its abrupt announcement concerning the DiDi fine, put an international spotlight on the secretive regulator and raised questions about the exercise and basis of its authority. Already subject to antitrust, labor, and privacy protection scrutiny, DiDi may have angered the CAC by moving ahead with its U.S. IPO after the regulator requested a delay to enable a cybersecurity review. The extended review process of more than a year—exceeding the original statutory scope and stipulated general period of 45 days or up to 3.5 months in contested cases (changed to five months under the revised rules)—and lack of a public decision on the case suggest the CAC may have been motivated more by political than data security concerns.

The CAC's original remit to manage and enforce requirements for online content has been expanded and codified in law to include policy and regulation on cybersecurity, data security, and privacy. The CAC thus enjoys potential jurisdiction as a supra-ministerial regulator over virtually all state and private sectors touched by nearly ubiquitous online activity. While other Chinese authorities have also been active in a regulatory rectification unleashed in November 2020 with the last-minute suspension of the Ant Group's planned IPO, the CAC is no ordinary Chinese regulatory agency. It is a merged party-state institution listed under the Central Committee of the Chinese Communist Party (**CCP**).

Originally established as a sub-office under the State Council known as the State Internet Information Office, it was always part of China's intertwined party-state propaganda system. In 2014, the State Council announced a "re-organized" and re-named CAC that was concurrently the state counterpart of a secretive CCP cybersecurity leading group's general office.

The CAC undertakes rulemaking and administrative licensing and punishment activities, generally in compliance with legally mandated procedures governing administrative agencies. It represents China in international cyber-related activities. However, it lacks many formal attributes of an administrative agency in the Chinese system, including institutional transparency and accountability. While the general principle that merged party-state entities should be treated as administrative agencies when performing state rather than party functions is gaining traction, the line between those two functions is not always clear. In light of the CAC's growing clout, its dual party-state status raises questions concerning its decision-making, daily operations, and accountability to its regulated public, which in addition to Chinese online actors includes foreign companies, organizations, and individuals doing business in and with China.

CAC's provenance

The CAC traces its origins to the CCP propaganda system. Its predecessor, whose Chinese name it still bears, was the State Internet Information Office (**SIIO**, 国家互联网信息办公室). The SIIO was initially established by the State Council General Office in May 2011 as an internal sub-office of the State Council Information Office (**SCIO**), itself a "government nameplate" of the CCP Central Committee's External Propaganda Office (**EPO**). The SIIO's announced mission was to unify multi-agency efforts to clean up the Internet, manage online content, news reporting and publication, and government online propaganda work—and investigate and punish website-related violations. The SIIO's first director was also the SCIO director, who concurrently held the party positions of EPO director and vice director of the CCP Central Propaganda Department (**CPD**).

The propaganda link continued when the SIIO was merged with the general office of the newly formed, multi-agency CCP Central Leading Small Group for Cybersecurity and Informatization (**Cyber LSG**). Reports on that LSG's first meeting in February 2014 revealed it was chaired by CCP General Secretary Xi Jinping, with State Council Premier Li Keqiang and propaganda doyen Liu Yunshan as vice chairs. A senior party propaganda official headed the Cyber LSG office (中央网络安全和信息化领导小组办公室), and concurrently served as SIIO director. In August 2014, the State Council authorized a "re-organized" (重新组建) SIIO to manage online information content and law enforcement. Although SIIO's Chinese name (generally shorted to 国家网信办) stayed the same, its official English name for state purposes was changed to the Cyberspace Administration of China, as used in China's official English-language media and in the state banner on its website. The official English-language announcement of the CAC's website launch indicated its dual identity: "Office of the Central Leading Group for Cyberspace Affairs, also named Cyberspace Administration of China, launched its official website on Dec 31."

A massive restructuring of party and state organs announced March 21, 2018, by the CCP Central Committee, intended to streamline governance and eliminate duplicative and overlapping party-state missions, elevated the Cyber LSG to a CCP central commission, whose official English name is the Central Cyberspace Affairs Commission (**CCAC**, 中共中央网络安全和信息化委员会). It also established a general office of CCAC. The CAC's party name, which appears in English next to the CCP hammer and sickle logo on its website, is accordingly the Office of the CCAC.

Not much is known about the composition and operation of the secretive commission. It is composed, like the former Cyber LSG, of members representing multiple agencies. Like other high-level deliberative bodies, the CCAC presumably deals with overall policy and coordination. However, not a single meeting of the CCAC has been reported. A report on a high-level April 2018 work conference on cybersecurity and informatization, convened shortly after establishment of the upgraded CCAC, identified Xi Jinping as chair of that commission, and Li Keqiang and Politburo Standing Committee Member and ideological theorist Wang Huning as vice chairs. A CAC report on a June 2022 meeting led by the CCAC to discuss online civilization construction provided a list of some 30 members of the CCAC and the Central Civilization Commission, but did not distinguish which members belonged to which commission. The CCAC sometimes co-issues policy documents with state agencies and acts unilaterally or collaborates with state agencies in other initiatives. The Cybersecurity Review Measures issued by the CAC and other authorities grant the CCAC legislated leadership and a final approval role in the review process.

The State Council formally made clear that the CAC was not part of its system in a March 22, 2018, companion notice to the CCP restructuring plan that set forth its reconstituted structure. That notice, which identified constituent components of the State Council system in a bulleted list, placed the CAC without a bullet under "State Council Offices" (办事机构) and stipulated that the dual-branded CAC was "a single institution with two nameplates," listed in the series of institutions directly under the Central Committee. Accordingly, the CAC would appear to not formally be an administrative agency, even when exercising the state functions assigned to it by the State Council in 2014 and subsequently codified in laws passed by the national legislature or authorized by the State Council. Indeed, while in some respects the CAC acts much like a normal administrative agency when undertaking regulatory activities, it demonstrates distinctly party attributes that raise questions as to its ultimate accountability.

The CAC's statutory basis

The CAC has cited the State Council's 2014 authorization to manage online information content and law enforcement as a legal basis for certain rulemaking and administrative punishment actions. Subsequent legislation substantially broadened the CAC's powers.

The 2016 Cybersecurity Law (**CSL**) codified the authority of the "state cybersecurity and information departments" (国家网信部门), generally deemed to refer to the CAC and, where appropriate, its local branches, to comprehensively plan and coordinate cybersecurity and related supervision and management efforts with multiple regulatory agencies having overlapping or complementary jurisdiction. This coordination authority specifically covered critical network equipment standards and certification and security reviews, including for outbound transfer of important and personal data. The 2021 Data Security Law (**DSL**) tasked the CAC with overall coordination of online data security and relevant regulatory matters and again authorized the CAC to regulate the export of important data, together with relevant State Council departments. China's 2021 Personal Information Protection Law (**PIPL**) then granted the CAC overarching powers for comprehensive planning, coordination, and supervision of personal information protection work and reiterated its authority over outbound personal information.

Despite the seemingly broad scope of CAC's statutory authorization, its direct rulemaking powers, apart from regulating information content and cross-border data transfer, remain unclear. For example, the CAC cited the CSL, DSL, and PIPL (the **Three Laws**) as the basis for its authority to unilaterally issue draft measures on outbound data transfer security assessment in October 2021 (now finalized). However, the CAC cited the State Council's specific authorization, in its 2021 annual legislative plan, for the CAC to lead the drafting of national regulations to implement the Three Laws in its November 2021 notice seeking comments on that draft. It also noted that it worked with unspecified relevant departments on the draft. Thus, while cautious in clarifying its legal basis and collaborative rulemaking in some cases, the CAC has also asserted jurisdiction in new and sometimes unexpected areas, including requiring prior security reviews of overseas listings that might endanger data and personal information security—and then unilaterally issuing a draft revision of the applicable measures to establish its legal authority to do so.

Administrative agency attributes

The CAC displays characteristics that suggest it is a state entity. It continues to carry its original Chinese name, which it uses for state purposes and translates as the *State* Internet Information Office, although now officially and consistently presented in English as the CAC. It also operates under its state identity when it represents China in meetings with global partners to collaborate on international privacy and data governance, digital poverty reduction, and promoting China's model of cyber governance.

However, many institutions that are formally identified as part of the party bureaucracy carry names containing "state" or "national," such as China's opaque Central National Security Commission (中央国家安全委员会), which has no state counterpart. In other cases, institutions are merely the state "nameplate" of the corresponding party entity, which the CAC, like the National Administration of State Secrets Protection, appears to be. The issue for determining its legal status hinges on whether the state-branded identity exercises independence from the party identity. Given the opacity surrounding how the CAC and CCAC operate and interact day-to-day, this is difficult to ascertain.

Notably, however, the laws giving the CAC statutory authority distinguish between it and "State Council departments," instead of referring to the CAC and "other" State Council departments, suggesting it is not deemed part of the State Council as a matter of law. Similarly, the draft regulations implementing the Three Laws contain numerous references to the "CAC, departments in charge, and regulatory departments" (国家网信部门和主管、监管部门), suggesting it is neither a government "department in charge" nor a regulatory department.

Nonetheless, the CAC's current leaders were all appointed through the State Council process, although only after their positions in the party counterpart were first announced: Director Zhuang Rongwen in August 2018 and Vice Directors Sheng Ronghua in May 2019, Niu Yibing in December 2020, and Cao Shumin in January 2022. The CAC also undertakes many activities characteristic of administrative agencies. However, it does not always comply with the increasingly comprehensive legal requirements of transparency, due process, and accountability applicable to such state agencies when they undertake rulemaking, licensing, enforcement, and dispute resolution.

Rulemaking

According to its website, since 2017 the CAC has under its state name been issuing departmental rules (部门规章), which are issued by State Council administrative agencies and are legally binding under China's Legislation Law. State Council regulations prescribe procedural requirements, such as public participation, for administrative agencies to follow when formulating department rules. While the CAC often adheres to the requirement to publish drafts for a 30-day comment period, on occasion it does so for shorter periods. It typically collects public input through the Ministry of Justice's central comment-seeking platform, as well as directly, as do other regulators such as the Ministry of Industry and Information Technology (**MIIT**). The CAC, however, has not publicly issued its own rulemaking provisions implementing the State Council requirements, as State Council regulatory agencies have, and does not publish annual rulemaking agendas, as called for by State Council regulations and as many regulatory agencies do.

Interestingly, the PIPL and the draft regulations implementing the Three Laws that were released for public comment by the CAC in November 2021 use a formulation that refers to "where laws, administrative regulations, *and CAC provisions* (法律、行政法规和国家网信部门规定) permit," rather than the usual "laws, administrative regulations, and departmental rules (法律，行政法规和规章)," which suggests CAC provisions may be deemed to not be departmental rules. If CAC rules are not legally binding departmental rules, what are they? One possibility is that they could eventually be formalized as a new category of legislation, as were the regulations formulated by the newly established State Supervision Commission, which is a joint (合署办公) party-state institution (co-located with the Central Discipline Inspection Commission) directly under the Central Committee. (This "joint" status is different from CAC's "one institution, two nameplates" label.)

CAC rules might also be a type of regulatory document (规范性文件) or intraparty regulation (党内法规). CAC issues regulatory documents, under the names of both the CAC and the CCAC Office or its Secretariat, and lists on its website. Such documents typically include opinions and notices and, when issued by administrative agencies, are not legally enforceable. Party institutions similarly issue party regulatory documents and, pursuant to CCP rulemaking provisions, intraparty regulations. Intraparty regulations traditionally were not applicable to non-party members but have increasingly been used to regulate areas formerly left to the state or issued jointly with state institutions.

Licensing

One of the CAC's original tasks was to approve various online content-related businesses, an activity that would normally be governed by the Administrative Licensing Law (**ALL**). The CAC has published procedures for obtaining press cards and online new reporting licenses that set forth requirements, as stipulated by the ALL. It also releases on its websites some lists of entities that have received licenses for various activities. However, the CAC has not published departmental rules implementing the ALL's procedural requirements, as most regulatory agencies have, which typically stipulate procedures for statutory rights to provide input on and file administrative appeals and lawsuits concerning licensing decisions.

Administrative punishment

The CAC was given enforcement authority from its 2011 founding. It typically uses its state name when issuing punitive orders, like ordering DiDi in 2021 to take down its apps and imposing on DiDi in 2022 the US$1.2 billion fine. Prior to the 2018 reorganization, the CAC issued provisions to enforce information content management (**Enforcement Provisions**). Those reference the Administrative Punishment Law (**APL**), which establishes procedures for imposing punishments such as fines, license revocations, and business closures. The Enforcement Provisions generally follow the APL prescribed procedures, permitting challenges and hearings regarding disputed actions, and stipulate that the CAC and its local branches are subject to related administrative appeals and litigation. However, unlike typical Chinese regulatory agencies, the CAC has not issued general rules to implement APL procedures for all its regulatory sectors. Moreover, it also has not updated the Enforcement Provisions after a substantial 2021 overhaul of the APL that strengthened due process rights and transparency, including publication of administrative punishment decisions that have social impact, such as the decision in the DiDi case. The CAC did not release any announcement, let alone a decision, after apparently concluding cybersecurity reviews of two other companies that were placed under review shortly after DiDi. Instead, those companies issued short statements that they had rectified unspecified security problems found in the review and would take effective measures to ensure the security of platform facilities and big data and maintain national security. Lastly, it is not clear that the Enforcement Provisions authorize the CAC to take action beyond the area of online information content.

Party attributes

As a merged party-state entity, the CAC displays strong party attributes along with the imperfect administrative agency indicia described above. Its explicit characterization as "one institution having two nameplates" and listing at least since March 2018 under the CCP Central Committee clarify its place as part of the CCP bureaucracy. The CAC's intertwining with the CCP and its propaganda system endures, through shared leadership with the CCAC Office, as well as with the CPD. Presumably, the CAC and the CCAC Office, as two nameplates for a single office, share additional personnel, although lack of transparency prevents confirmation. According to addresses provided in various rulemaking and other notices, they are co-located. The CAC's website graphically illustrates its dual identities: a party banner bearing the CCP hammer and sickle logo next to the CCAC Office name revolves continuously, alternating with its state banner carrying the State Council logo and CAC name.

Other data points indicate the predominance of the CAC's party identity, including that the CCAC Office name is always listed before that of the CAC. The CAC's current director, Zhuang Rongwen, is identified on the CAC website and in articles and media reports first as Deputy Director of the CPD, second as director of the CACC Office and, in third place, director of the CAC. The CAC's four deputy directors similarly are first identified as deputy directors of the CCAC Office.

Institutional opacity

Unlike most administrative agencies, the CAC does not publish its organizational structure, other than the names and brief biographies of its director and four deputy directors. It has not released its *sanding* ("three determinations") provisions (三定规定) that spell out an agency's main duties, structure, and personnel arrangements, as administrative agencies typically do—and as the CCP promotes.

Although CAC Deputy Director Niu Yibing sits on the national open government affairs leadership small group, the CAC does not publish an annual open government information (**OGI**) report, as required by State Council OGI Regulations applicable to administrative agencies. Some merged party-state entities like the National Administration of State Secrets Protection, and at least one local CAC, do publish OGI reports. The CAC has also not published departmental OGI implementation rules, as other agencies do. Its website does not contain the normal OGI webpage for proactive release of stipulated information, or provide a channel to request OGI. The CAC also does not publicly release its

annual budgets and final accounts, as do most administrative agencies, including fellow regulators such as the MIIT, and many party organizations.

China's Supreme People's Court held in 2018 that information produced by CCP organizations and CCP documents jointly issued with the government in general constitute party affairs information and need not be disclosed under the OGI Regulations. However, following the 2018 restructuring, after which several state entities "hang their nameplates" with the CPD, the State Council instructed the CPD that, in principle, joint party-state entities that independently perform statutory administrative functions in their own names should be treated as administrative organs. Accordingly, information they produce in their own name during the process of independently performing statutory administrative functions should be subject to OGI obligations. Nonetheless, while several merged entities that were listed under the Central Committee in the 2018 restructuring continue to issue annual OGI reports, others, like the CAC, do not.

The CAC does publish selected documents, licensing, and other regulatory information, and speeches on its website. However, like other CCP organizations, it sometimes releases summaries of documents rather than the full text, as with its opinions on implementing a CCP–State Council rule-of-law government initiative that reportedly promotes the transparent operation of administrative power.

Remedies

The only remedy for challenging CAC behavior offered on the CAC website is filing complaints concerning violations of CCP discipline or writing to the Director's Mailbox. Administrative agency actions are normally subject to administrative reconsideration and litigation, a petition process, and complaints and reports. Regulatory agencies typically have their own implementing rules governing administrative licensing, punishment, reconsideration, and other matters that set forth rights and procedures for bringing appeals and lawsuits, as well as seeking state compensation. There is no record that the CAC has established any relevant procedures implementing these fundamental administrative matters. Moreover, data security, and possibly cybersecurity, reviews conducted by the CAC will be final and not subject to appeal.

The CAC's recently finalized Outbound Data Transfer Security Assessment Measures provide only for an internal reassessment (复评) of any challenged result, which is final, although the Enforcement Provisions purport to grant rights for those who are dissatisfied with a CAC punishment decision to file for administrative reconsideration (复议) and litigation, both of which are processes governed by law. However, it is not clear whether the CAC has been or can be subjected to administrative reconsideration or sued, as can most administrative agencies other than those engaged in national defense and foreign affairs. Not many cases appear to have been attempted against the CAC bureaucracy, and none at the central level have been located. A 2019 judgment held that the defending Harbin CAC counterpart was not an administrative organ subject to lawsuits.[1] However, in a 2020 action that was dismissed on grounds that the requested information at issue was not subject to disclosure, the defendant Shanghai CAC counterpart had responded to the OGI request, and appears not to have contested its status as a defendant.[2]

Implications of the CAC's party identity

China's one-party political system has always confronted the issue of politics vs. professionalism—"red vs. expert." In recent years, the CCP has generally directed the state apparatus to pursue more effective governance to deliver economic growth and social stability through greater transparency, due process, and legal accountability, all under its political leadership. However, the CCP's heightened involvement in state governance in recent years threatens to reduce the accountability of merged party-state institutions like the CAC and to potentially politicize decision-making.

While the State Council (and some scholars) have espoused the principle that joint party-state entities should be treated as administrative agencies when performing state rather than party functions, the premise of that view is that such entities should follow administrative procedures when conducting state activities. It was not clear that the CAC had legal authority to require a cybersecurity review of DiDi's foreign listing, halt new user registrations, or order apps to be taken down. The CAC was, however, acting in accordance with recent CCP policy that called for enhanced scrutiny of cross-border data security.

To be sure, the CAC does seek public input, often cooperates with other agencies in drafting and issuing rules and regulatory documents, and generally acts like a normal government regulator in rulemaking. Shortly after its move against DiDi, the CAC did launch a rulemaking officially expanding its jurisdiction to cover advance review of overseas IPOs. However, it acted unilaterally in issuing the draft and approving the final version, rather than jointly with other regulators, as is required by the CSL, and as it had done when drafting and issuing the original cybersecurity review measures. We also do not know how the CAC and its Cybersecurity Review Office that issued the announcement of the DiDi review in July 2021 coordinate with the other authorities that are supposed to be involved in the review process.

The CAC has also established some procedures that comply generally with administrative laws applicable to various government activities. However, it has never released basic information about its structure and operations, including how it interacts with the also opaque CCAC in decision-making, let alone published OGI, financial, or other reports required of administrative agencies. Moreover, it is unclear whether any of the normal remedies available to the regulated public can be employed against the CAC, in the event it departs from due process and fairness in handling the wide array of regulatory matters within its purview. For example, it is not clear that the CAC could be held legally responsible in the manner that state organs may for mishandling personal information, although its personnel, as "public employees," and under CCP disciplinary rules, can be subject to internal sanctions under the CSL for leaking personal information.
Numerous other merged or joint party-state entities increasingly populate China's regulatory landscape. They typically are granted statutory powers by law, but are not subject to the law themselves. But the CAC seems to carry uniquely broad powers. The Chinese government's will to become a strong cyber power, paired with the importance of the Internet and cybersecurity to China's dual pursuit of national security and economic development, makes the CAC's politicization especially important. Its merged party-state status—making it a political and party, not administrative, organ—and consequent opacity thus raise concerns about its decision-making and accountability to the regulated public, which includes foreign companies, organizations, and individuals doing business and undertaking other activities in and with China.

Footnotes

[1] 巫宇达诉哈尔滨市互联网信息办公室一审行政裁定书，（2019）黑0109行初23号.

[2] 陈荣诉诉上海市互联网信息办公室（中共上海市委网络安全和信息化委员会办公室）政府信息公开答复函二审行政裁定书，（2020）沪03行终597号.

Abbreviations

Abbreviation	Full form	Chinese	Note
ALL	Administrative Licensing Law	行政许可法	
APL	Administrative Punishment Law	行政处罚法	Official translation: Law of the People's Republic of China on Administrative Penalty
CAC	Cyberspace Administration of China		Refers at once to both the CCAC Office and the SIIO, a single entity with two nameplates.

CCAC	Central Cyberspace Affairs Commission (of the CCP)	中共中央网络安全和信息化委员会	Literally: Central Commission for Cybersecurity and Informatization (CCCI)
CCAC Office	Office of the CCAC	中共中央网络安全和信息化委员会办公室	
CCCI	[see CCAC]		
CCP	Chinese Communist Party	中国共产党	
CPD	Central Propaganda Department (of the CCP)	中共中央宣传部	
CSL	Cybersecurity Law	网络安全法	
Cyber LSG	Central Leading Small Group for Cybersecurity and Informatization	中央网络安全和信息化领导小组	
DSL	Data Security Law	数据安全法	
Enforcement Provisions	Administrative Enforcement Provisions for Internet Information Content Management	互联网信息内容管理行政执法程序规定	
EPO	External Propaganda Office (of the CCP Central Committee)	中共中央对外宣传办公室	
MIIT	Ministry of Industry and Information Technology	工业和信息化部	Literally: Ministry of Industry and Informatization
OGI	open government information	政府信息公开	
PIPL	Personal Information Protection Law	个人信息保护法	
SCIO	State Council Information Office	国务院新闻办公室	Literally: State Council News Office
SIIO	State Internet Information Office	国家互联网信息办公室	
Three Laws	[CSL, DSL, and PIPL]		