CLAWS

ISSN 23939729

No. 138

2026

MANEKSHAW PAPER

Cyberspace Administration of China (CAC)

Abhishek Acharya

CENTRE FOR LAND WARFARE STUDIES

Field Marshal Sam Hormusji Framji Jamshedji Manekshaw, better known as Sam "Bahadur", was the 8th Chief of the Army Staff (COAS). It was under his command that the Indian forces achieved a spectacular victory in the Indo-Pakistan War of 1971. Starting from 1932, when he joined the first batch at the Indian Military Academy (IMA), his distinguished military career spanned over four decades and five wars, including World War II. He was the first of only two Field Marshals in the Indian Army. Sam Manekshaw's contributions to the Indian Army are legendary. He was a soldier's soldier and a General's General. He was outspoken and stood by his convictions. He was immensely popular within the Services and among civilians of all ages. Boyish charm, wit and humour were other notable qualities of independent India's best known soldier. Apart from hardcore military affairs, the Field Marshal took immense interest in strategic studies and national security issues. Owing to this unique blend of qualities, a grateful nation honoured him with the Padma Bhushan and Padma Vibhushan in 1968 and 1972 respectively.

Field Marshal SHFJ Manekshaw, MC
1914-2008

CLAWS Occasional Papers are dedicated to the memory of Field Marshal Sam Manekshaw

MANEKSHAW PAPER No. 138, 2026

Cyberspace Administration of China (CAC)

Abhishek Acharya

Centre for Land Warfare Studies
New Delhi

Editorial Team : CLAWS

ISSN : 23939729

Centre for Land Warfare Studies
RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010
Phone +91-11-25691308 Fax: +91-11-25692347
Email: **landwarfare@gmail.com**, website: **www.claws.co.in**
CLAWS Army No.33098

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an independent Think Tank dealing with national security and conceptual aspects of land warfare, including conventional & sub-conventional conflicts and terrorism. CLAWS conducts research that is futuristic in outlook and policy-oriented in approach.

CLAWS Vision: To be a premier think tank, to shape strategic thought, foster innovation, and offer actionable insights in the fields of land warfare and conflict resolution.

CLAWS Mission: Our contributions aim to significantly enhance national security, defence policy formulation, professional military education, and promote the attainment of enduring peace.

Disclaimer: The contents of this paper are based on the analysis of materials accessed from open sources and are the personal views of the author. The contents, therefore may not be quoted or cited as representing the views or policy of Government of India, or the Ministry of Defence (MoD), or the Centre for Land Warfare Studies.

Published in Bharat by

Sabre & Quill Publishers, New Delhi, India
www.sabreandquill.com / sabreandquill@gmail.com

Contents

- **Abstract 5**
- **Background.....7**
  - Aim 8
  - Scope.....8
  - Origins.....9
- **Evolved Structure 12**
- **Institutional Interworking of CAC.....15**
  - Horizontal Civil–Security Coordination 15
- **Military and Intelligence Overlay in Crisis 17**
- **Functional Roles and Power Dynamics 20**
- **Implications and Recommendations for India.....22**
- **Conclusion.....25**
- **Appendices.....26**
  - Appendix-A 26
  - Appendix-B.....28
  - Appendix-C 31
- **References.....33**

Cyberspace Administration of China (CAC)

Abstract

The Cyberspace Administration of China (CAC) is the cornerstone of China's Cyber Governance Architecture and reflects Beijing's strategic approach to treating cyberspace as a controlled, security-critical domain. Formally established in 2014, the CAC emerged from China's long-standing emphasis on information control, censorship, and regime stability, later expanding to include cybersecurity, data governance, and critical infrastructure protection.

At the apex of China's cyber system is the Central Cyberspace Affairs Commission (CCAC), chaired by President Xi Jinping. The CCAC provides unified strategic direction by integrating political security, ideological control, economic development, and national defence in cyberspace. The CAC functions as the executive arm of the CCAC, translating Party intent into enforceable regulations and operational coordination. Its institutional design gives it a dual identity of a Chinese Communist Party (CCP) organ and a state regulatory authority, allowing it to exercise exceptional influence across ministries, provinces, security agencies, and the private sector.

The CAC consolidated previously fragmented cyber responsibilities, becoming China's central authority for internet regulation, online content control, data governance, cybersecurity enforcement, and crisis management. Vertically, it operates through a nationwide network of provincial and Municipal

Cyberspace Administrations (MCAs), ensuring uniform and rapid execution of central directives at the local level. Horizontally, the CAC coordinates closely with key stakeholders like the Ministry of Public Security (MPS) for cybercrime and domestic enforcement, the Ministry of State Security (MSS) for counterintelligence and data security, the Central Propaganda Department for ideological guidance, and the Ministry of Industry and Information Technology (MIIT) for telecom and technical infrastructure oversight.

Rather than executing all functions directly, CAC orchestrates a dense ecosystem of specialized technical bodies. These include **TC260** for information-security standardization, **CNCERT** for cyber incident response, **CAICT** for policy research and technical assessments, and certification agencies responsible for security testing and compliance. Through these entities, CAC embeds political priorities into technical standards, regulatory audits, and platform governance.

A main feature of the CAC-led system is its **Crisis-Ready Architecture**. China deliberately blurs the distinction between peacetime governance and crisis response, allowing a smooth transition from peacetime to crisis. It is appreciated that during a crisis, CAC synchronizes civilian regulation with intelligence operations by MSS and military cyber operations conducted by the **Cyber Space Force (CSF)**, with coordination occurring at the Party apex rather than through conventional command chains. This enables seamless civil–military integration consistent with China's doctrine of integrated information warfare.

In essence, the CAC operates as a **'super-regulator'**, combining policy formulation, enforcement, ideological control, technical standard-setting, and national-security coordination. Its operating logic prioritizes Party authority over administrative autonomy, data-centric state power over individual privacy, and continuous

readiness over reactive crisis management. While rooted in an authoritarian political system, the CAC model demonstrates how institutional coherence and centralised coordination can generate significant cyber power.

Background

China's main strategic preoccupation in cyberspace has been domestic to prevent the spread of Western liberal thinking via the internet. From 2003 onwards, at the United Nations, it advocated the principle of 'cyber sovereignty' whereby states would be able to exert more control over their 'sovereign' portion of the internet. It was also in 2003 that China began implementing its 'Golden Shield Project', a programme of internet-based internal surveillance and censorship that became known as the Great Firewall of China, as an attempt to exert sovereign control. As part of this, from 2009 onwards, China undertook efforts to block certain US software applications (such as Facebook, Twitter, and YouTube) because of conflicts with its censorship laws[1].

In 2013, after ten years of partial reforms aimed at enhancing the country's cyber capabilities, the leaders of the Chinese Communist Party (CCP) were shocked by the revelations in the leaks by US defector Edward Snowden. The leaks made clear the continuing difference between the US and China on cyber capability, and particularly the weakness of China's cyber defences (in terms of protecting networks rather than controlling content).

In the pre-2014 times, the Chinese concept of information security had the unique characteristic of giving more importance to Internet content than to technical cybersecurity. This is in contrast to the Western idea of emphasising the technical threats to computer networks. This emphasis has led to a focused national effort to increase censorship and surveillance infrastructure rather than coordinate technical standards and enforcement mechanisms. As China puts more effort into defence against the threat of

terrorism, separatism, and extremism than defending against and technical exploitation by foreign intelligence services and economic cybercrime[2]. However, post 2014 China has increased its technical infrastructure for protection of its Critical Internet Infrastructure (CII), and in 2014 President Xi Jinping instigated a wave of internet-related organisational reforms and new laws and regulations, with the 27 Feb 2014, new Cybersecurity and Informatization Leading Group (CILG) was established. This displayed President Xi's personal commitment as the first party head to chair a leading small group related to information management. The CILG is chaired by Xi Jinping with ex-Premier Li Keqiang and ex Standing Committee member Liu Yunshan as vice chairs, with nineteen other Politburo or ministerial-level officials as members. The leading group prioritises internet security and information management as a single concept, trying to resolve the lack of an integrated approach that has been the root cause. President Xi has attributed to internet security and information management as 'two wings of one bird, two wheels on one car.'[3] A later name change in 2018, from "Central Leading Group" to "Central Cyber Commission" or the Central Cyberspace Affairs Commission (CCAC), was largely symbolic, signalling that this organization was not an ad hoc or provisional affair, and that digital policy would become one of the central pillars of the Party's overall program.[4]

Aim

The paper aims to understand the overall structure of the Cyberspace Administration of China (CAC) and its role in securing the cyber infrastructure.

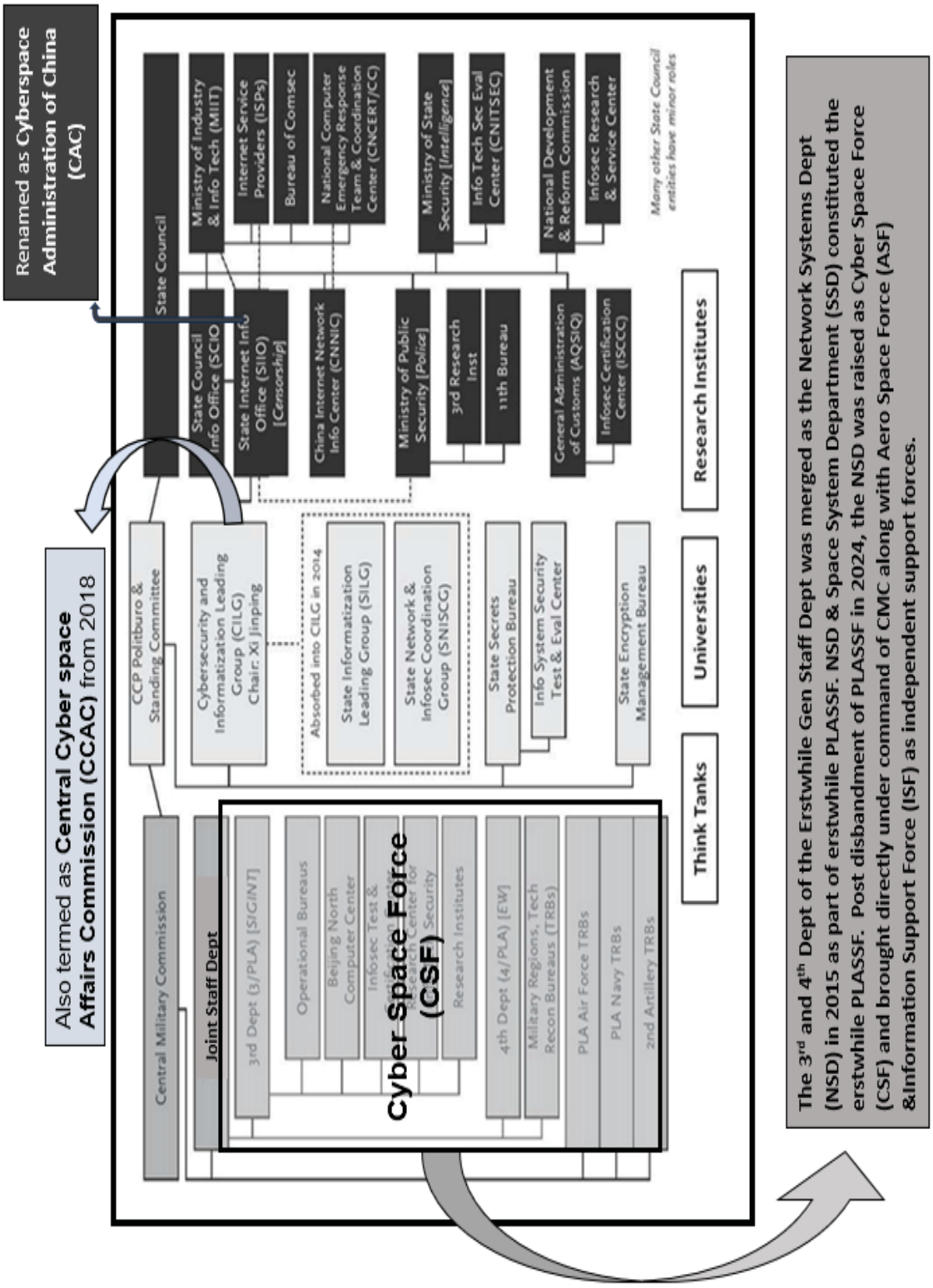
Scope

The paper covers Origins, Structure, and Institutional Interworking of the Cyberspace Administration of China with related Cyber organisations, including the military.

Origins

Initial Actors in the PRC Cyber Security Strategy Management. The agencies involved in China's Cyber Security Strategy Management can be divided mainly into civil and military sides. The military side consists of units within the PLA. This has been shown on the left side of the diagram given at next page. The civil side includes CPC, working groups, and institutions affiliated to the Chinese government, technology, telecommunication, globally active informatics companies, hacker groups, and cyber civil militia. The top decision-making bodies of the civil side are the Politburo Standing Committee, the State Council, and the Central Military Commission as it exists in all decision-making processes of China. The diagram depicts the mesh of official institutions that play a role in managing Chinese cybersecurity policy. At the centre of the chart are CCP entities, including the new Cybersecurity and Informatisation Leading Group (CILG), later termed as Central Cyberspace Affairs Commission (CCAC), chaired by Xi Jinping, which subsumed State Informatisation Leading Group (SILG) and State Network Infosec Coordination Group (SNISCG).[5]

The CCP State Secrets Protection Bureau manages all classified information and has been increasingly active in cybersecurity policy since the 2009 revision of the State Secrecy Law. The CCP State Encryption Bureau is in charge of encryption for the government, military, and industry, including restricting the export and import of any encrypted devices. China wants to enforce compliance with indigenous encryption standards. It demands access to all foreign commercial encryption codes, and later exempting those without encryption has been a constant source of friction with foreign firms in China. State Secrets Bureau manages all the important secret network systems and has been increasingly involved with the technological changes China is witnessing[6].



Source: Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron (ed), China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, Oxford University Press, 2015 and further amendments as per inputs in 2016 and 2024 by Lt Col Abhishek Acharya

Origin of The Cyberspace Administration of China. The Internet security management was initially handled by the State Internet and Information Office (SIIO), the Ministry of Industry and Information Technology (MIIT), the Ministry of Foreign Affairs, the Ministry of Public Security (MPS), and the PLA. However, there was no clear coordination mechanism for network security between these different agencies. This led to the formation of the Cyberspace Administration of China (CAC) in 2014.

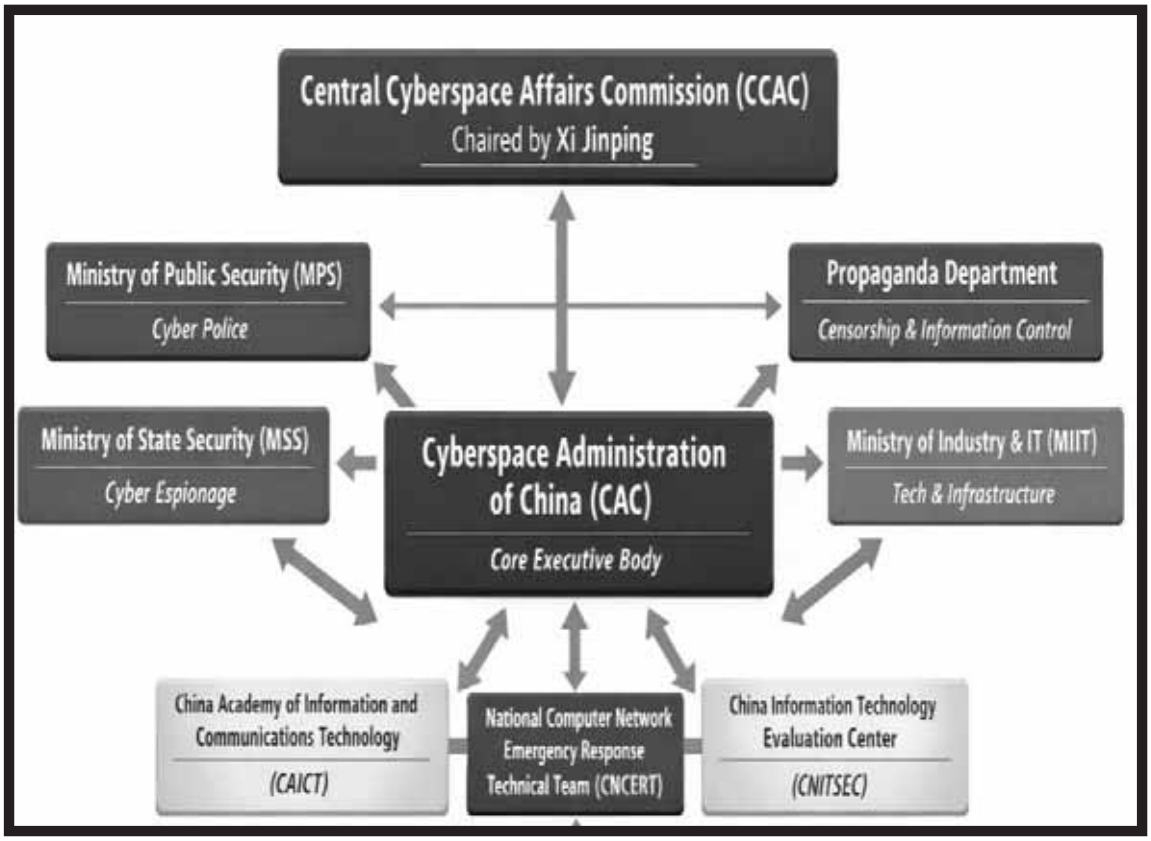
The CAC was raised in May 2011 as a subordinate office under the State Council Information office (SCIO) and termed as the State Internet Information Office (SIIO). In 2014, SIIO gained authority over all online content, effectively usurping the powers of the vast majority of the traditional propaganda apparat from the online sphere[7]. It gained direct access to the Office of the Central Cyberspace Affairs Commission (CCAC), chaired by Xi Jinping, in February 2014 and took over two departments from MIIT, covering cybersecurity coordination and informatisation promotion. Later that year, it gained authority over CNNIC, which runs the Chinese Domain Name System (DNS). It also took control over online emergency responder CNCERT/CC in 2018. Reflecting this broadening of responsibilities, its English-language name changed to Cyberspace Administration of China in 2014, although its Chinese-language name remains the same[8].

The CAC is the central Internet regulator, censor, oversight, and control agency for China. The CAC signifies an attempt to combine propaganda with technological innovation and development. The Cyberspace Administration of China (CAC) was formally established in 2014 to serve as China's top internet regulator, consolidating fragmented internet governance functions in China under a single authority. Functionally, CAC is the executive arm of the Central Cyberspace Affairs Commission (CCAC), a high-level body under the Chinese Communist Party (CCP) tasked with

determining cyberspace strategy and policy[9]. This "dual identity", as both a Party organ and a state regulatory body, gives the CAC unique power and reach, making it central to the CCP's efforts to institutionalize cyber-sovereignty, data security, and online ideological control. The CAC's institutional design reflects a broader trend in digital governance[10]. The CAC is responsible for cyberspace security and internet content regulation. Its major functions are directing, coordinating and supervising online content management and handling administrative approval of businesses related to online news reporting.

Evolved Structure

Evolved Functioning Architecture of the CAC. To understand the CAC's present role in Cybersecurity, it is important to understand its position in the overall Cyber Security Architecture of China, where CCAC is the apex authority giving strategic guidance, with CAC as its main executive body, which carries out coordination with other important stakeholders like the MSS and MPS. Propaganda Dept and MIIT. The CAC has certain specialised resources under it, like Technical Standardisation (TC260), National Computer Network Emergency Response Technical Team (CNCERT), etc. These are explained in subsequent paras.



Evolved Functional Architecture

Party-Centric Control Architecture. China's cyberspace governance operates within a party–state fusion model, where ultimate authority resides with the Chinese Communist Party (CCP) rather than the government bureaucracy. At the apex is the Central Cyberspace Affairs Commission (CCAC), as shown above, a CCP-led small group-style body chaired by the General Secretary[11]. The CCAC sets strategic direction for cyberspace policy, integrating political security, regime stability, economic development, and national defence. All major cyber actors, civilian, security, and military, ultimately align their activities with CCAC guidance.

Within this framework, the Cyberspace Administration of China (CAC) functions as the central executive and coordinating organ. Institutionally, CAC wears multiple hats, it is a CCP body, a State Council agency, and the operational office of the CCAC. This

hybrid status allows CAC to translate Party intent into enforceable regulations while coordinating horizontally across ministries and vertically down to provincial and local cyberspace offices called as Municipal Cyberspace Administrators (MCA).

Core Responsibilities of CAC. CAC's day-to-day functioning spans in four interlinked domains:

- **Content and Narrative Control**. Regulation of online media, social platforms, algorithms, and news dissemination to ensure alignment with Party ideology and political priorities.
- **Data and Cyber Regulation**. Implementation of the Cybersecurity Law, Data Security Law, and Personal Information Protection Law through licensing, inspections, security reviews, and compliance audits.
- **Platform and Technology Governance**. Oversight of major digital platforms, recommendation algorithms, cross-border data transfers, and critical information infrastructure.
- **Coordination and Crisis Management**. Acting as the civilian hub for cyber incident response and information control during emergencies.
- **Cyber Regulation via the Municipal CAC at the local level**. The CAC formalises the new agendas through national legislation and by setting up offices in each of the country's 31 provincial-level administrations. Further, there are a total of 137 of these local Cyberspace administrators for carrying out regulatory, development, and surveillance tasks as part of China's Internet governance.

Institutional Interworking of CAC

CAC does not execute all these tasks directly. Instead, it orchestrates with a dense network of specialised organisations. These important specialised organisations are explained as follows:-

Horizontal Civil–Security Coordination

- **Ministry of Public Security (MPS)**. MPS operates as the primary domestic enforcement arm. Its cyber police units investigate cybercrime, police online speech violations, and conduct technical surveillance. Through its specialized units (such as the *Network Security Protection Bureau* 11), MPS handles content violations, cybercrime, and security investigations on the ground. In practice, CAC sets policy and regulatory standards, while MPS executes law-enforcement operations under those frameworks [12].

- **Ministry of State Security (MSS)**. MSS focuses on counter-intelligence, political security, and external cyber espionage. While formally separate from CAC, MSS interacts closely with it on issues of data security, foreign technology risk, and cross-border information flows. CAC's data localization and security review regimes provide MSS with legal and administrative leverage to limit foreign access to Chinese data and platforms. Further Details of MSS are given in **Appx A.**

- **Central Propaganda Department**. The Propaganda Department provides ideological guidance and messaging priorities. CAC acts as the technical and regulatory executor of propaganda directives in the online space turning abstract narrative guidance into platform rules, content deletion standards, and algorithmic controls.

- **Ministry of Industry and Information Technology (MIIT)**. MIIT historically oversaw telecom infrastructure, networks, and technical standards; before 2015, it held significant influence over "cyberspace security." After CAC's rise, MIIT retained a supportive role. It remains deeply involved in technical infrastructure regulation, industrial IT policy, and network-market access. In technical standardization, MIIT collaborates with CAC via bodies like Technical Committee 260 (TC260)[13].

- **Municipal Cyberspace Administrations (MCAs) Local Execution of CAC Authority**. A critical but often underappreciated layer of China's cyber governance system is the role of **MCAs**. MCAs serve as the local execution arm of the CAC authority, translating central directives into routine governance and crisis response at the city level. MCAs are not autonomous regulators. They are embedded in a **vertically integrated Party–State hierarchy**, receiving policy priorities, enforcement campaigns, and political guidance from higher-level CAC bodies. These roles include censoring the internet to maintain social stability, regulating China's internet industry and infrastructure, and promoting the development of local digital economies.[14] They thus serve as the **"last-mile" implementers** of national cyber policy. Further Details are given in **Appx B**.

Technical and Quasi-Government Bodies. Certain important specialised technical entities operate under CAC's guidance. These organizations give CAC technical depth while keeping strategic control firmly political. These are as follows: -

- **Technical Standardisation (under TC260)**. The National Information Security Standardization Technical Committee (TC260) is a central body for creating and maintaining

information security standards in China. While nominally independent, TC260 is closely linked to CAC. Its leadership includes CAC officials, and its secretariat is housed in the China Electronics Standardisation Institute (CESI) [15]. TC260's membership spans multiple agencies, including CAC, MIIT, MPS, the State Secrecy Administration, and the State Cryptography Administration, showing how data and security technical standards are a deeply interagency affair. CAC's involvement in TC260 is instrumental. It uses the standards developed by TC260 as part of its regulatory toolkit for data protection, critical infrastructure, and cybersecurity certification.

- **National Computer Network Emergency Response Technical Team (CNERT)**. China's national incident response body is responsible for monitoring threats, coordinating responses, and information sharing during cyber incidents.

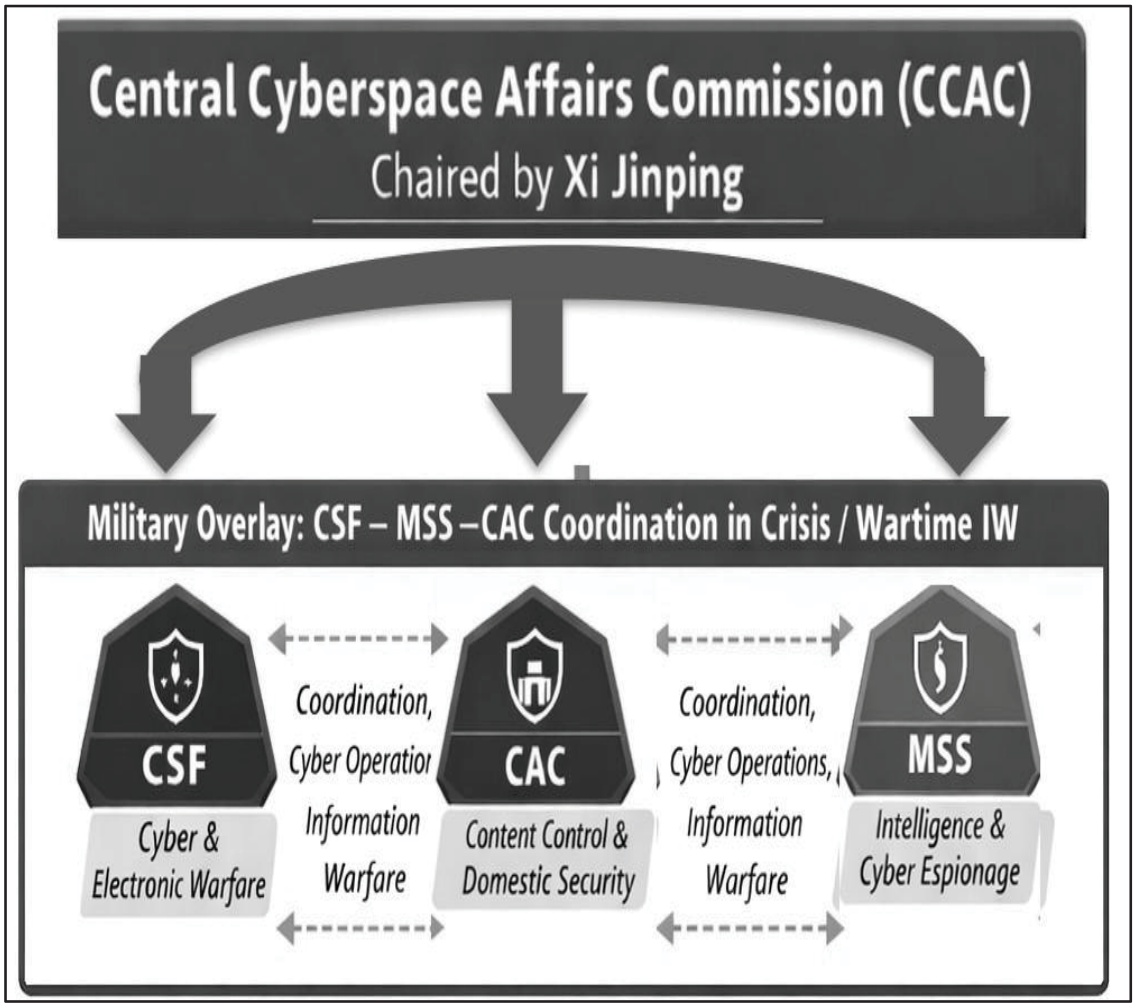
- **China Academy of Information and Communications Technology (CAICT)**. A research and standards body that provides policy support, technical assessments, and pilot frameworks for CAC regulations.

- **China Information Technology Evaluation Centre (CNITSEC)** conducts security testing and certification, particularly for critical systems and products.

Military and Intelligence Overlay in Crisis

Under normal conditions, the Cyber Space Force (CSF) operates outside CAC's authority. Its reporting through the Central Military Commission[16]. However, the governance system is designed for integration during a crisis or wartime. In such scenarios, the following actions are taken:-

- **CSF**. It conducts offensive and defensive cyber operations, electronic warfare, and information operations against adversary networks.
- **MSS** It provides intelligence preparation of the cyber battlespace, including attribution, human intelligence, and long-term access operations.
- **CAC**. It secures the domestic information environment by tightening content control, managing public opinion, restricting data flows, and ensuring civilian networks support national objectives.



Coordination. It is appreciated that coordination occurs only at the Party apex (CCAC and broader CCP national security mechanisms) rather than through formal command chains, enabling seamless synchronization without unified command. This enables seamless blending of civilian regulation, intelligence activity, and military cyber operations, which Chinese doctrine frames as integrated information warfare. Moreover, there will be a requirement for sharing real-time data of digital signatures / tech assessment of various cyber-attacks from outside, especially during a crisis, and therefore will warrant direct coordination between CAC and CSF; this will be in the domain of Cyber Emergency Response Team (CERT).

Smooth Transition from Peace Time to Crisis. A defining feature of the CAC-led system is the blurring of peacetime and crisis governance. Legal frameworks allow CAC to escalate from routine regulation to emergency control without formal declarations. This normalizes exceptional measures and ensures constant readiness for information confrontation.

Operating Logic of the CAC. Taken together, the functioning environment of CAC can be summarised as a permanent information-security posture characterised by the following attributes: -

- Party authority over the administrative hierarchy.
- Data-centric statecraft over individual-centric privacy.
- Crisis-ready legal frameworks over ad hoc emergency law.
- Civil–Military synchronisation over direct command.

In effect, CAC is the linchpin that transforms cyberspace into a governed battlespace, continuously aligning political security,

economic development, and coordination of military preparedness under the CCP leadership.

Functional Roles and Power Dynamics

CAC has shown its prowess by blocking foreign VPNs, closing and monitoring the most popular messaging application in China, WeChat, and coordinating cyber-attacks against anti-censorship groups like GreatFire.org, an organisation seeking to bring transparency to the Great Firewall. The various departments and their responsibilities are given at Appx C in brief. Putting all of the above together, the CAC is a super-regulator in China's cyberspace, with a mandate that straddles policy formulation, regulation, enforcement, and ideological control. The specific functional roles are illustrated as follows: -

- **Policy and Rulemaking**. CAC issues regulations and detailed implementing measures under China's major data/cyber laws (e.g., Cyber Security Law (CSL), Data Security Law (DSL), and the Personal Information Protection Law (PIPL)[a]. It is also empowered to draft sensitive rules on cross-border data transfer, algorithm regulation, and content governance[17].

- **Enforcement**. CAC coordinates security assessments, audits, and data-transfer approvals. It also has direct power to fine or order corrective action against platform operators based on the breach of the three laws.

a The **Cyber Security Law (CSL)** sets the network security obligations, protection of Critical Information Infrastructure (CII), and the Multi-Level Protection Scheme (MPLS), enabling inspections and penalties. The **Data Security Law (DSL)** treats all data as a national security asset, classifies "important" and "core" data, and tightens cross-border data transfers. The **Personal Information Protection Law (PIPL)** regulates personal data with extraterritorial reach and heavy penalties.

- **Coordination with Other Ministries**. CAC does not operate alone, it mandates, delegates, or co-opts other agencies (MIIT, MPS) into its regulatory regime to cover the full "cyber domain" (technical infrastructure, content, crime).
- **Standards and Certification**. By driving technical standardisation (via TC260), CAC shapes the technical baseline for compliance, product security, and data protection.
- **Security and Intelligence**. In coordination with MSS and MPS, CAC's data-governance role dovetails with national-security priorities. The CAC's policy direction supports not only digital regulation but also intelligence and stability objectives.

Furthermore, the CCP dictum is fundamental, CAC is embedded in the CCP's organisational structure (via CCAC), and its leadership overlaps with the Party's propaganda apparatus. This ensures that cyberspace governance is not purely bureaucratic, but also ideological.

Impingement of Democratic Rights of Chinese Citizens. The CAC significantly affects democratic rights in China by exercising extensive state control over online speech, information flows, and digital participation, thereby limiting freedoms commonly associated with democratic societies such as freedom of expression, access to information, and political dissent. As China's central internet regulator operating under the Chinese Communist Party's cyberspace governance framework, the CAC enforces content-control rules requiring digital platforms to remove information considered politically sensitive or harmful to "social stability," effectively shaping permissible public discourse online[18]. Through regulatory instruments such as the *Provisions on the Governance of*

the Online Information Content Ecosystem and enforcement campaigns like "Qinglang," the CAC obliges technology companies to conduct proactive monitoring and censorship, producing widespread self-censorship among citizens, journalists, and academics[19]. Scholars further observe that the CAC's authority under the Cybersecurity Law (2016), Data Security Law (2021), and Personal Information Protection Law (2021) enables extensive state access to data and strengthens digital surveillance capacities, which may deter political mobilization and criticism of government policies. Because enforcement standards are broadly framed and politically interpreted, citizens possess limited avenues for transparent legal challenge or independent judicial review, constraining online pluralism and civic participation. It can be said that CAC governance embodies China's doctrine of cyberspace sovereignty, where parties' security and information control take precedence over participatory democratic norms and individual expressive rights[20].

Implications and Recommendations for India

China's Cyberspace Administration (CAC) represents one of the most institutionally integrated cyber governance models globally. While operating within a democratic political system, India can take certain lessons from CAC that are relevant to India's evolving cybersecurity architecture. The following examines the implications of China's CAC-led system for India and identifies practical, democratic, and constitutionally compatible recommendations to improve India's cyber governance, crisis preparedness, and strategic coordination.

- **Institutional Coherence Is the Primary Source of Cyber Power**. China's experience demonstrates that cyber effectiveness derives less from technological superiority and more from institutional coherence. The CAC functions

as a central coordination hub that synchronizes policy formulation, regulation, enforcement, technical response, and crisis management across multiple organs. India's cyber ecosystem also has similar independent functional entities. Strategic coordination is vested in the National Cyber Security Coordinator (NCSC) under the National Security Council Secretariat (NSCS), while policy rests with MeitY, incident response with CERT-In, critical infrastructure protection with NCIIPC, cybercrime enforcement with MHA and I4C, intelligence with NTRO, telecom security with DoT[21], and military cyber operations with the Defence Cyber Agency and individual service Cyber organisations. CAC has been globally recognised as the most institutionally integrated cyber governance model. The level of integration and institutional coherence in the Indian context needs to be determined and tested, as there are multiple ministries involved.

- **National Level Doctrine for Cyberspace Operations**. The Joint Armed Forces Doctrine for Cyber Space operations was released on 08 Aug 2025, a joint doctrine at the national level incorporating NSCS, Meity, NTRO, MoD, MHA etc needs to be formulated for defining escalation thresholds, lead authority, inter-agency coordination, and integration with military cyber operations. This will enable a smooth transition from peace time to a crisis.

- **Crisis Ready Architecture**. The CAC system is designed for continuous readiness, with no sharp institutional distinction between peacetime and crisis governance. Legal authorities, institutional relationships, and operating procedures allow rapid escalation without ad hoc restructuring. The cyber incidents in India are often treated as technical disruptions or law-and-order issues rather than

as strategic national security challenges. Though the National Cyber Crisis Management Plan (NCCMP) has been in place, the details are not known. A whole-of-nation approach is required for a long-term solution to the problem.

- **Local Level Execution is Essential for Scale and Speed**. China's use of provincial and municipal CACs demonstrates that cyber governance must possess territorial depth. Central policy is multiplied through standardised local execution bodies that conduct inspections, enforce compliance, and escalate controls rapidly. India's system relies heavily on central agencies, while state-level cyber capacity remains uneven. State police cyber cells and sectoral CERTs operate with varying capability, limited standardization, and weak vertical integration. There is a requirement to create State Cyber Coordination Cells aligned vertically with CERT-In and NCSC at the centre so that both state and centre work in tandem, with the state benefiting from the centre. Also, there is a requirement to enhance CERT-In's authority to mandate technical measures during active incidents.

- **Cyber Governance to be Treated as a Strategic Domain**. CAC treats cyberspace as an integrated domain encompassing political security, economic development, data governance, public opinion, and military preparedness. Cyber regulation is therefore aligned with industrial policy, data sovereignty, and strategic competition. India's approach remains largely sectoral and defensive, emphasising cybercrime prevention, infrastructure protection, and IT risk management. India needs to utilise cyber governance more as a tool of strategic statecraft and economic resilience.

Conclusion.

The Cyberspace Administration of China (CAC) exemplifies modern China's integrated cyber-governance model combining Party authority, state regulatory power, and intelligence oversight. Its institutional design reflects a deliberate strategy to unify digital regulation, ideological control, and national security under a centralized, politically embedded body. Understanding the CAC's structure and its interworking with MIIT, MPS, MSS, and TC260 is essential for grasping how China approaches cybersecurity, data governance, and the future of its digital sovereignty.

Appendices

Appendix-A

Ref para 15 (b)

Ministry of State Security (MSS)

1. The MSS (China's primary intelligence agency) intersects with CAC on matters of national security, data security, and cyber-espionage. MSS is the key player in the military-civil fusion programme of China. They coordinate with military research institutes, military academics, and such civilian institutions, industries, and think tanks both within and outside the country. It is engaged in economic intelligence, counter-intelligence and economic espionage activities in China and internationally to protect the economic interests of China. MSS is engaged in the acquisition of foreign companies, mergers and acquisitions (M&A), economic espionage, conceptualisation and execution of information propaganda and campaign through national and international media, either by themselves or mostly through covert operations through networks of shell companies, both Chinese and non-Chinese, located in the respective countries. These shell companies collect data; process and analyse the same in the name of Big Data and IT services in the respective countries.

2. The modus operandi is to outsource the task of data collection, processing, and analysis as export of IT services. The analysis, along with certain raw data, is passed to Chinese agencies. The overall supervision is performed by MSS with the help of different non-state actors, state actors and Chinese companies. It coordinates with companies for the acquisition and development of Cyber tools for the purpose of gathering intelligence and surveillance. Over a period, MSS has gained expertise and operates with greater sophistication in its tactics, techniques, and procedures, and

extends its operations covering the entire globe. Several of the Advanced Persistent Threats (APT) like APT 3, APT 10, APT15, APT 20, and APT 27, etc., are associated with MSS and operations cover the entire globe.

3. MSS has emerged as a highly capable institution in cyberspace, demonstrating increasing sophistication and operational security while undertaking a global campaign of cyber espionage for economic, political, and strategic purposes. According to policy analysis, MSS plays a supervisory role, particularly under China's Data Security Law (DSL), when data is considered a strategic national-security resource. In Chinese cyber strategy, intelligence agencies like MSS are integrated into broader state-party cyber-governance: MSS supports investigations and strategic direction, especially on high-risk, sensitive, or classified data[22].

Appendix-B

Ref para 15 (e)

Municipal Cyberspace Administrations (MCAS): Localised Execution of China's Cyber Power

1. Municipal Cyberspace Administrations (MCAs) constitute the most operationally decisive yet analytically underexamined layer of China's cyber governance system. While the Cyberspace Administration of China (CAC) provides national-level orchestration, MCAs translate strategic intent into continuous, territorially grounded control of cyberspace. Without MCAs, CAC's authority would remain declaratory; with them, it becomes executable.

2. **Institutional Positioning and Authority**. MCAs are vertically subordinate to provincial and central CAC bodies and horizontally embedded within municipal Party–state structures. They derive authority not from independent statutory mandates but from Party leadership mechanisms, administrative delegation, and campaign directives. There is a total of 137 MCAs spread across China[23].

3. **Multi-Role Functional Design**. These roles include censoring the internet to maintain social stability, regulating China's internet industry and infrastructure, and promoting the development of local digital economies. The priorities of these roles shift dynamically based on political priorities and threat perceptions, allowing flexible governance in respective provincial municipalities. These are explained as follows: -

(a) **Regulatory.** Enforcement of platform compliance, data governance rules, and cybersecurity standards;

(b) **Developmental**. Support for local digital economy initiatives, smart-city projects, and technology firms;

(c) **Surveillance-oriented**. Online monitoring, content control, and coordination with public and state security organs. By analysing a unique dataset on areas of responsibility from 137 MCAs, it is found that MCAs are designed to prioritise their surveillance role by censoring the internet and maintaining social stability.

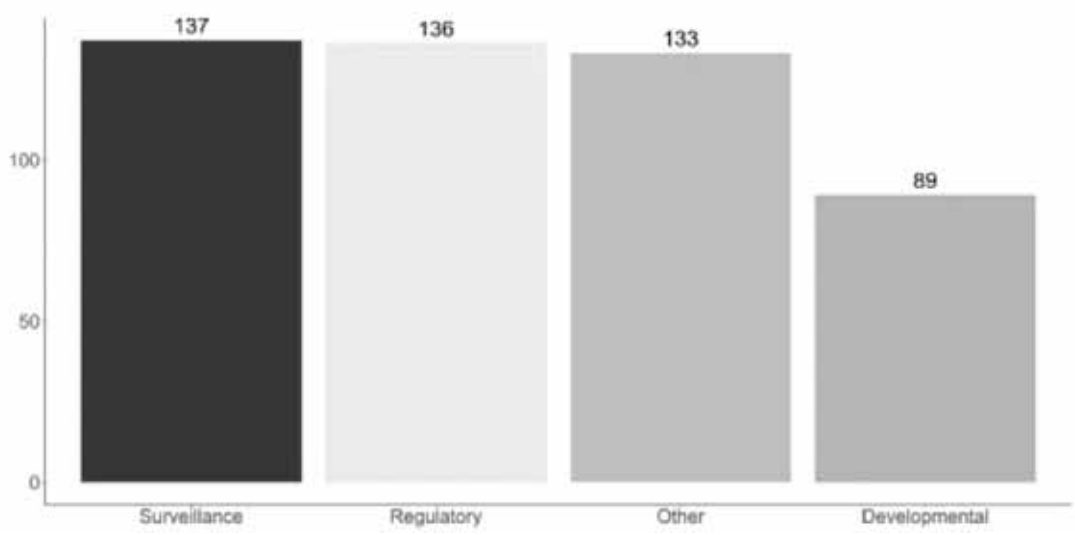
4. **Smooth Transition from Peace Time to Crisis**. A defining feature of MCAs is the absence of a clear boundary between routine governance and crisis response. The same authorities, personnel, and technical systems used for everyday regulation are immediately repurposed during emergencies. This design enables rapid escalation without legal or organizational delay.

5. **Embedded Security Coordination**. At the municipal level, MCAs maintain standing coordination mechanisms with Public Security Bureaus, State Security offices, and local propaganda departments. These relationships ensure fast convergence of intelligence, enforcement, and narrative control, reinforcing the CCP's ability to dominate the information environment during periods of stress.

The Multiple Roles of MCAs in China's Internet Governance.

6. **MCAs as Strong Surveillance and Regulatory Actors**. Ref the table below, it has been found that, of the three assigned roles, i.e., surveillance, regulatory, and developmental among the 137 MCAs in the dataset, surveillance is the most universally assigned role, appearing in the responsibilities of all 137 MCAs. Regulatory roles follow closely, present in 136 of the 137 MCAs. In contrast, only 89 MCAs list developmental responsibilities[24]. This distribution reflects the hierarchical ordering of state roles discussed earlier, in

which surveillance and stability maintenance are prioritized within China's party-centric governance model. This brings out that the CAC, as the central organ of internet governance, is widely perceived as a strong surveillance actor. While regulatory roles are nearly universal and often coexist with surveillance roles, developmental roles appear more selectively assigned and may be contingent on local political-economic contexts. However, the presence of developmental roles in over 60% of MCAs (89 of 137) suggests that digital development remains a significant, if secondary, goal even within a system dominated by surveillance imperatives.



Number of MCAs Assigned Surveillance, Regulatory, or Developmental Roles

Source: Data compiled by the authors from 137 online MCA budget reports. "Other" denotes tasks beyond the three state roles, typically of a purely administrative nature, such as managing the daily operations of the MCAs or developing their internal organisational capacity.

Article: Three Faces of the State in Local Cyberspace Administrations: Development, Regulation, and Surveillance in China's Internet Governance, 08 Oct 2025, Journal of Chinese Political Science.

Appendix-C

Ref para 22

Departments under CAC[25]

1. **Bureau of Policies and Regulations**. Focuses on internet issues; drafts internet policies, regulations, and other key documents; offers policy suggestions for internet and IT, and reviews documents for standardisation.

2. **Bureau of Network Security Coordination**. Supervises the general management of network security and cooperation. Bureau of Network Data and Technology. Looks after issues on network data and resolves technical problems.

3. **Bureau of International Cooperation**. Coordinates and handles international communication and coordination on internet issues.

4. **Bureau of Mobile Network Management**. Coordinates and manages mobile networks.

5. **Bureau of Informatization Development**. Promotes the advancement of IT and the development of digitization in other sectors.

6. **Bureau of Network News Information Communication**. Overseas, the distribution of public information and news is in online media.

7. **Bureau of Comprehensive Coordination, Management and Law Enforcement Supervision**. Supervises coordination between bureaus and law enforcement inspection on internet issues.

8. **Bureau of Emergency Management**. Develops emergency action plans and conducts the ministry's response to emergencies related to internet issues.

9. **Bureau of Planning and Finance**. Manages budget and expenses; organises internal audits and performance examinations; offers finance, taxation, and pricing recommendations and manages ministry finances and assets.

10. **Bureau of Internet Social Work**. Promotes social networks for internet issues and takes part in the management of online communities.

11. **Bureau of Network Comments**. Overseas public opinions on the internet. It has the authority to collect, check, issue warnings and delete certain internet posts and videos.

12. **Bureau of the Secretary**. Manages internal dissemination of information, communications, and security safeguards.

13. **Bureau de Cadre**. Manages human resources, including issues of retired cadres.

References

1 IISS, CYBER CAPABILITIES AND NATIONAL POWER: A Net Assessment date 28 Jun 2021.

2 China in the Cyber Domain. Maj Gen PK Mallick, 2022.

3 Ibid.

4 Creemers, Rogier et al., "China's Cyberspace Authorities Set to Gain Clout in Reorganization", New America, March 26, 2018

5 China in the Cyber Domain. Maj Gen PK Mallick, 2022.

6 ibid

7 "Notice concerning Empowering the Cyberspace Administration of China to be Responsible for Internet Information Content Management Work", China Copyright and Media, August 26, 2014,

8 China's Cyber Governance Institutions Dr. Rogier Creemers | Summary January 2021 by Leiden Asia centre

9 Chinafy, What is the Cyberspace Administration of China (CAC)? By Gabrielle Roper posted on 02.Jun.25

10 Springer nature Three Faces of the State in Local Cyberspace Administrations: Development, Regulation, and Surveillance in China's Internet Governance. 10 Nov 2025

11 In the league of its own: The CAC, The Diplomat Mercy A .Kuo 28 Mar 2023

12 China in the Cyber Domain. Maj Gen PK Mallick, 2022.

13 Teneo, China Cybersecurity and Data Regulation What Multinationals Should Know. Oct 2021

14 Three Faces of the State in Local Cyberspace Administrations: Development, Regulation, and Surveillance in China's Internet Governance, 08 Oct 2025 Journal of Chinese Political Science

15 Leiden Asia Centre China's Cyber Governance Institutions Jan 2021

16 China's Cyber Operations: The Rising Threat to American Security, Pg 34, 2022 by Margin Research LLC

17 IAPP, China's key enforcement agencies and lessons learned from recent actions 31 Aug 2021

18 The Three Laws: The Chinese Communist Party Throws Down the Data Regulation Gauntlet by Washington and lee law review Volume 79 Issue 3 Summer Article 10, 2022

19 Rogier Creemers, "Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century," *Journal of Contemporary China* 05 Sep 2016

20 The Three Laws: The Chinese Communist Party Throws Down the Data Regulation Gauntlet by Washington and lee law review Volume 79 Issue 3 Summer Article 10, 2022.

21 Ministry of Home Affairs, Cyber Security Infrastructure PIB 02 Dec 2025

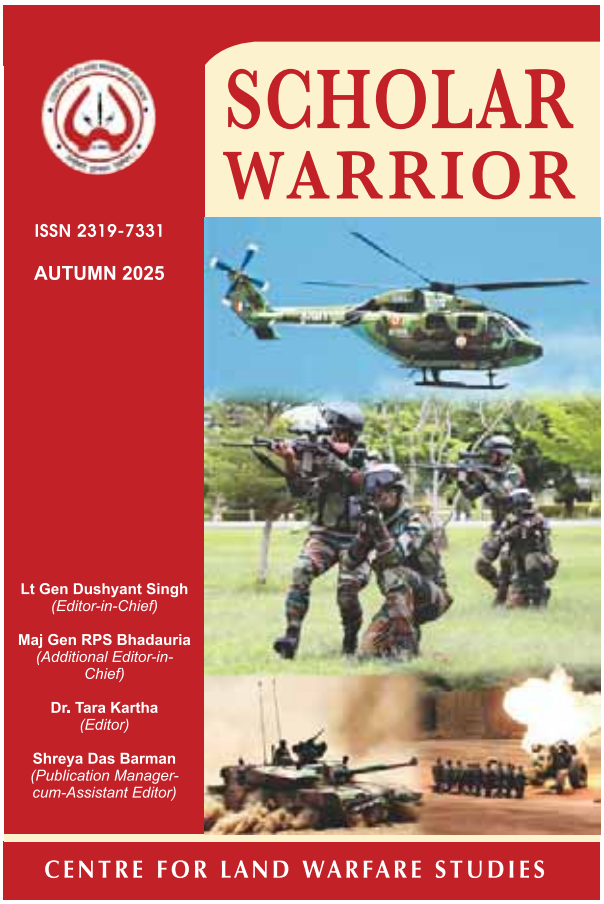
22 Cyber-DNA-of-China by VIF, Dr Gulshan Rai, Mar 2022

23 Three Faces of the State in Local Cyberspace Administrations: Development, Regulation, and Surveillance in China's Internet Governance 08 Oct 2025 Journal of Chinese Political Science

24 ibid

25 China in the Cyber Domain. Maj Gen PK Mallick, 2022.

SUBSCRIBE NOW



SUBSCRIPTION RATES

IN INDIA
☐ Rs.500/- per copy

SAARC COUNTRIES
☐ US $ 15 per copy

OTHER COUNTRIES
☐ US $ 20 per copy

☐ Rs.1000/- Annual Subscription (2 issues)

TO SUBSCRIBE SEND YOUR REQUEST TO

Centre for Land Warfare Studies (CLAWS)
RPSO Complex, Parade Road, Delhi Cantt, New Delhi - 110010
Tel: +91-11-25691308
• Fax: +91-11-25692347 • Army: 33098
E-mail: landwarfare@gmail.com
www.claws.co.in

The "Cyberspace Administration of China (CAC)" is the central pillar of China's cyber governance architecture and reflects China's approach to treating cyberspace as a strategically controlled domain. Established in 2014, the CAC evolved from China's emphasis on information control and censorship into a powerful institution responsible for cybersecurity, data governance, online regulation, and critical infrastructure protection. Operating under the "Central Cyberspace Affairs Commission (CCAC)", chaired by Xi Jinping, the CAC integrates political security, ideological control, economic development, and national defence within a unified cyber framework.

The CAC functions both as a Party organ and a state regulator, enabling centralized coordination across ministries, provincial administrations, security agencies, and private technology firms. It works closely with the Ministry of Public Security (MPS), Ministry of State Security (MSS), and the "Ministry of Industry and Information Technology (MIIT)", while overseeing technical bodies such as National Computer Network Emergency Response Technical Team (CNCERT) and China Information Technology Security Evaluation Centre (CNITSEC). Its crisis-ready structure supports seamless civil–military integration, aligning cyber governance with China's broader doctrine of integrated information warfare and national security preparedness.

• • •

Lieutenant Colonel Abhishek Acharya was commissioned into the Corps of Signals in 2004. He holds a BE in Electronics and Telecommunication from National Institute of Technology (NIT) Raipur and MSc in Defence and Strategic Studies from DSSC Wellington. He has served in four Division Signal Regiments including an Armoured Division, two in Hight Altitude Areas near LAC and LOC and one in Assam. He has been OC Communication in a Corps, tenanted an appointment of GSO1 (China) and served in Army Centre of Electromagnetics (ACE), Mhow. He has commanded an Electronic Warfare Unit in North East and a Signal Unit in an Independent Armoured Brigade on the Western Borders. He is presently a Senior Research Fellow (SRF) at Centre For Contemporary China Studies (CCCS) at Ministry of External Affairs.

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an independent Think Tank dealing with contemporary issues of national security and conceptual aspects of land warfare, including conventional & sub-conventional conflicts and terrorism. CLAWS conducts research that is futuristic in outlook and policy oriented in approach.

CLAWS Vision: To be a premier think tank, to shape strategic thought, foster innovation, and offer actionable insights in the fields of land warfare and conflict resolution.

CLAWS Mission: Our contributors aim to significantly enhance national security, defence policy formulation, professional military education, and promote the attainment of enduring peace.

Website: www.claws.co.in Contact us: landwarfare@gmail.com

SABRE & QUILL

MRP: ₹ 100.00 US$ 5.00