Mobilizing Cyber Power: The Growing Role of Cyber Militias in China's Network Warfare Force Structure

Kieran Green

July 2025

Acknowledgements

The author extends heartfelt thanks to Winnona Bernsen and John Chen for their invaluable feedback during the drafting of this manuscript. Sincere appreciation also goes to Simon Weiss for his assistance in preparing the maps included in this report.

Table of Contents

List of Acronyms

Acronym	Full Name
AMS	Academy of Military Sciences
APT	Advanced Persistent Threat
CPPCC	Chinese People's Political Consultative Conference
CMC	Central Military Commission
CTF	Capture-the-Flag Competition
MCF	Military-Civil Fusion
MPS	Ministry of Public Security
MSS	Ministry of State Security
NCRE	National Computer Rank Examination
NDMC	National Defense Mobilization Commission
NDU	National Defense University
NPC	National People's Congress
PAFD	People's Armed Forces Department
PAP	People's Armed Police
PRC	People's Republic of China
PLA	People's Liberation Army
PLACSF	People's Liberation Army Cyberspace Force
PLAISF	People's Liberation Army Information Support Force
PLASSF	People's Liberation Army Strategic Support Force
SOE	State-Owned Enterprise
UAV	Unmanned Aerial Vehicle

Executive Summary

Over the past decade, the People's Republic of China (PRC) has undertaken a sweeping reform of its cyber reserve forces, transforming its cyber militia system from a peripheral asset into a strategically relevant component of the People's Liberation Army's (PLA's) broader cyber warfare architecture.[*] [1] Within China, cyber militias are paramilitary units composed of civilian volunteers operating under the dual leadership of local governments and the PLA. These units are organized by civilian work units (e.g. state-owned enterprises, universities, and the commercial technology sector) and are principally tasked with supporting the defense of critical network infrastructure, logistics systems, and communications platforms. While historically the role of cyber militia forces has been largely auxiliary in nature, they increasingly function as a regularized reserve force that trains alongside active-duty PLA units and that are integrated into Theater Command-level operational planning.

This report presents the first detailed study of China's cyber militia system since 2015. It draws from an analysis of 136 individual militia units, as well as authoritative Chinese-language military writings and mobilization documents in order to detail the structure, evolution, and operational role of China's modern cyber militia system. The report's key findings are as follows:

The Party-state's ongoing reforms to China's cyber militia system have greatly increased PLA network warfare resilience and surge capacity.

- China's cyber militia system provides the PLA with a scalable reserve force capable of expanding operational capacity in the network domain with minimal lead time. Unlike conventional reserve formations, which require intensive training in weapons systems and field operations, cyber militia units draw on civilian personnel who already possess high-value technical expertise in offensive cyber operations, network reconnaissance, and systems exploitation.
- As a result, the functional divide between China's active-duty cyber forces and its militia-based reserves is far narrower than in traditional military domains. Select militia units can pivot from rear-echelon support roles to frontline operational functions with little latency, allowing the PLA to surge capacity for broader, more sustained cyber campaigns at a scale that would otherwise be difficult to achieve using uniformed forces alone.

[*] In Chinese military nomenclature, the term "militia" (民兵) refers to paramilitary forces composed of civilian volunteers operating under the dual leadership of local governments and the PLA. In contrast, "reserve forces" (预备役部队) are formally organized, trained, and administered by the PLA as part of its structured military system. While these two categories are nominally distinct, many sources use the terms interchangeably within the PLA context, especially within discussions of operational roles and doctrine. For the purposes of this paper, the term "militia" is used by default, as it remains the more commonly encountered nomenclature. However, it is important to note that the PRC is increasingly training and integrating these forces into the PLA's order of battle in a manner that more closely resembles the role and function of traditional reserve units.

Cyber militia forces function as a key supplement to the PLA in high-risk contingencies such as cross-Strait operations or flare-ups in the South China Sea.

- PLA military officials and defense academicians have identified cyber militia forces as a vital supporting force for network operations in specific scenarios, such as a future Taiwan invasion contingency or crisis in the South China Sea. These units' familiarity with relevant local civilian networks, distributed architecture, and flexibility of employment offer the PLA a means of shoring up over-stretched active-duty units during periods of high demand.
- Authoritative PLA commentary suggests that these units will be used not only for rear-area support but also to supplement offensive cyber missions in South China Sea and cross-Strait scenarios. Cyber militia units train regularly in simulated offensive and defensive cyber operations and are expected to participate in tasks such as deception operations, public opinion control, and technical support for island landings and maritime operations.

China's cyber units are becoming more professionalized and diversified, with participation expanding beyond universities and SOEs to include elite commercial cybersecurity firms.

- Since 2018, the Party-state has implemented reforms to China's cyber militia structure that dictate stricter recruitment quotas, more regular joint exercises with PLA units, and more standardized training procedures. These policy "sticks" are accompanied by a number of "carrots" including incentives such as tax breaks, procurement preferences, and political branding in order to encourage participation from high-end private cybersecurity firms.
- Cyber militia units such as those operated by Antiy Labs and Qihoo 360 represent the vanguard of this effort. Such units contribute personnel, tools, and infrastructure to the PLA's mobilization system. These partnerships blur the line between state and private cyber capabilities and suggest that Chinese cybersecurity firms with global commercial reach may act as vectors for state-aligned operations in a conflict.

Introduction

Over the past decade, the People's Republic of China (PRC) has overseen a systematic expansion and restructuring of the People's Liberation Army's (PLA) cyber capabilities. This policy undertaking reflects the Chinese Party-state's growing emphasis on integrating cyber operations, electronic warfare, and emerging technologies such as artificial intelligence into joint operations and conventional warfighting doctrine.[2] Much of the PLA's progress in this domain has been driven by increased budgetary allocations, refined talent acquisition strategies, and a concerted focus on high-end capability development.[3] However, equally instrumental in this process has been the PLA's ability to draw upon the resources, personnel, and technical expertise of the private sector through various military-civil fusion (军民融合), or MCF initiatives.[*] [4] This strategy has facilitated the quiet but steady evolution of China's cyber militias from loosely organized auxiliaries into more capable, professionalized and operationally relevant reserve forces.

China's cyber militia system has matured considerably over the past decade, marked by both an expansion in organizational scope and a diversification of its personnel base. The aggregate number of cyber militia *fendui* (分队) or elements in the PRC has grown at a steady pace, as local defense mobilization authorities have stood up network warfare forces in order to comport with guidance from China's central military authorities.[†] [5] Moreover, the composition of these units has also changed. What began as a reserve force primarily composed of university-affiliated technical specialists and personnel from state-owned enterprises (SOEs) has expanded to include recruits from leading private-sector cybersecurity firms. At the same time, cyber militia units have grown more active, regularly participating in joint training exercises with PLA forces and other militia formations.

While considerable analytical attention has been paid to the role of civilian enterprises in enhancing the PLA's offensive cyber capabilities, the impact of military-civil fusion on the development of China's cyber militia forces remains comparatively underexamined. The last holistic study on this subject was conducted in 2015, leaving a notable gap in the literature despite the continued evolution of the cyber militia system.[‡] This absence is particularly significant given

[*] In Party-state nomenclature, the term "military-civil fusion" refers to the process of breaking down institutional silos and encouraging resource sharing between China's commercial sector and defense industrial base in order to facilitate military modernization.

[†] In PLA terminology, *fendui* (is a general term for units below the battalion level, such as squads, platoons, or companies. It contrasts with *budui* (部队), which refers broadly to units at the regiment level and above. In militia or auxiliary contexts, *fendui* is often used to describe smaller, task-specific detachments (such as those focused on cyber defense, communications, or logistics) that operate within a larger organizational framework.

[‡] For further reading see: Robert Sheldon and Joe McReynolds, "Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York: Oxford University Press, 2015), 188–222. For a broader survey of recent developments in China's national defense mobilization infrastructure see: Devin Thorne. *Inside China's National Defense Mobilization Reform: Capacity Surveys, Mobilization Resources, and "New-Type" Militias*. Recorded Future, March 10, 2022.

the expanding scale and strategic relevance of these forces. As an increasingly capable reserve component, cyber militia units afford the PLA greater operational flexibility in cyberspace, allowing for enhanced distribution of effort across mission types and improved surge capacity during periods of crisis or conflict.

Collectively, these units play an increasingly prominent role in China's broader defense mobilization system by supporting missions such as defending critical infrastructure, securing information systems, and guiding public opinion. Moreover, China's cyber militia system serves two vital ancillary functions. First, it allows the PLA to preserve its core operational forces for high-priority missions by offloading auxiliary and support tasks to less specialized units. Second, it provides a latent pool of highly skilled personnel who can be mobilized rapidly in response to crises or wartime exigencies. These two functions are becoming increasingly salient as the PLA continues to refine its force structure in preparation for potential conflict scenarios in key strategic theaters such as the Taiwan Strait and the South China Sea. By offloading lower-tier cyber defense and mobilization responsibilities to militia units, the PLA can achieve greater strategic economy of force by allowing elite cyber operators to focus on high-priority offensive and expeditionary missions.

This report examines the development of China's cyber militia system over the past 10 years. It begins by outlining the evolution of the legal and regulatory frameworks used to muster cyber militia forces, as well as changes in militia organization, recruitment methods, and procurement of equipment and infrastructure. The report then turns to the current structure and function of cyber militia forces, including the types of civilian work units that supply personnel, how these forces are integrated into the broader PLA order of battle, and the range of missions they undertake. The report also includes two case studies that provide insight into how the system operates in practice. The first focuses on Qihoo 360, a major Chinese cybersecurity firm that has established a dedicated cyber militia unit in coordination with local defense mobilization authorities. The second examines Antiy Labs, a commercial cybersecurity firm that operates China's largest single cyber militia element and serves as a national model for militia capacity building. The report concludes by assessing how these developments affect China's ability to compete with the United States and its allies in cyberspace, while also identifying key limitations and operational challenges facing the cyber militia system. An interactive map is appended to display the known locations and types of cyber militia units identified during this research.

Methodology

In order to assess the structure and capabilities of China's cyber militia forces, this research paper relies upon two broad categories of sources. The first source category is composed of articles, news reporting, and other authoritative commentary from PLA-affiliated military reporting and

peer-reviewed scholarship, with particular emphasis on sources affiliated with China's defense mobilization system. These materials detail how Chinese military thinkers and local defense authorities conceptualize the role of cyber militia units, and how that thinking has evolved over the past decade under Xi Jinping's leadership. The second category is composed of a partial taxonomy of China's cyber militia forces based on a data set that examined 136 individual cyber militia units. This effort is intended to map the types of work units or *danwei* (单位) from which these militia units are drawn, examine the range of mission sets they are tasked with in practice, and provide a rough sense of their geographic and institutional dispersion.[*]

It bears noting that researching China's cyber militia system presents a distinct methodological challenge, particularly when compared to traditional analyses of the PLA order of battle. Unlike active-duty PLA units, militia detachments (especially in emerging domains like network operations and electronic warfare) are comparatively fluid. The composition and structure of these units are subject to change based on local mobilization needs and the administrative discretion of regional People's Armed Forces Department (PAFD, 人民武装部) offices. Units may be stood up or disbanded with little notice, and even enduring formations often draw personnel from civilian work units that change over time. This instability complicates efforts to assess the force in a consistent, longitudinal manner.

To mitigate this challenge, this study takes a "below the neck" approach to gauge the strength and composition of China's cyber militias examining units at the corps grade level and below.[†] [6] Rather than attempting to build a formalized cyber militia order of battle, it focuses on identifying discrete instances of cyber militia activity across a variety of jurisdictions and institutional contexts. In the aggregate, these data points make it possible to ascertain broader trends in cyber militia force composition and capability development and highlight key instances of operational experimentation across various localities. Nevertheless, the findings in this report should be understood as a snapshot based on available open-source materials and are necessarily subject to a degree of extrapolation and inference.

The History and Institutional Basis of China's Cyber Militia Forces

Since the founding of the PRC, militia forces (民兵) have played an integral role in the country's national defense architecture. China's militia forces are administered by the PAFD, and

[*] In this context, a danwei or "work unit" refers to an individual's place of employment or organizational affiliation. During the Mao era, danwei functioned as all-encompassing social and administrative entities, providing services such as healthcare and housing in addition to employment. In the present day, the term is used in official or bureaucratic contexts to identify an individual's work organization.

[†] "Below the neck" (脖子以下) is a term used by the PLA during its 2015 organizational reform to describe the second phase of restructuring, which focused on units below the corps grade level. The first phase addressed corps-grade and higher-level organizations ("above the neck," 脖子以上), while the second phase extended reforms downward to tactical and grassroots units.

form one leg of China's armed forces triad alongside the PLA and the People's Armed Police (PAP).[*] [7] The role and utility of the militia have evolved in tandem with China's shifting military doctrine. During the Mao era, militia forces were a foundational element of the "People's War" concept, which blurred the lines between civilian and soldier to deter invasion by presenting the prospect of a mass mobilized populace.[8] Despite China's shift toward a more professionalized defense force structure in the late 1970s and 1980s, the ethos of mass mobilization has nevertheless remained embedded in the PLA's institutional culture. Modern doctrinal texts, such as the 2020 edition of the *Science of Military Strategy*, continue to emphasize the integration of regular forces with militia and other irregular elements.[9] Furthermore, under Xi Jinping, the People's War principle has been reinterpreted through the lens of MCF. This formulation positions militia forces as a critical conduit through which national defense objectives are supported by civilian infrastructure and expertise.[10]Accordingly, militia forces serve dual functions: they contribute to the civilian economy in peacetime while providing a latent reservoir of technical and human capital that can be mobilized during national emergencies. In this context, the militia constitutes a flexible force that can be used to respond to urgent, complex, or politically sensitive contingencies.[11]

Although cyber militia units have existed in the PRC since the late 1990s, their institutional status remained poorly defined for much of their early development.[12] It was not until 2005 that the Central Military Commission (CMC) formally codified their role by issuing directives mandating that work units within colleges and universities establish dedicated information support teams.[†] [13] Around the same time, local PAFD offices began experimenting with training regimens tailored for network militia units, marking a nominal shift toward more structured integration into local defense mobilization systems. However, prior to 2013 this process of force construction unfolded slowly and unevenly. During the late 2000s, a number of local PAFD offices assembled a patchwork of subunits ostensibly intended to support emerging "informatized" (信息化) warfare requirements, but the organizational logic guiding their formation was frequently inconsistent.[14] These efforts were largely the product of broad and often vague directives from the Party center that encouraged grassroots incorporation of cyber capabilities into existing militia forces but lacked accompanying guidance on their organizational structure and mission set. As a result, early

[*] According to the Military Service Law of the People's Republic of China, the militia is defined as a "mass armed organization that is not separated from production" (不脱离生产的群众武装组织). That is, a reserve force composed of civilians who retain their regular employment while remaining integrated into the national defense mobilization system. By design, these units exist in a dispersed (散在) form during peacetime and are intended to be concentrated and operationalized (紧密) during wartime or large-scale emergencies. This organizational posture is encapsulated by a frequently cited axiom among PAFD officials that militias are to "serve in peacetime, respond to emergencies in times of crisis, and fight in wartime" (平时服务、急时应急、战时应战).

[†] It is worth noting that the Chinese source material on this point is somewhat ambiguous, as it references a directive issued by the CMC that has not been made publicly available. Consequently, it remains unclear whether all colleges and universities are required to maintain standing cyber militia units, or merely to possess the capacity to mobilize them when called upon. Subsequent Party-state literature published suggests the latter is more likely. Many educational institutions examined in this report did not establish network militia forces immediately following the issuance of the directive, instead doing so only in response to specific requests from their overseeing PAFD offices during the 2010s.

cyber militia development lacked doctrinal coherence and institutional standardization. This deficiency would later be addressed through reforms initiated during Xi Jinping's tenure in office.

Spotlight: China's National Defense Mobilization System

As with other categories of militia forces, China's cyber militia units are overseen by the National Defense Mobilization Commission (NDMC, 国防动员委员会), a joint body established in 1994 and co-led by the State Council and the CMC.[15] Within this structure, the NDMC's People's Armed Forces Mobilization Office (人民武装动员办公室), one of six NDMC offices, manages network and information warfare militia units alongside other reserve forces.* [16] The NDMC system maintains a vertically integrated structure that mirrors the Party-state's administrative hierarchy. Mobilization committees operate at the central (中央), provincial (省), municipal (市), and district (区) levels, each aligned with its corresponding Party Committee.[17] While both the PLA and local governments share command authority, local military organs ultimately exercise peacetime operational control. Their command structure is characterized by two primary linkages: "theater command–provincial military district–military sub-district or PAFD office" (战区—省军区—军分区/人武部), and "local Party committee and government–military organs at the same level" (地方党委政府—同级军事机关).† [18]

Across all its administrative tiers, the National Defense Mobilization Committee is responsible for three principal functions concerning militia oversight. First, they are responsible for identifying and maintaining visibility over local human capital and material resources that may potentially be organized into militia units.[19] This entails conducting regular inventories of technical expertise and infrastructure within their jurisdiction and assigning personnel to militia formations based on both local capabilities and central-level tasking requirements.[20] Second, local National Defense Mobilization Committees are charged by the CMC with ensuring the combat readiness of their respective militia forces. This task is executed through local militia training bases (民兵训练基地), operated by corresponding PAFD offices.[21] These facilities provide technical and tactical instruction to network militia units, provision electronic equipment to militia personnel from PAFD stockpiles, and facilitate joint training exercises with regular PLA units operating in the same geographic area.[22] Third, the mobilization system plays a critical role in transitioning militia units from peacetime reserve status to wartime operational support. In a national emergency or wartime contingency scenario, local PAFD offices are responsible for activating militia elements, deploying them, and integrating them into the broader PLA operational and command architecture.[23]

* NDM's other five offices are charged with managing economic mobilization, civil air defense, traffic and transport readiness, defense education, and overarching coordination efforts.

† This is a general rule that primarily applies to urban areas; however, a similar structure exists in rural regions, where equivalent responsibilities are carried out by county-level (县) organizations rather than municipal or district bodies.

Evolution of China's Cyber Militia System Under Xi Jinping

Under Xi Jinping, cultivation of cyber power has become a central pillar of the PRC's broader objective to build a military force capable of rivaling and eventually surpassing that of the United States.[24] The most visible manifestation of this ambition has been the structural reorganization and expansion of China's formal cyber forces, beginning with the establishment of the PLA Strategic Support Force (PLASSF) in 2016 and continuing with its subsequent subdivision into more specialized entities, including the Information Support Force (PLAISF) and the Cyberspace Force (PLACF).[25] Parallel to this institutional reform, the Party-state has also taken steps to more effectively leverage the civilian economy for cyber operations through mechanisms such as mandating that commercial firms share newly-discovered vulnerabilities and exploits with databases managed by China's military and security services.[26]

Less conspicuous, but no less significant, has been the steady expansion and professionalization of the cyber militia system. Under Xi's leadership, the number of cyber militia detachments has grown, while their operational integration with the PLA has deepened.[27] Party-state efforts have focused on enhancing the technical proficiency of militia personnel, formalizing training regimes, and improving the mechanisms through which these units are employed and mobilized. The effect of these undertakings has been to remediate longstanding inefficiencies in the cyber militia system and transform it into a more capable, scalable, and strategically relevant asset in China's broader cyber force architecture.

Throughout the 2010s and early 2020s, the PRC has significantly shifted its approach to building and deploying cyber militia forces. Although the PRC has not issued a single authoritative policy document detailing the reform of its cyber militia forces, its new strategic direction can be inferred from academic articles, conference proceedings, and military news outlets affiliated with the PAFD and the PLA. Among the most authoritative of these sources is a 2017 article by An Weiping (then-Deputy Chief of Staff of the PLA's Northern Theater Command) published in *National Defense Reference* (国防参考), a journal focused on strategic issues published by the PLA Press.[*28] This commentary offers a rare candid contemporary perspective on how the upper echelons of PLA leadership aimed to reform and enhance China's cyber militia capabilities. In his article, An identifies four central areas of focus for enhancing China's cyber militia capabilities. First, he calls for the coordination of military-civil fusion departments across all levels of government, the military, and the state bureaucracy.[29] This would involve the creation of dedicated command and coordination agencies capable of mobilizing cyber resources nationwide. Second, he highlights the importance of strengthening the legal and regulatory framework to guide military-civil integration in cyberspace, with the aim of standardizing how civilian cyber capabilities are

[*] In the PLA, a theater command (战区) is a top-level joint operational command responsible for conducting military operations within a designated geographic area. Each of China's five Theater Commands (Eastern, Southern, Western, Northern, and Central) integrates ground, naval, air, and rocket forces under a unified command structure.

leveraged in support of state objectives.[30] Third, he advocates continued investment in dual-use infrastructure (e.g. cyber ranges, public mobile networks, fiber-optic systems, and satellite platforms) jointly managed by military and civilian authorities.[31] Fourth, he underscores the need for tighter integration between civilian and military actors, both for peacetime tasks like training and emergency response, and for preparing cyber militia forces to contribute to wartime operations.[32] An's recommendations reflect an emerging doctrinal consensus on the future of China's cyber militia system that emphasized institutional coordination, legal standardization, talent integration, and the construction of strategically relevant technical infrastructure.* These principles foreshadow the trajectory that such reforms would follow in subsequent years.

The key inflection point in the institutional reform of China's cyber militia system occurred at the 2018 National Conference on Cybersecurity and Informatization (全国网络安全和信息化工作会议). The conference was attended by senior members of Party leadership including Xi Jinping and served as a seminal event for shaping the trajectory of China's cybersecurity architecture and advancing civil-military integration within the digital domain. Although the official proceedings and directives issued at the conference have not been publicly released, authoritative post-conference commentary from figures within the national defense mobilization and cyber militia apparatus suggests that the meeting played a decisive role in recalibrating the Party-state's approach to national cyber defense.

The core policy prescription emerging from the conference centered on the view that personnel from China's civilian sphere could play a critical role in supplementing the overstretched network operations forces of the PLA. However, such involvement was deemed acceptable only under the strict supervision of the Party-state. This emphasis reflected concerns among senior Party leadership that increasing reliance on private-sector actors risked eroding the boundary between state authority and non-governmental participation in national defense.[33] The conference proceedings emphasized the indispensability of private-sector capabilities (particularly in terms of infrastructure and technical expertise) while cautioning against the delegation of core defense responsibilities to non-state actors.[34] Implicit in these discussions was a warning against the overreliance on private sector capabilities for national cyber defense absent direct military supervision (e.g. the substitution of military personnel with civilian contractors or volunteers in roles deemed sensitive to national security). However, rather than advocating for a strict bifurcation between military and civilian roles, the conference endorsed a model emphasizing

* Interestingly, An Weiping's article also potentially reflects behind-the-scenes policy deliberations that may not be fully reflected in official state directives. In particular, An contends that the Ministry of State Security (国家安全部门, MSS) should assume a leading (主导) role in the planning and oversight of national cyber reserve forces. He further advocates for the MSS to guide "top-level legal and policy frameworks that would facilitate the development of cyber defense reserve capabilities, resolve questions of interagency division of labor, coordinate promotional strategies, and align competing institutional interests." However, no other sources surveyed in this study explicitly reference the MSS in this context, suggesting that its role remains deliberately obscured or confined to an advisory capacity within broader Party-state decision-making structures.

stronger Party-state oversight of civilian cyber capability providers and their deeper integration into the national defense mobilization system.[35] Under this framework, private-sector support to the PLA in cyberspace would continue, but only under a framework that was "militarized, systematized, and systemic" (军事化、体系化、系统化). This formulation was designed to ensure that non-military actors engaged in cyber defense remained under clear national command authority and aligned with Party-state strategic intent.[36] The conference proceedings further underscored the need for cyber militia units to become more operationally relevant and standardized in their capabilities. Accordingly, it advocated increased resourcing for militia elements drawn from civilian work units, alongside expanded joint training with their uniformed PLA counterparts.[37]

The principles articulated at the 2018 National Conference on Cybersecurity and Informatization have since served as a roadmap for the Party-state's ongoing reform of China's National Defense Mobilization System. China's military and civilian cyber governance authorities have enacted these reforms across four key dimensions: legal and regulatory foundations, organizational structure, human capital development, and the construction of equipment and infrastructure. The following sections will examine how China's militia reform effort has unfolded across each of these dimensions.

Legal and Regulatory Reforms

The ongoing development of cyber militia forces in the PRC has not emerged from a single landmark piece of legislation. Instead, it reflects a pattern of normative institutionalization driven by policy imperatives, administrative restructuring, and incentive realignment within China's broader MCF framework. The Party-state has allowed this process to evolve organically through local experimentation, with provincial and municipal defense mobilization authorities formulating their own policy prescriptions to comply with central guidance mandating closer military-civil cooperation in the field of cyber capability development. This process has manifested in a variety of ways, such as cultivating partnerships between national defense mobilization authorities and centers of cyber expertise in academia and industry, increasing government capacity to mobilize resources for localized cybersecurity defense, and incentivizing both public and private actors to participate in state-led initiatives. In this context, China's legal structure has functioned less as a tool of prescriptive regulation and more as a permissive architecture legitimating the PLA's and local governments' improvisation.

A small number of national laws provide the legal scaffolding for this growth in network militia capacity. Most prominent among them is the 2017 Cybersecurity Law, which mandates that network operators cooperate with public security and intelligence organs and promotes talent

development and the construction of a national cybersecurity defense system.[38] * While the law does not reference militia forces directly, its provisions create a legal basis for mobilizing civilian technical expertise in support of state-led cybersecurity operations. For instance, Hou Jiabin, an analyst at the PLA Nanjing Political College (解放军南京政治学院), asserted that the Law would facilitate deeper military-civil integration by enabling the Party-state to draw on university and enterprise resources for national defense applications in domains such as network and information warfare.[39]

However, the realization of cyber militia development has taken place primarily through Party and administrative mechanisms. The reorganization and standardization of militia forces has been implemented through the Central Military Commission's National Defense Mobilization Department and codified in internal frameworks such as the "Compilation of Rules in the Standardized Management of Militia Construction" (民兵队伍建设规范化治理成果汇编) and the "Implementation Measures for the Rectification of Militia Organizations of the Central Military Commission's National Defense Mobilization Department" (中央军委国防动员部民兵组织整顿工作实施办法).† [40] Although the full text of these documents has not been made publicly available, subsequent releases from relevant government bodies indicate that they have guided ongoing militia rectification efforts. In particular, these secondary documents allude to central guidance mandating the reorganization of personnel and equipment reserves, improvement in data collection on local mobilization capacity, and enhancement of readiness to meet the PLA's evolving operational demands.[41] They furthermore stipulate that the aforementioned reforms are primarily carried out by county- and district-level PAFD offices, which coordinate with local Party committees, PLA units, and civilian enterprises to identify potential recruits, assign unit roles, and conduct training.[42]

MCF serves as the primary institutional framework for driving these developments. As part of this broader strategy, the Party-state explicitly encourages provincial governments and military organs to support the formation of cyber militia units within large-scale cybersecurity and internet firms.[43] These cybersecurity and internet companies, in turn, are expected to contribute personnel, training facilities, and threat intelligence capacity in exchange for political favor or access to government contracts.[44] Such arrangements are rarely framed in legal terms. Rather, they reflect the Party's broader strategy of embedding national defense obligations as normative expectations across the civilian economy.[45] Hence, while the legal foundation for marshaling cyber militia forces remains diffuse and deliberately flexible, it is nonetheless coherent in its intent: to establish a legal and political environment in which the mobilization of civilian cyber capabilities for Party-state purposes is both normalized and expected. The resulting regulatory structure fuses permissive

* Other relevant laws include the 2016 National Security Law of the People's Republic of China (中华人民共和国国家安全法) and the 2020 National Defense Law of the People's Republic of China (中华人民共和国国防法)

† These efforts are further embedded in national planning instruments such as provisions in local 14th Five-Year Planning documents that outline roadmaps for militia reform.

legal structures with local Party Committee-led planning and oversight, collectively designed to expand China's cyber defense capacity without ceding control over its political or operational direction.[46]

Organizational Reforms

Alongside legal and regulatory reforms, the PRC has also undertaken efforts to restructure the organizational system responsible for mobilizing cyber militia forces. This development has unfolded as part of a broader effort to transform latent "national defense potential" (国防潜力) into actualized "national defense strength" (国防实力).[47] This transformation reflects a guiding conceptual framework in the PLA's approach to militia reform that the technical, intellectual, and organizational resources distributed across Chinese society (particularly in the technology industry) represent an untapped strategic reserve.[48] According to this line of thinking, the Party-state's chief organizational challenge has not been the absence of talent or equipment, but the inability of the militia system to effectively identify, train, and integrate these assets into the operational architecture of the PLA.

Under Xi Jinping, this problem has received sustained attention from the Party-state. One of the early organizational efforts entailed enumerating the human and technical cyber potential embedded in Chinese universities. By 2010, most major academic institutions in China had registered their "cyber militia potential," including inventories of qualified personnel and relevant hardware.[49] These assets were formally catalogued with the intent of legally mobilizing them under emergency or wartime conditions. However, converting this potential into usable combat power required systematic reforms to data architecture, personnel management, and coordination mechanisms between the PLA and local civilian authorities.

The Party-state's development of national- and provincial-level "cyber defense talent databases" (网络防御专用人才数据库) has been central to this process.[50] These data repositories support targeted recruitment, pre-screening of potential militia personnel, and the modularization of training programs, allowing for scalable onboarding tailored to specific operational requirements.[51] Such databases also facilitate "theater joint combat data" (联合作战数据) sharing between local PAFD offices and the PLA's Theater Commands enabling more dynamic decision-making and improved alignment between militia resources and operational needs.[52] Moreover, Theater commanders now conduct annual spot inspections and mobilization audits to verify the location, quantity, and usability of key cyber and technical resources.[53]

These reforms culminated in the establishment of a new Joint Command Organization and Operation System (联合指挥机构编组运行体系) by 2024.[54] While the details of this system appear to be classified, open-source material suggests it enables integrated command-and-control functions between PLA and militia units, particularly at the Theater Command and sub-Theater

Command levels. The COVID-19 pandemic served as a proving ground for this schema, forcing local Party committees to coordinate operational planning with their military counterparts in a wartime-adjacent environment.[55] Local PAFD offices used this period to pilot data-driven "smart mobilization" (智慧动员) tools, refine interagency collaboration with the Ministry of Public Security (MPS), PAP, and garrison units, and identify cyber mobilization shortfalls under real-world stress conditions.[56]

Reforms to the national defense mobilization system have also sought to clarify lines of authority and integrate militia planning more closely with PLA operational requirements. During peacetime, cyber militia personnel are now incorporated into regularized emergency response detachments that are used to assist in missions such as natural disaster relief.[57] This dual-use structure is managed through local National Defense Mobilization Committees (国家国防动员委员会) that harmonize joint training and deployment planning among stakeholders such as the PLA, local governments, and enterprise-level institutions.[58] Conversely, in wartime, command authority over cyber militia forces is vested solely in the PLA, with Theater Commanders typically exercising direct command over all cyber militia units within their respective areas of responsibility.[59]

The cumulative effect of these reforms has been to standardize cyber militia construction and bring local practices into closer alignment with top-down PLA doctrine.[60] At present, a growing number of county- and district-level units now adhere to uniform standards for force generation, equipment provisioning, and training benchmarks. This trend is largely driven by rectification efforts designed to enforce previously neglected regulations on militia readiness and training, which heretofore contributed to a lack of unit cohesion and operational effectiveness. As one military sub-district commander observed:[61]

> "There was [previously] organization but lack of cohesion, strength but lack of combat effectiveness, demand but lack of execution, and system but lack of coercive force. Under the new model, units report greater clarity in mission design, improved training focus, and more robust integration with operational plans"

Accordingly, the organizational maturation of China's cyber militia forces has significantly enhanced the PLA's ability to mobilize society-wide cyber capabilities in support of national defense.

Human Capital Reforms

Another major focus of the Party-state over the past ten years has been enhancing the overall quality of cyber militia forces by improving the technical capabilities and political reliability of their members. Although the PRC had established a capacity for mustering network militia forces from its civilian infrastructure by the early 2010s, the units that were raised during

this period often lacked warfighting potential.[62] In particular, these forces were frequently hampered by challenges in personnel quality, political reliability, structural turnover, and lack of integrated training and command systems.

These shortcomings are reflected in authoritative contemporary writings from the period. A particularly illustrative source is a 2010 master's thesis authored by Gu Gang, who at the time served as the Department Head of an unnamed urban PAFD unit (城区武装部长) responsible for overseeing the mobilization of both militia and reserve forces. Gu observes that network militia forces were frequently recruited from university student populations, which presented a ready-made pool of talent that possessed the requisite technical skills necessary to serve effectively as network operators.[63] However, this recruitment strategy presented several limitations. Specifically, the inherently transient nature of student life, combined with competing demands such as academic obligations and family responsibilities, hindered the accumulation of institutional experience and cohesion within cyber militia units.[64] Gu also raised concerns about morale and "national defense consciousness" among student soldiers, asserting that:[65]

> "From the perspective of ideological awareness, the long-term peaceful environment has weakened the national defense awareness and sense of crisis of the whole society… in the current critical period of national economic and social development transformation, in the special period when college graduates are under great employment pressure, the enthusiasm of college militia to participate in national defense activities and the awareness of college militia to participate in war cannot meet the needs of actual combat."[66]

In addition to personnel-related shortcomings, early cyber militia detachments were hindered by significant structural and organizational deficiencies. While seldom acknowledged explicitly in official sources, it appears that many of these units were initially established to fulfill top-down political mandates from Party leadership, rather than being designed with a clearly defined operational role or mission set. As such, they often functioned as unfunded mandates, lacking the institutional support necessary to ensure meaningful capability development. As of 2010 there was little evidence to suggest that cyber militia units were conducting substantive, field-based training in coordination with PLA forces or conventional militia counterparts.[67] Just as striking was the absence of a centralized mechanism for coordinating cyber militia activities across relevant institutions.[68] No effective command structure existed under the National Defense Mobilization Commission to align training protocols, mobilization procedures, or resource distribution between local PAFD and affiliated academic institutions.[69] This lack of a unified framework for command, coordination, and control significantly hampered efforts to integrate cyber militia development into the PLA's broader strategic planning and operational systems.

In response to persistent capability gaps and structural inefficiencies, the Party-state has undertaken a series of targeted reforms over the past decade aimed at reshaping the composition,

training, and functional role of cyber militia units. These efforts have unfolded along three primary lines of effort.

First, the Party-state has sought to diversify and professionalize cyber militia recruitment, particularly within academic institutions.[70] Specifically, it has sought to reduce reliance on university students, whose high turnover (due to graduation and subsequent employment elsewhere) was seen as problematic.[71] Instead, PAFD recruitment strategies have increasingly prioritized early-career professionals and junior academic staff, thereby fostering greater institutional memory and enhancing unit cohesion.[72]

The second line of effort has focused on expanding the sources from which cyber militia personnel are drawn. While universities and SOEs remain important recruitment pools, there has been a deliberate shift toward engaging the broader civilian tech sector, including medium and large private enterprises, as well as independent technical specialists.[73] This approach reflects a recognition that effective cyber mobilization must incorporate non-traditional talent pools. Yuan Yi, a scholar affiliated with the Academy of Military Sciences, encapsulated this sentiment in a 2015 article where he called for accelerating the development of non-professional cyber warfare forces composed of cyber militia units, law enforcement police, patriotic hackers, and network technicians. He specifically emphasizes the recruitment of "geniuses, peculiar talents, and eccentric talents" (奇才、偏才、怪才) deemed essential for "specialized domains and operational requirements" (特殊领域和作战急需).[74] This imperative was further underscored by the CMC's 2016 "Opinions on Deepening the Reform of National Defense and the Army" (中央军委关于深化国防和军队改革的意见), which calls for a reduction in legacy militia structures and a reallocation of resources toward cultivating high-value personnel for emerging mission areas.[75] These measures include expanding militia construction in frontier domains, improving the reserve system for information warfare, and better aligning force generation with market-driven skill development and operational imperatives.[76]

The third line of effort centers on strengthening technical training and political-ideological education. This reform effort was intended to address persistent bottlenecks in combat readiness and governance challenges at the intersection of military and civilian authority.[77] Recognizing these points of friction, provincial Party Committees (working in coordination with their respective PAFD offices) have conducted regular grassroots-level assessments to better understand operational weaknesses over the past 10 years. These reviews revealed systemic issues, including fragmented political and ideological work discipline, poorly structured training programs, inconsistent enforcement of discipline, and low morale among many cyber militia units.[*78] In response, the PAFD introduced corrective measures to enhance the quality and efficacy of cyber

[*] The Party uses the term "political and ideological work" (政治思想工作) to refer to a structured system of instruction aimed at instilling loyalty to the CCP. This education is overseen by the PLA's political work system and delivered through regular classes, lectures, and study sessions. It plays a central role in maintaining Party control over the armed forces and ensuring the ideological conformity, discipline, and morale of personnel.

militia units. For instance, in many localities, training programs have been expanded to include more realistic wartime scenarios, with cyber militia personnel increasingly participating in live-fire exercises and joint field deployments.[79] Even those personnel assigned to rear-echelon or technical duties are now expected to undergo operational field training in order to promote stronger unit cohesion.[80] Simultaneously, more stringent political education has been institutionalized through more frequent lectures, study sessions, and standardized ideological curricula aimed at reinforcing Party loyalty and cultivating an understanding of the militia's strategic responsibilities.[81]

Equipment and Infrastructure Acquisition Reforms

The evolution of the PRC's cyber militia system has also entailed a concerted effort to enhance operational readiness through improved training infrastructure and the provisioning of modern equipment. Historically, militia units have operated at a significant disadvantage relative to their active-duty counterparts, particularly in terms of access to mission-essential resources such as dedicated training facilities, cyber ranges, and advanced hardware.[82] These limitations were primarily the result of chronic budgetary constraints, which inhibited the ability of local PAFD offices to independently acquire, requisition, or maintain necessary technical infrastructure. The absence of foundational capabilities not only constrained training opportunities but also curtailed the operational utility of cyber militia formations during periods of heightened national demand.

However, in recent years the Party-state has pursued a range of public-private initiatives designed to close these capability gaps. In particular, partnerships among civilian enterprises, academic institutions, and PLA entities have resulted in the co-development of cyber training ranges.[83] These jointly operated and maintained facilities serve both educational and national defense functions. Specifically, they allow for the safe development, testing, and validation of cyber warfare tactics, while also providing a controlled venue for executing structured network attack drills.[84] The core functions of these training ranges typically include:[85]

- Threat analysis and vulnerability assessment across cyberspace domains.
- Early warning and incident detection for cybersecurity events.
- Response and mitigation protocols to ensure rapid containment and system recovery.
- Continuity of operations and protection of critical information infrastructure.

In parallel with infrastructure upgrades, the PLA and associated defense mobilization bodies have increased the provision of modern equipment to cyber militia units. Select militia formations have been equipped with advanced command-and-control vehicles, virtual reality-enabled training platforms, and BeiDou satellite-enabled handheld terminals.[86] These material improvements have markedly increased the functional capacity of network and information warfare militia units, allowing them to operate with enhanced mobility, situational awareness, and communications.

Assessing the Structure, Role and Functions of China's Cyber Militia System

The goals guiding reforms to the PRC's cyber militia system are both far-reaching and ambitious. Yet despite a decade of institutional investment, the broader militia system overseen by the PAFD remains in the midst of a protracted process of capacity building and operational refinement. This raises the question: how do China's cyber militia units currently operate, and to what extent have recent reforms translated into tangible improvements in effectiveness? More pointedly, where do cyber militia forces fit within the PLA's evolving order of battle, and how significant are they to China's broader military and national security apparatus? To address these questions, the following section provides a representative snapshot of cyber militia operations as they exist in practice. It focuses on identifying the organizational structure and functional roles of these units, the types of personnel that staff them, and the mission sets they are tasked with supporting. In doing so, it seeks to assess both the operational relevance of these forces and their integration within the PLA's wider warfighting and mobilization ecosystem.

The Role of Cyber Militia Forces Within Modern PLA Doctrine

The revitalized role of militia forces has become increasingly evident in the context of the PRC's evolving approach to cyberspace strategy. PLA sources generally acknowledge that safeguarding China's domestic information space presents a formidable challenge, owing to the vast size and complexity of the national network attack surface. Managing this digital terrain (particularly under conditions of heightened threat or wartime mobilization) demands a scale of manpower and technical capacity that China's uniformed forces cannot fulfill on their own. This operational gap is explicitly acknowledged in PLA doctrinal writings. For instance, a 2017 PLA operational guidance text on cyber operations notes that:[87]

> "In information warfare, the network penetrates all areas of warfare. Cyberspace attack and defense confrontation has the characteristics of full process, full field, and full elements. Therefore, cyberspace warfare is not only the task of professional cyberspace combat forces, but also the task of other combat forces—especially network defense, which requires full participation and comprehensive defense."

The theoretical foundation for this division of roles is also present in key doctrinal texts. For instance, the 2020 edition of the *Science of Military Strategy* emphasizes the growing importance of reserve and militia forces in providing "service support for multidomain integrated joint operations" (多领域一体化联合作战).[88] Building on this conceptual foundation, Party theorists and military planners also emphasize the importance of expanding the aperture through which cyber militia units are drawn. Accordingly, China's cyber forces are constituted of professional military information warfare forces (军队专业的信息作战力量), as well as civilian

information technology professionals (社会上的专业信息技术力量), broader segments of the non-technical public (非技术力量和广大人民群众), and even sympathetic foreign actors aligned with Chinese interests abroad (域外进步力量).[89] In this schema, the PLA, Ministry of State Security (MSS), and MPS constitute the core of China's offensive and reconnaissance capabilities, functioning as the spearhead in cyberspace operations that is supported by state-approved technical teams, private-sector actors, and vetted researchers.[90] These supporting forces function as a force multiplier providing strategic depth for China's core cyber operators and serving as a latent resource pool that can be mobilized in times of heightened need.

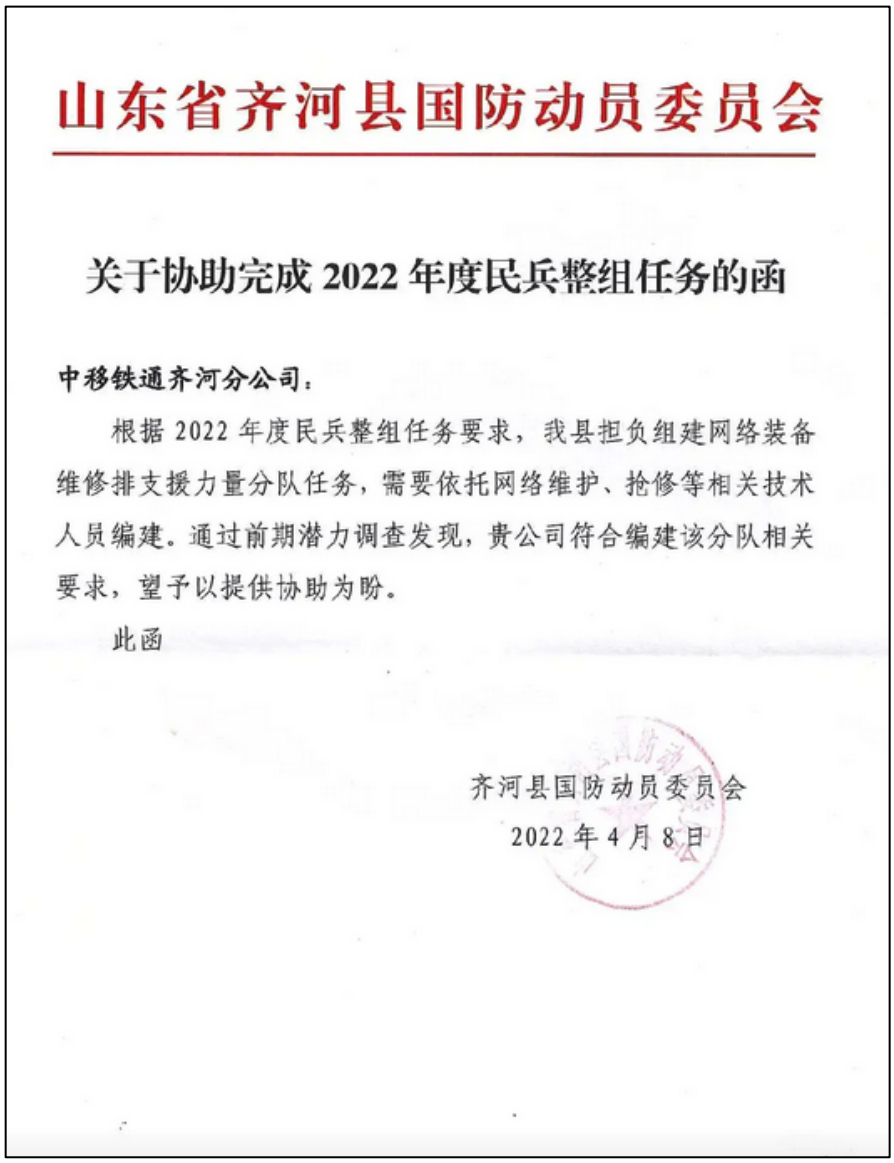
Force Generation Processes

The organization and staffing of cyber militia units in China are managed primarily at the local level, where Party Committees and PAFD offices work in tandem to fulfill unit formation requirements issued from higher authorities. Force generation follows a tiered structure aligned with the Party-state's administrative hierarchy. At the top, provincial and municipal National Defense Mobilization Committees coordinate resource identification and determine overall force structure needs.[91] Municipal governments are typically responsible for tasking specific work units with specific roles within the National Defense Mobilization System, while county and district-level PAFDs oversee implementation by assigning personnel, tracking readiness, and conducting annual updates to ensure centralized unit management and cross-regional deployment.[92]

In practical terms, this process often begins with the issuance of force generation quotas by provincial or county-level mobilization authorities.[93] These authorities draw on existing mobilization databases and conduct outreach to relevant institutions (e.g. universities, SOEs, and commercial entities) within their jurisdiction to assess available human capital and technical resources.[94] Based on this assessment, selected work units are directed to form or maintain the capacity to rapidly stand up cyber militia units. In some cases, this means establishing formal detachments. In others, it entails maintaining the latent capacity to mobilize on short notice, in keeping with the PLA's broader objective of ensuring that reserve militia forces can be "mobilized, employed, and prevail" (拉得出, 用得上, 打得赢) in moments of crisis.[95]

The precise mechanisms used by the Party-state to secure institutional compliance remain unclear. However, it is telling that the militia system has historically relied on the administrative leverage the Party-state holds over SOEs, public universities, and other government-linked entities. These organizations, which are often recipients of state funding and regulatory oversight, are well-positioned to receive taskings from local mobilization authorities and have few formal grounds to resist. To date, there is limited evidence that the Party-state has attempted to compel wholly private firms to raise cyber militia units in peacetime, though there are indications that authorities still

seek to maintain an inventory of the human and technical resources available to them across both public and private sectors.[*96]



山东省齐河县国防动员委员会

关于协助完成 2022 年度民兵整组任务的函

中移铁通齐河分公司：

根据 2022 年度民兵整组任务要求，我县担负组建网络装备维修排支援力量分队任务，需要依托网络维护、抢修等相关技术人员编建。通过前期潜力调查发现，贵公司符合编建该分队相关要求，望予以提供协助为盼。

此函

齐河县国防动员委员会

2022 年 4 月 8 日

Figure 1: Mobilization order for the China Mobile Qihe Branch (中移铁通齐河分公司) from the Shandong Qihe Province requesting them to form a "network equipment maintenance platoon."[† 97]

[*] Chinese sources are generally vague about the specific form these inventories take. However, it is reasonable to infer that at a minimum they include rosters of personnel with relevant technical skill sets, political backgrounds, and other pertinent attributes such as prior military experience.

[†] A translation of the main body of the letter reads as "According to the requirements of the 2022 militia group task, our county is responsible for the task of forming a network equipment maintenance platoon support force detachment, which needs to be established by relevant technical personnel such as network maintenance and emergency repair. Through the preliminary potential investigation, it was found that your company meets the relevant requirements for the establishment of this detachment, and we hope to provide assistance."

Figure 2: Newly-recruited members of the China Mobile Qihe Branch (中移铁通齐河分公司) militia reporting for in-processing. [98]

While the predominant mechanism for establishing cyber militia units continues to rely on mobilizing state-affiliated entities, the Party-state has gradually begun exploring incentive-based models aimed at broadening private sector participation.[99] This shift reflects a growing recognition that cutting-edge cybersecurity capabilities and innovation are increasingly concentrated in privately held firms. Consequently, greater integration of these entities into the national defense framework is viewed as both strategically necessary and operationally advantageous. A notable example of this emerging approach can be found in a policy proposal authored by the commander of the Huaihua Military Sub-district in Hunan Province which advocated for the creation of a preferential enlistment system for enterprises willing to organize militia detachments.[100] Under this model, participating companies would be eligible for coordinated tax relief, including reduced or exempted fees, and could incorporate militia-related expenditures into tax deduction categories.[101] Additional incentives would include preferential access to state-backed loans, favorable consideration in government procurement and project bidding, and public recognition through the designation of "brand projects" (品牌工程) linked to national defense contributions.[102] Similar proposals have called for the use of government-financed development projects, subsidized loans, and expanded social investment channels to support military-civil fusion in the cyber domain.[103]

These views have also been echoed among high-profile private-sector actors. For instance, Xiao Xinguang who founded the cybersecurity firm Antiy Labs and is a delegate to both the National People's Congress (NPC) and the Chinese People's Political Consultative Conference (CPPCC), has advocated for institutional support mechanisms to strengthen cyber militia capacity.[104] In a 2020 policy proposal, he called for establishing dedicated funding lines,

streamlined administrative processes, and practical training systems to ensure a high level of operational readiness among militia personnel and units.[105] He also proposed that provinces with a strong cybersecurity industry base should be provided with special financial allocations, which would be used to build mirror nodes or sub-engineering platforms.[106] These assets would support localized cyber militias capable of conducting joint training with their respective Theater Commands, thereby forming more regionally responsive reserve forces.[107]

Although the degree to which these recommendations have been fully implemented remains unclear, the growing trend of flagship cybersecurity firms provisioning militia units to the PAFD order of battle suggests an increasing appetite within the private sector for deeper engagement with China's armed forces. It is plausible that many commercial entities view alignment with Party-state strategic objectives as a pathway to securing preferential access to state resources and competitive advantage, rather than a political obligation or burden. As such, participation may be driven not only by patriotic obligation, but also by a pragmatic calculus. Namely, that alignment with Party-state strategic priorities offers privileged access to state resources, regulatory favor, and expanded commercial opportunities.[*] [108]

In addition to collective mobilization through work units, there are also sporadic cases of direct individual recruitment into cyber militia programs.[109] These recruitment efforts target university students identified through national defense education initiatives or high-profile cybersecurity competitions.[110] Participants are typically drawn in with promises of advanced technical training (deemed valuable for future employment prospects) as well as modest material incentives such as daily stipends.

[*] Additionally, the Party-state is often the primary (and in some cases the sole) source of revenue for many of these private entities. Given that government spending is finite, supporting cyber militia units may position these companies more favorably to receive a share of limited contract opportunities.

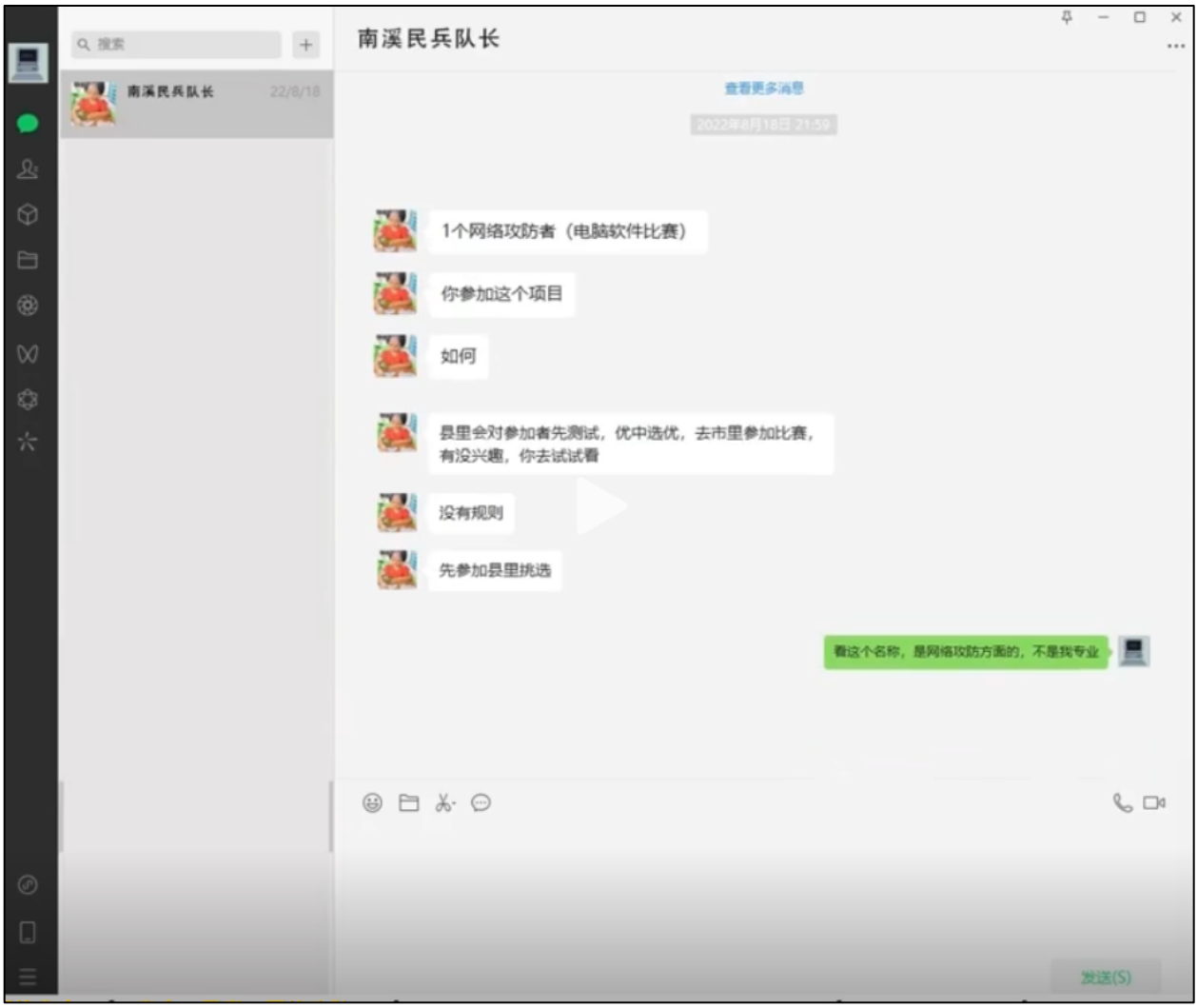


Figure 3: Excerpt from a WeChat conversation posted to Douyin depicting a recruiter reaching out to a student about participating in a cybersecurity competition to gain entry to a militia unit.[*] [111]

Other cases point to the use of public outreach and targeted advertising to attract individuals with specialized technical skillsets into cyber militia ranks. For example, a cyber militia unit in Gansu Province disseminated a "Basic Militia Recruitment Order" through multiple channels (such as television broadcasts, internet platforms, and public WeChat accounts) to recruit professionals in fields such as surveying and mapping, network engineering, communications, electrical systems, and heavy machinery operation.[112] In other instances, recruitment efforts have been embedded within broader national defense education initiatives, with cyber militia formation occurring alongside the establishment of affiliated groups such as military enthusiast clubs and

[*] A translation of the conversation is as follows:
Captain of Nanxi Militia: "1 Cyber Attacker (Computer Software Competition); You can join this project; The county will test the participants first, select the best ones, and send them to the city to participate in the competition. If you are interested, you can try it out; no rules; first you must participate in the county selection process."
Respondent: Judging by the name, it's about network attack and defense, which isn't really my area of expertise.

veterans' associations.[113] These developments underscore a growing diversification of recruitment strategies aimed at cultivating a technically capable cyber reserve force.

Recruitment and Work Unit Composition

One of the more notable developments in the evolution of China's cyber militia system over the past decade is the Party-state's effort to diversify the range of institutions contributing to cyber militia force generation. As mentioned earlier in this section, the majority of network militia forces are traditionally drawn from universities and SOEs in the telecommunications and electronics sectors.[114] In recent years, however, the scope of participation has expanded to include a broader cross-section of private industry, reflecting the military's growing interest in tapping into commercially developed technical capabilities.[115]

Broadly speaking, the division of labor among contributing institutions remains functionally aligned with their civilian specialization. Communications support units are typically sourced from major telecommunications SOEs, such as China Telecom (中国电信) and China Unicom (中国联通), while the bulk of network operations detachments continue to be drawn from faculty and students within academic institutions.[116] This organizational structure is consistent with longstanding practices, whereby units are task-organized into mission-specific elements focused on network monitoring, reconnaissance, offensive cyber operations, and network defense.*[117]

A more recent and noteworthy trend is the increasing involvement of private-sector cybersecurity firms in cyber militia construction. While early efforts primarily involved SOEs and public institutions, there is growing evidence that select private companies have begun to contribute forces or capabilities that are integrated into the PLA's broader operational architecture.[118] As of 2018, at least 30 domestic network companies had entered into cooperative relationships with the PLA. While many of these arrangements likely involved resource sharing or technical support rather than the formal standing up of militia units, their emergence nonetheless signals a gradual shift toward deeper military-private sector integration in the cyber domain.[119] The full extent of these partnerships remains unclear, but the trajectory suggests a slow expansion of the cyber militia's institutional base beyond its traditional public-sector confines.

* For instance, a 2006 report authored by personnel from the Jiangsu Provincial Military Region's Mobilization Department (江苏省军区动员处) outlines the formation of militia computer network warfare units across key sectors, including postal and telecommunications systems, the electronics industry, network enterprises, and scientific research institutes.

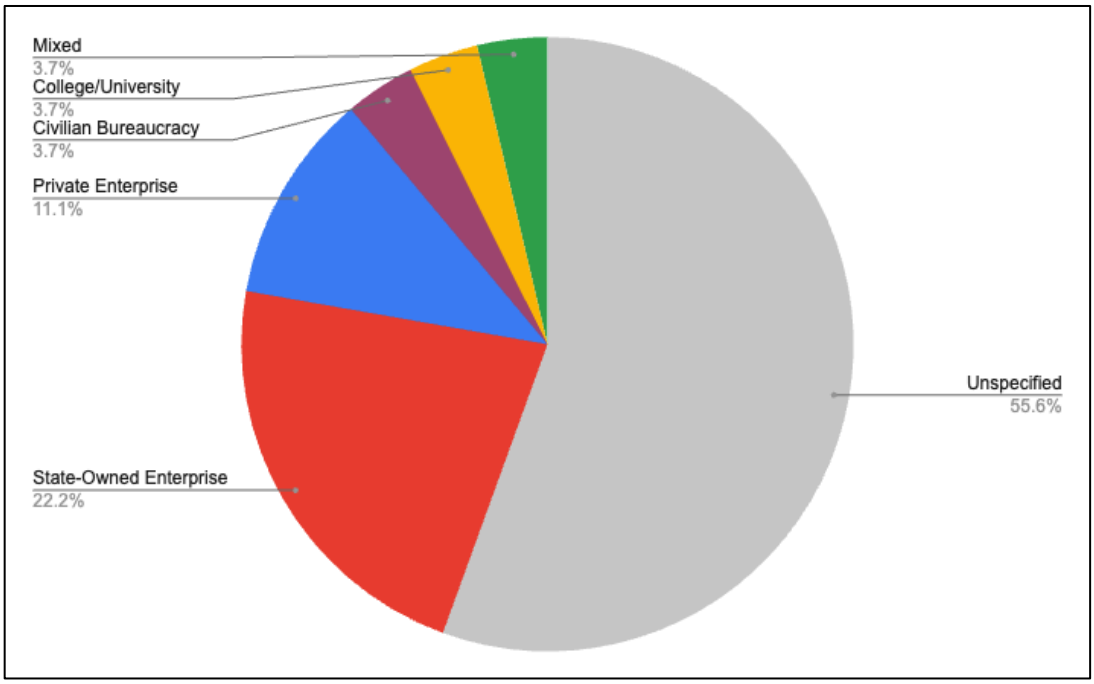


Figure 4: Composition of Militia Communications Operations and Maintenance Units[120]

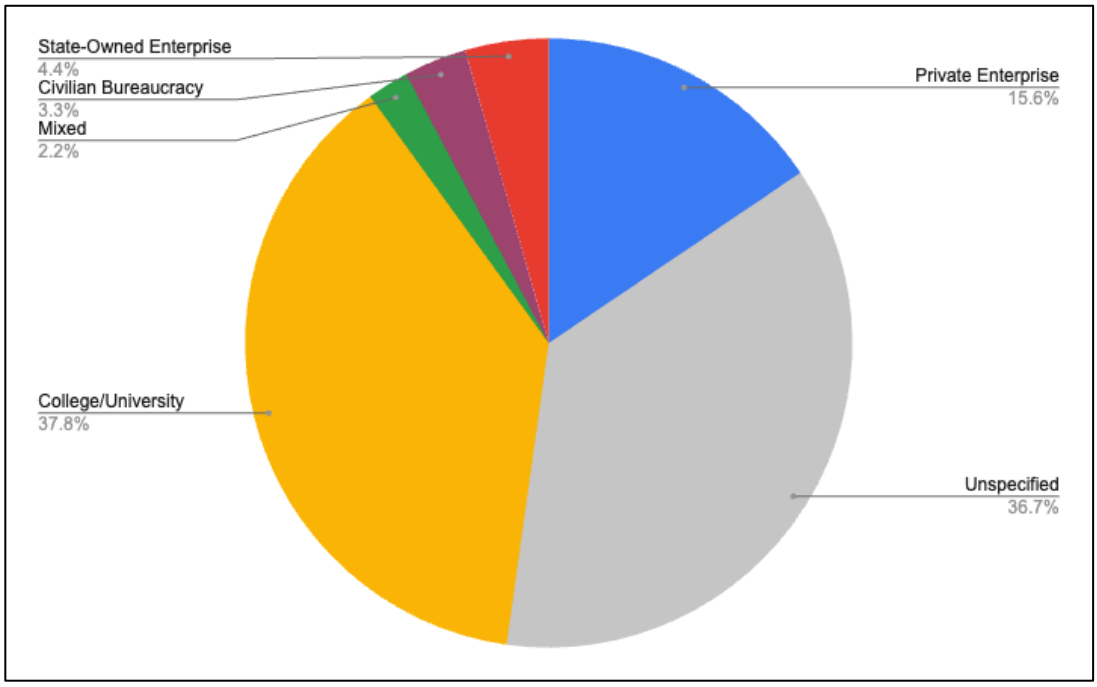


Figure 5: Composition of Militia Network Warfare and Cybersecurity Units[121]

When conducting recruitment, some PAFD offices eschew the practice of drawing militia units entirely from one work unit, and will instead draw personnel from multiple companies.[122] This approach is intended to lessen the administrative burden on any one company by preventing

the wholesale removal of their highly specialized technical staff for extended periods of time.*[123] The establishment of such units in spite of the logistical challenges of assembling individuals from disparate work units points to sustained top-down direction from higher-level military authorities to build out cyber-capable militia forces.

Category (区分)		**Organizing Unit (组建单位)**	**Detachments (分队数)**	**Number of Personnel (人数)**		
Specialized Forces (特殊力量)	Cyber Detachment (网络分队)	Beiguan Subdistrict Office (10 personnel each from Tietong and China Telecom) (北关街道办事处 [铁通、电信各 10 人])	1	50	80	80
		Dongguan Subdistrict Office (10 personnel from the South Campus of Shaanxi University of Technology) (东关街道办事处 [陕西理工大学南校区 10 人])				
		Zhongshan Street Subdistrict Office (10 personnel from the Cybersecurity Division, Hantai Branch, Hanzhong Public Security Bureau) (中山街街道办事处 [公安汉台分局网监支队 10 人])				
		Hedongdian Town (10 personnel from the North Campus of Shaanxi University of Technology) (河东店镇[陕西理工大学北校区 10 人])				
		Zongying Town (10 personnel from Hanzhong Vocational and Technical College) (宗营镇[汉中职业技术学院 10 人])				
	Information Personnel (信息员)	Two personnel from each subdistrict office and town (办事处、镇各两名)		30		

Figure 6: Example of a mixed-work unit cyber militia formation[124]

Notably, despite the relatively important role that network warfare militia units occupy within the broader mission structure of the PRC, they typically represent only a small fraction of

* Alternatively, some companies have proactively tailored their training and scheduling practices to support PAFD operations. Rather than adhering to a rigid schedule, these companies coordinated with militia organizers to select training dates and formats that minimized business disruption.

a given militia's total personnel. For instance, in Hantai District of Hanzhong, Shaanxi Province, only 29 out of 1,033 militia members were assigned to network attack and defense roles.[125] This trend underscores the continued scarcity of personnel with the requisite technical skillsets, especially in economically underdeveloped or rural areas.

The uneven distribution of China's cyber militia forces is further evinced by their geographic concentration in economically advanced regions. The highest density of identified units is found in coastal provinces such as Jiangsu, Zhejiang, and Guangdong, as well as centrally administered municipalities like Shanghai— all areas characterized by mature high-technology sectors and strong industrial bases. One notable exception to this trend is Hunan Province, which serves as a key node in China's national defense science and technology infrastructure despite lacking a robust commercial tech base.* Conversely, cyber militia presence is comparatively sparse in strategically sensitive but less economically developed areas such as Xinjiang and Tibet, suggesting that force distribution remains contingent on the availability of skilled labor and relevant institutions rather than purely on operational defense imperatives.

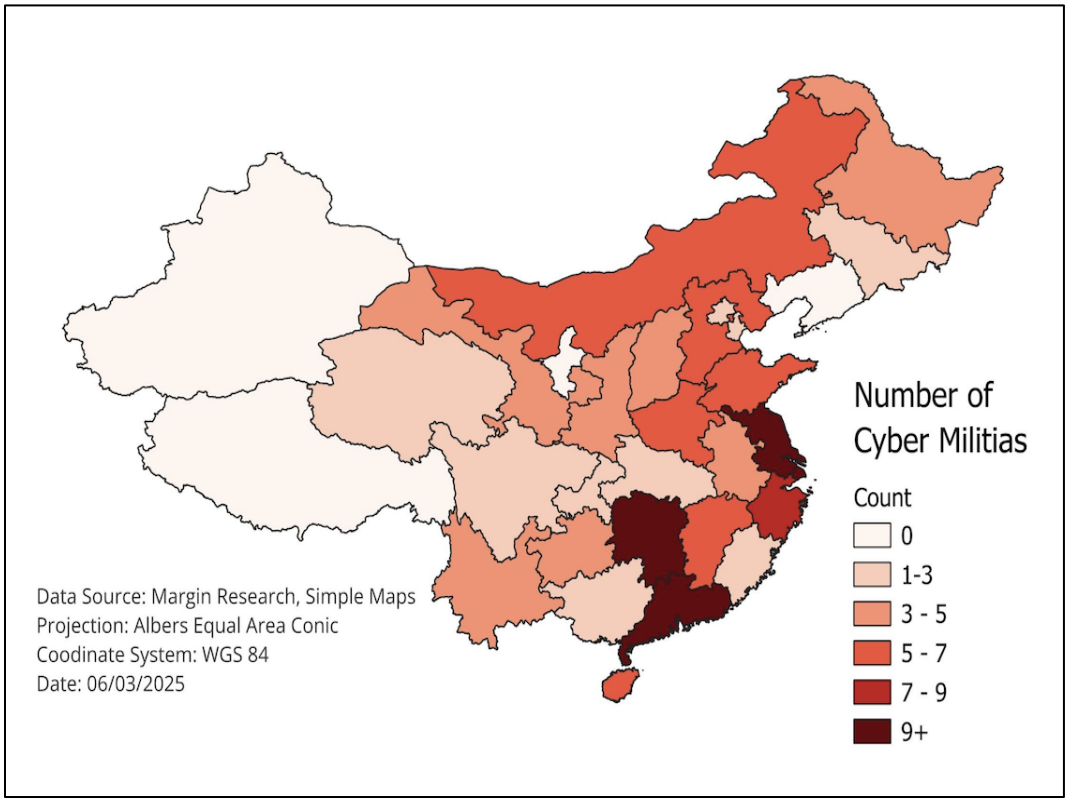


Figure 7: Provincial distribution of cyber militia units.[126]

* For instance, the main campus of the National University of Defense Technology (NUDT) is located in Changsha in Hunan.

This pattern becomes even more apparent when examining the locality-level basing of cyber militia elements. Units are overwhelmingly concentrated in major urban centers, reinforcing the conclusion that cyber militia recruitment and organization are driven primarily by access to human capital and technological infrastructure, rather than a top-down alignment with the PLA's regional operational requirements.

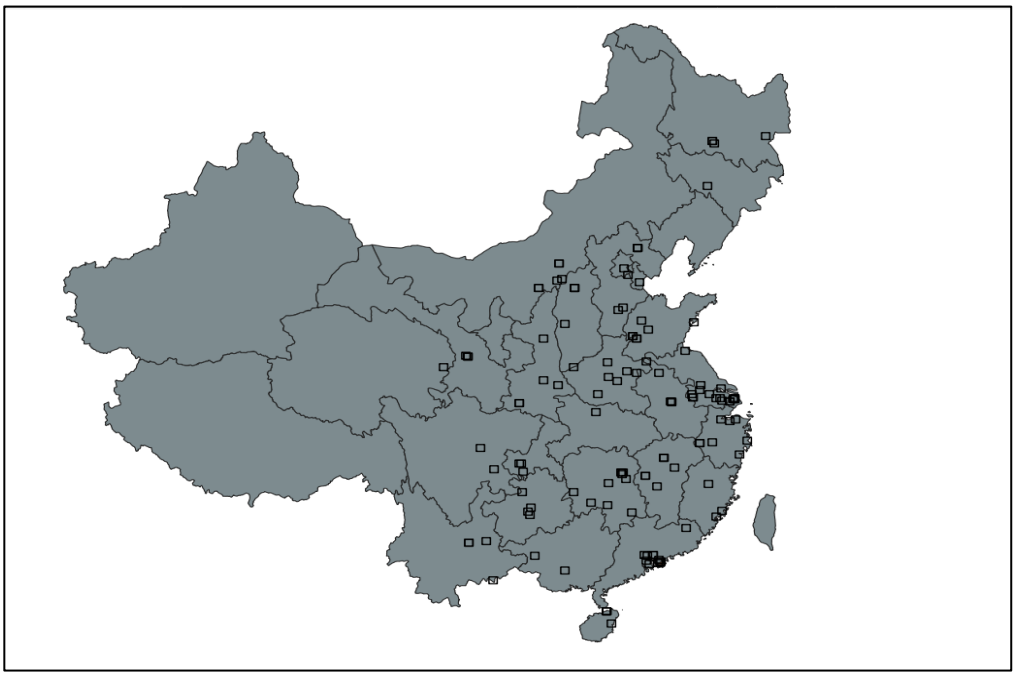


Figure 8: Geographic dispersion of cyber militia forces.[127]

Membership Requirements

Having established the institutional sources from which cyber militia units are drawn, it is necessary to examine the characteristics of those selected to serve within them. In keeping with the Maoist axiom of recruiting troops who are both "red" and "expert," cyber militia recruitment emphasizes quality over quantity.*[128] This approach dictates that membership in cyber militia forces is subject to a dual imperative. Personnel must possess both the technical acumen required for modern information warfare and the political reliability (i.e., loyalty to the Chinese Communist Party) deemed essential for working on sensitive national security tasks.[129] Accordingly, militias typically structure recruitment around a prioritization framework emphasizing "high-tech talent first, professional skill first, and demobilized military personnel first" (高科技人才优先、专业技术优先、退役军人优先), designed to ensure that militias are made up of individuals with demonstrated organizational ability, political reliability, and technical competence.[130]

* The "red" vs. "expert" dichotomy refers to a historical tension in the PRC between political loyalty and technical competence or professional expertise, respectively.

Cyber militia personnel are recruited from a range of professional sectors, including cybersecurity firms, research institutes, telecommunications operators, IT companies, and universities.[131] Specific employee profiles sought include network engineers, software developers, systems administrators, and in some cases, individuals with offensive security experience such as penetration testers or individuals with backgrounds in vulnerability research.[132] Foreign language specialists are also recruited, although their exact role is ambiguous (though it would be reasonable to assume that they aid missions pertaining to foreign intelligence collection or cross-border cyber operations).[133] When recruiting these personnel, PRC authorities appear increasingly willing to relax certain traditional standards in order to secure high-value technical talent. This includes adjusting norms related to unit size, age distribution, fitness requirements, veteran-to-civilian ratios, and Party membership, while also broadening the permissible channels from which recruits may be drawn.[*134] Leadership selection for these units tends to draw from demobilized PLA personnel, early and mid-career academic faculty, and other individuals with proven reliability and administrative capacity.[135†] The degree to which CCP membership is required for militia leadership positions remains unclear. However, there are indications that Party affiliation (or at least expressed interest in joining the Party) is a preferred credential.[‡136]

Equally important to technical competence is political reliability. A central priority of the Party-state has been to strengthen the ideological foundation of militia units through sustained political and ideological education. This is especially critical for cyber militia personnel involved in tasks related to public opinion management or countering enemy psychological warfare, which may involve suppressing dissent or managing "contradictions among the people" during wartime or emergency conditions.[137] In the words of one Party-affiliated author:[138]

> "The world has entered a new period of turbulence and change, and ideological struggles have become more complex. Hostile forces are attempting by every means to infiltrate our country through ideology. We must tighten our awareness of struggle, strengthen the ideological foundation of loyalty to the Party, and ensure that the militia remains absolutely loyal, absolutely pure, and absolutely reliable."

Accordingly, training regimens incorporate significant political content, aimed at cultivating "loyalty to the Party, love for the people, and dedication to the country" (忠于党、热爱人民、献身国家).[139] These educational measures include structured lectures, guided study sessions, film screenings of revolutionary or patriotic content, and organized group discussions. They also

[*] This trend is corroborated by a limited number of data points. For instance, one cyber militia detachment in Zhenjiang reported an average member age of 32, which is significantly older than the usual demographic for PRC militia units that typically composed of individuals in their twenties

[†] The prioritization of educators is logical, as they are likely to have already undergone ideological vetting, possess relevant subject matter expertise and, in many cases, are already Party members.

[‡] For instance, one network militia unit in the Yingshan Military Sub-District requires that an active CCP cadre serve as the team leader, a Party member from the Yingshan organizational unit act as the political instructor, and a technically proficient specialist be appointed as the deputy team leader.

feature regular briefings on China's overall "national defense situation" (国防形势) designed to provide ideological grounding and instill a sense of importance of regarding missions assigned to militia units.[140]

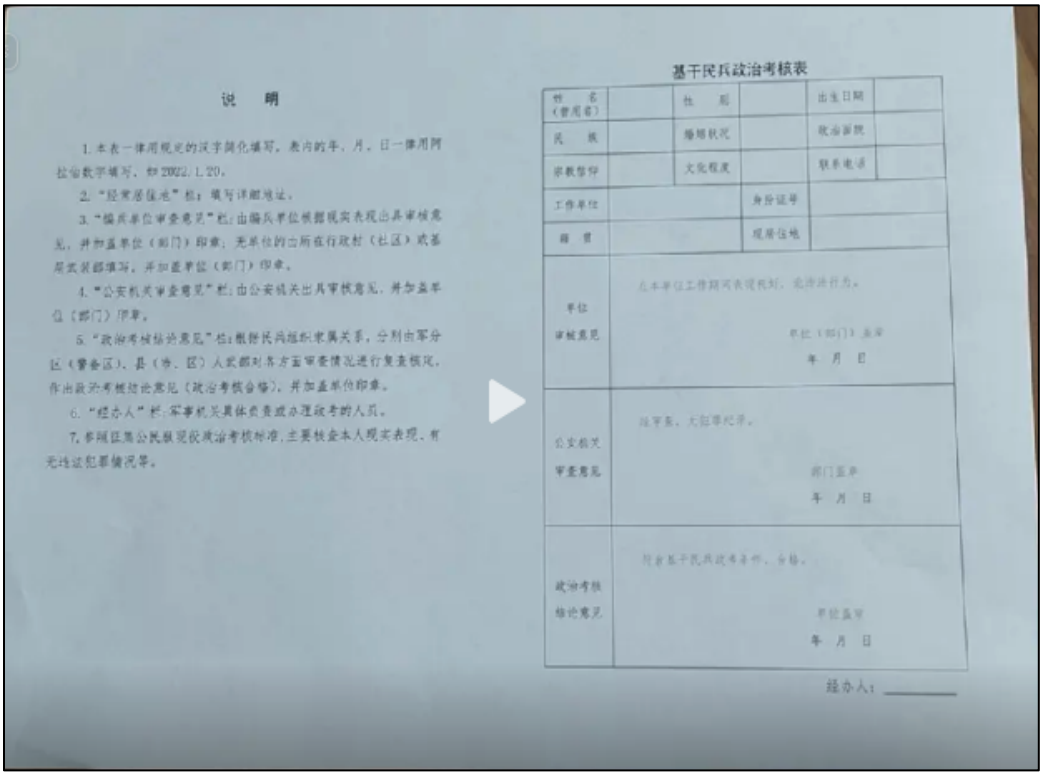


Figure 9: Questionnaire from the "Basic Militia Political Assessment Form" (基干民兵政治考核表) used to screen cyber militia members.[*] [141]

Organizational Structure

The PRC operates a tiered, locality-based organizational framework for the development of its cyber militia forces, following the guiding structure of "province forms companies, cities form teams, and counties form squads" (省建连、市建队、县建班).[142] This system is designed to ensure administrative oversight and scalability across regional levels, aligning cyber mobilization efforts with the broader national defense architecture. Units within this system are typically organized geographically, dividing responsibility by region, district, or street-level jurisdictions.[143] In turn, work units that support militia construction (e.g., specific enterprises, clusters of enterprises, or affiliated work units) are organized according to their core competencies.[144]

[*] The form includes sections for detailed residence information, reviews and official seals from the respondent's work unit and local MPS office, and a final political assessment by military officials to verify political reliability and the absence of illegal or criminal conduct.

Within this structure, cyber militia units are categorized into three core types based on function and personnel composition. The first category, referred to as "standing units" (常备型), consists of relatively stable formations embedded within government telecommunications regulatory agencies, state-owned or major private telecom providers, and large-scale network technology enterprises.[145] These units maintain consistent operational readiness and serve as the primary force for executing cyber defense missions under Party-state direction. The second category, reserve units (储备型), draw from technically skilled individuals employed in small- and medium-sized IT enterprises, as well as organized networks of independent cybersecurity enthusiasts.[146] Personnel selected for these units are expected to possess mid-level or higher offensive and defensive cyber capabilities consistent with industry standards and are placed into a managed talent pool for surge activation when required. The third category, "expert units" (专家型), comprises elite personnel recruited from universities, research institutes, and commercial firms with strong innovation capacity in technical fields. These units are composed of specialists (including senior engineers, academic experts, and R&D leaders) who serve in key technical, advisory, and leadership roles in support of complex or high-priority cyber missions.[147]

Type	**Work Unit Source**	**Primary Characteristics**
Standing (常备型)	Government telecom regulators, telecom carriers, large IT enterprises.	Permanent units with low personnel units; mainly used for operational tasks related to civilian infrastructure operations.
Reserve (储备型)	Medium/small IT firms, cyber enthusiast communities.	Personnel with mid-level industry skills; managed talent pool that can provide surge capacity when needed.
Expert (专家型)	Universities, research institutes, high-tech firms with R&D capacity.	Highly skilled specialists such as senior engineers, academics, and specialists; fulfills technical advisory and mission-critical roles

Organizational structures and unit sizes within China's cyber militia system appear to vary considerably based on locality and mission requirements. However, most available reporting suggests that individual militia squads typically consist of 10 to 30 personnel, with larger units composed of multiple such squads.[148] These squads constitute the basic organizational building blocks for operational deployment and serve as the primary entities for executing combat

missions.[149] Structurally, cyber militia formations appear to generally adhere to conventional military organizational norms, with clearly defined roles and chains of command. For example, one telecommunications support unit based in Shandong Province was reported to consist of a platoon leader (排长), one maintenance engineer (维修工程师), two team leaders serving concurrently as network technicians (班长兼网络技术员), one team leader serving as a data technician (班长兼数据技术员), and eleven network equipment repair specialists (网络设备修理员).[150]

Training for these forces is structured around a rotational model designed to maintain continuous operational readiness across units. Annual training tasks and professional development timelines dictate the phased rotation of squads, with city-level emergency battalions and county-level emergency companies designated for active standby.[151] Under this model, cyber militia units are placed on rotating standby schedules according to seasonal demands and evolving mission requirements. These units are maintained at staggered readiness levels. Those completing prior rotations, currently in training, or preparing for upcoming cycles are assigned differentiated combat readiness levels.[152]

Mission Sets

The mission sets for China's cyber militias are organized into four primary categories. First, they serve as one of the primary guarantors for managing and securing critical national network infrastructure. Second, they act as a reserve force for network attack and defense operations undertaken by the PLA. Third, they provide essential support for the protection and concealment of network targets, serving as decoys or false targets to obscure key assets. Fourth, they function as the backbone of efforts to shape and influence domestic online public opinion. Mission assignments for work units are designated by the local PAFD office, which evaluates those units' core competencies and ensures that these assignments are in alignment with regional defense priorities and operational requirements.[*] [153] Importantly, these mission sets are not mutually exclusive. Depending on available resourcing and operational requirements, local PAFD offices may assign multiple functional roles to individual militia units in order to address capability shortfalls and ensure mission coverage.[154]

[*] For example, in university-affiliated militia units, personnel are typically drawn from specialized departments such as information security, communication engineering, electronic information engineering, and computer science. This structure is mirrored across other militia elements responsible for various aspects of information warfare. To wit, university-affiliated electronic warfare units are composed of personnel from departments such as electronic science and technology, applied physics, and electronic information engineering. Similarly, psychological warfare elements at universities are staffed by individuals from relevant departments such as psychology, communication, journalism, and ideological and political education.

Safeguarding Network Infrastructure

Cyber militia units serve as a "main force" (主体力量) in the defense and sustainment of critical public infrastructure such as telecommunications networks, IT platforms, industrial control systems, and other essential services.[155] * Functionally, these units are responsible for tasks such as identifying and mitigating system vulnerabilities, deploying specialized IT personnel to restore communications infrastructure following cyberattacks or kinetic disruptions, and participating in joint defense exercises targeting high-value nodes such as telecommunications hubs, DNS infrastructure, and energy sector control systems.[156] They also support the deployment of mobile communications platforms (e.g., portable VSATs) to maintain command-and-control continuity in degraded or blackout conditions.[157]

Figure 10: Flag Presentation with the communications support unit of China Telecom Xiaonan Branch. [158]

* The characterization of cyber militia units as the "main force" in safeguarding network infrastructure appears somewhat incongruent with the statutory mandates of institutions such as MPS, CNCERT, and CAC, which also hold responsibilities in this domain. While the precise division of labor among these actors is not fully apparent, source material indicates that militia units serve as a key operational layer in ensuring the resilience and functionality of dual-use network infrastructure that supports PLA mission sets.

In addition to network and communications maintenance tasks, cyber militia forces are integrated into broader protective frameworks through cross-training with other militia components. These responsibilities may encompass support to air defense early warning networks, counter-reconnaissance against adversary electronic surveillance systems, electromagnetic spectrum management, network asset monitoring, network-based surveillance operations, and the implementation of camouflage and deception measures to protect critical infrastructure.[159]

Providing a Reserve Force for the PLA

In addition to their primary role in safeguarding infrastructure critical to PLA operations, cyber militia units serve as a strategic reserve force for the PLA during wartime. Collectively, these militia forces possess capabilities that parallel those of the PLACSF and PLAISF, and can be task-organized based on mission requirements or the operational units they support.[160] These tasks encompass specific cyberspace combat roles, including information reconnaissance, electronic warfare, and counter-network intrusion operations.[161] Additionally, cyber militia personnel serve as a replenishment pool to reinforce front-line PLA network units that are spread thin due to an overload of tasking or that have been physically attrited from combat.[162]

Figure 11: Staff from Suzhou University representing the Xiangcheng District Militia Attack and Defense Squad.[163]

As a general rule, PLA cyber militia units serve as rear-echelon support elements, tasked with sustaining network operations through backend functions such as firewall maintenance, system patching, and routine network defense.[164] This support role enables front-line PLA cyber

forces to focus on high-priority offensive and strategic missions during periods of heightened tension or armed conflict. However, it is important to note that many of the cyber militia teams (particularly those specializing in network attack and defense) possess the technical proficiency to conduct offensive cyber operations if required.[165] These capabilities include signal jamming, network intrusion, and the deployment of malicious code aimed at degrading or paralyzing adversary command, control, and communications infrastructure.[166]

Cyber militia units generally train to meet the operational needs of their overseeing Theater Command. In many cases, this entails training for specific conflict scenarios, such as potential contingencies in the South China Sea or the Taiwan Strait. For instance, since at least 2013 the Hainan Provincial Military District has fielded more than 100 professional militia detachments focused on supporting "maritime informatized warfare" (海上信息化战争).[167] These units provide communications and engineering support and contribute to a wide range of missions, including air defense, maritime patrols, electronic warfare, and information operations.[168] Over the past ten years, training for these units has become increasingly integrated into joint exercises with frontline PLA units and other specialized militia detachments, such as those operating unmanned aerial vehicles (UAVs) or conducting electronic warfare.[169] These stepped-up training efforts appear to be motivated in large part by the operational needs of the Southern Theater Command, with one PLA commentator noting that:[170]

> "At present, the situation in the South China Sea is becoming increasingly tense and urgent. The Hainan Provincial Military District focuses on ensuring victory in the maritime information war and vigorously strengthens the joint exercises and training of the maritime militia and active troops."

Moreover, while specific cyber militia units have not been publicly designated for participation in a Taiwan-related contingency, authoritative commentary strongly implies that their involvement is anticipated in high-intensity conflict scenarios, such as island landing operations.[171] One PLA-affiliated analyst, for example, frames the development of cyber militia capabilities explicitly within the context of cross-Strait conflict, arguing that "once the militia network attack and defense team forms combat effectiveness, it will be an important supplement to the PLA's future anti–'Taiwan independence' military struggle."[172] Such assessments indicate that PLA operational planners anticipate cyber militia forces will serve as a meaningful supporting element in future wartime operations and structure force deployment plans with that role in mind.

Strategic Deception

The third core mission set assigned to China's cyber militia forces involves supporting efforts to conceal and deceive adversary targeting in cyberspace by serving as "false and disguised targets" (充当虚假和伪装目标). This entails militia units constructing decoy systems designed to mislead hostile cyber operators and divert attacks away from critical military or government

infrastructure.[173] Operational examples may include the deployment of honeypots that mimic sensitive systems, the emulation of encrypted command-and-control traffic to obfuscate genuine communications, the registration of spoofed domains to disrupt malware operations, and the orchestration of staged outages or fabricated vulnerabilities intended to bait intrusion attempts.[174] Collectively, these efforts aim to complicate adversary decision-making, saturate targeting cycles, and obscure the operational footprint of China's cyber forces.

Among the various mission sets attributed to cyber militia units, this deception function is the least documented in available sources. It remains unclear how widely such capabilities are distributed across militia formations or to what extent the PLA formally integrates deception operations into its cyber doctrine. This lack of detail may reflect the operational sensitivity of such missions. Alternatively, it may indicate that such missions are sparingly assigned to elite militia units with advanced competencies.

Public Opinion Management

An often-overlooked but essential function of the PRC cyber militia forces is their role in conducting public opinion guidance (舆论引导) aimed at shaping perceptions among China's civilian populace.[175] The Party-state regards information security as extending beyond the technical protection of networks and the electromagnetic spectrum to include the ideological stability of the domestic information environment.[176] To this end, China has built an expansive system for monitoring and shaping public discourse, integrating propaganda work, censorship mechanisms, and public opinion surveillance across multiple state bureaucracies.[177] However, even in peacetime, these systems operate at or near capacity.[178] Accordingly, in crisis scenarios such as major public health emergencies or periods of elevated geopolitical tension, the Party-state often turns to militia units to reinforce its information control apparatus.

The inclusion of public opinion guidance in the cyber militia portfolio reflects the PLA's understanding of the information domain as a unified construct encompassing cyberspace, the electromagnetic spectrum, psychological operations, and intelligence collection.[179] Militia units are organized to align with this framework by securing communications infrastructure, countering hostile information operations, and engaging civilian populations in ways that reinforce CCP narratives and support the Party's broader information control objectives.[*] [180]

Within cyber militia formations, public opinion guidance responsibilities are typically undertaken either by dedicated public opinion monitoring detachments (网络舆情分队) or by dual-hatted technical units that combine cyber defense functions with information control tasks.[181] Regardless of organizational structure, these units share a common set of responsibilities. They are tasked with monitoring online discourse across social media platforms and internet traffic,

[*] To wit, it is not uncommon to see public opinion specialists, psychological warfare personnel, and "legal struggle" (法律斗争) teams organized alongside cyber operators within the same broader cyber militia detachment.

identifying narratives that deviate from Party-sanctioned messaging, and evaluating the potential for digital content to generate public unrest.[182] Their operational duties also include conducting sentiment analysis, suppressing so-called "harmful rumors" (有害谣言), and promoting state-aligned narratives.[183] Curiously, this mission set places cyber militia units under dual lines of accountability. On one hand, they support local Party Propaganda Departments and MPS bureaus in the realm of public opinion control; on the other, they report to local military authorities for tasks related to network defense and information operations. It remains unclear how command authorities reconcile these overlapping responsibilities (e.g. whether through standardized procedures or on a more decentralized, ad hoc basis).

A rare public example of cyber militia employment in a real-world contingency occurred during the COVID-19 pandemic. From 2020 to 2023, cyber militia units were mustered through the national defense mobilization system to assist both in technical support and public sentiment control. [184] As part of this effort, district-level network militia detachments compiled and disseminated daily reports on COVID-related online discourse, maintained 24-hour surveillance of public opinion channels, and countered so-called "misinformation and rumor propagation."[185] These militia units' local knowledge, coupled with technical expertise, allowed them to identify pain points within the population and shape communication strategies accordingly.[186] Beyond public opinion monitoring, cyber militia personnel also assisted with practical support tasks, such as analyzing population movement and health data to aid companies in returning to work, and conducting in-person operations including surprise inspections, emergency transport, and frontline epidemic prevention. [187]

Figure 12: Sanmenxia District Militia Public Opinion Monitoring and Guidance Platoon deployed to assist pandemic response efforts during the COVID-19 Pandemic[188]

This aspect of China's cyber militia mission set is particularly significant because it offers a window into how the system might function during other crisis scenarios, such as future high-intensity conflicts. It is conceivable that in a wartime contingency, militia units would likely be called upon to help manage the domestic consequences of sustained attrition (such as high casualty rates among PLA personnel) and to mitigate the psychological and social strains imposed on the civilian population. In such contexts, cyber militia forces could serve as a powerful extension of the Party-state's information control apparatus. The fact that these units are both familiar with local information conditions and straddle the military and civilian information domains renders them well-suited to reinforce public support for wartime efforts, disseminate Party-approved narratives, and cultivate a shared sense of national purpose and collective sacrifice.

Spotlight: Cyber Militia Participation in National CTF events

Participation in cybersecurity competitions such as Capture the Flag (CTF) exercises has become a regular component of cyber militia training and talent identification across China.[189] These events offer a platform for sharpening the technical skills of cyber militia personnel, reinforce alignment between militia and active-duty PLA mission sets, and functioning as an informal recruitment mechanism.[190]

Figure 13: Cyber militia members participating in a CTF competition held during a training session for Anhui Province network militia detachments.[191]

The organizing entities and structure of these events vary widely. In some cases, local PAFD offices or Information Mobilization Offices (信息动员办) coordinate competitions that appear to be limited to military participants.[192] In other instances, the events are co-organized with academic institutions or leading private-sector firms such as Tencent.[193] This latter category typically features a broad base of participants from government agencies, SOEs, universities, private firms, and militia units.[194] Lastly, at higher echelons there is some evidence that Theater Commands have also hosted similar exercises involving militia components, although details on those competition proceedings remain unavailable to the public.[195]

Case Studies: China's New Cohort of Cyber Militias in Action

To demonstrate the evolving character of China's cyber militia system, this section features two case studies examining militia detachments affiliated with Qihoo 360 and Antiy Labs. These entities were primarily selected due to the relative transparency of their organizational structures and the availability of open-source reporting on their operations, composition, and institutional affiliations. While these examples do not reflect the typical cyber militia unit in terms of scale or sophistication, they are nonetheless significant. Both Qihoo 360 and Antiy represent the leading edge of industry participation in national defense mobilization and serve as models of what the

Party-state envisions as the future standard for cyber militia development. As such, their example offers valuable insight into the strategic direction and institutional aspirations shaping China's cyber militia reform agenda.

Qihoo 360

Since 2020, Qihoo 360 Technology Incorporated (三六零安全科技股份有限公司) has operated a cybersecurity militia unit (网络安全民兵分队) under the Jiuxianqiao Street (酒仙桥街道) militia unit based in Beijing's Chaoyang District.[196] The unit was jointly established by the 360 Group Party Committee and the Jiuxianqiao Street Party Working Committee (酒仙桥街道党工委) under the auspices of the Central Commission for Integrated Military and Civilian Development (中央军民融合发展委员会) and other unspecified military entities.[197] Its stated mission is to develop and maintain advanced cybersecurity defense capabilities in support of the PLA, in order to prepare for and prevail in future cyber conflicts. Reflecting this orientation, senior Qihoo executives have characterized its militia as a "cutting-edge cybersecurity defense force designed to help the PLA prevail in future cyber warfare."[198] Since its establishment, the unit has received repeated commendations from Party-state authorities and was nominated for the 2021 Spark Plan (火种计划) Digital Economy Party Building Outstanding Innovation Project Award (数字经济党建优秀创新项目提名奖).* [199]

* The "Spark Plan" (火花计划) is a national-level initiative aimed at fostering grassroots innovation and strengthening digital infrastructure, particularly in rural and underdeveloped regions.

Figure 14: Flag presentation by Jiuxianqiao Street Militia members[200]

Figure 15: Jiuxianqiao Street Militia unit members. [201]

Figure 16: Li Jianhua (李建华), Senior 360 VP (far right) alongside other militia representatives.[202]

Mission Set and Relationship with the Party-state

As one of the largest network security companies in China, Qihoo 360 plays a central role in supporting China's military and strategic aims in cyberspace.[203] The firm's leadership has made explicit the ideological and operational alignment between cybersecurity and state power, both by acting as a vendor for the PRC and PLA, as well as being closely integrated with Party-state cyber governance through ad hoc mechanisms and also formal engagements such as the National People's Congress and Chinese People's Political Consultative Conference. For example Qi Xiangdong, chairman of 360 Enterprise Security Group, has asserted that "cybersecurity is tied to national security, regime consolidation, social stability, and the outcome of war," framing cyberspace as "a new battlefield in the struggle between the enemy and us."[204] As such, the company maintains a demand-driven posture toward PLA requirements by aligning research and development efforts with military needs, and facilitating infrastructure and resource-sharing arrangements between civilian and military cybersecurity actors.[205] In this context, the Jiuxianqiao Street Militia serves as a formal channel through which Qihoo 360 contributes directly to the PLA's cyber defense efforts by providing network defense support, threat intelligence, and other related forms of assistance.[206] Qihoo 360 also advances PLA capabilities by producing dual-use tools and platforms with offensive and defensive applications.[207]

Unit Composition and Organizational Structure

The Jiuxianqiao Street Militia is led by "active military cadres with specialized tactical expertise" (分队的指挥员以具有一定战术思想的军队现役干部为主) and operates as a self-contained unit that reports to local military authorities.[208] Its personnel are drawn from Qihoo's

internal technical workforce, with recruitment focused on software developers and network researchers supported by hardware and operations staff. In order to support the sustainment and replenishment of these forces, Qihoo conducts annual surveys and maintains a registry of its employees with relevant technical backgrounds.[209] When recruiting members for the militia, Qihoo prioritizes Party members, probationary members, and active Party applicants in its selection process.[210] The majority of these militia possess bachelor's degrees or higher and have attained at least Level 2 certification (计算机二级) on China's National Computer Rank Examination (NCRE).[*] [211] Collectively, these data points suggest that a broad swathe of Jiuxianqiao Street militia members possess both a high degree of technical acumen and political reliability.

The Jiuxianqiao Street Militia's training architecture is designed to promote both political reliability and operational capability. A dedicated Party branch embedded within the militia structure is tasked with political education and ideological indoctrination with the aim of "arming the militia with the Party's advanced theories and ideas" and creating an "iron-blooded division that serves the people and is loyal to the Party."[†] [212] This political framework manifests through structured study sessions and ideological reinforcement programs administered by the unit's Party branch.[213] Additionally, the unit conducts frequent functional training sessions through guest lectures delivered by cybersecurity specialists and military officers, including national defense academicians from premier institutions such as the Academy of Military Sciences (AMS) and China's National Defense University (NDU).[214] Collectively, this curriculum fosters technically proficient cadres who can serve as reliable local network security guarantors that can also interface with uniformed PLA units to conduct joint operations.

[*] The National Computer Rank Examination (全国计算机等级考试) or NCRE is a standardized test administered by the Ministry of Education in China that assesses computer proficiency across various levels. In this case with Level 2 (计算机二级) typically indicates competence in a programming language (such as C, C++, Java, or Python) or in common software applications.

[†] In the context of Chinese private companies, a Party Branch (党支部) is the most basic unit of Communist Party organization, typically established when a company has at least three Party members; it focuses on grassroots Party activities and ideological work. A Party Committee (党委) is a higher-level body formed in larger companies or groups with a greater number of Party members, and it has broader authority over political and organizational matters. A Party Group (党组) is a more flexible, temporary structure usually embedded within the leadership of a company or institution to ensure Party oversight over major decisions, even when a full committee or branch is not present.

Figure 17: Qihoo 360 Party members. [215]

Operational Capabilities and Technical Competencies

The Jiuxianqiao Street Militia provides operational support to a wide range of Party-state entities, including direct assistance to the PLA through its militia framework and "network protection" (护网) services to China's internal security services such as the MPS.[216] The militia's core mission set includes the following tasks:

- Constructing network defense systems for military internet services and functioning as a threat intelligence-sharing platform to provide early warnings to the PLA.[217]
- Partnering with small- and medium-sized enterprises on technology research and development projects to ensure the availability of cyber defense solutions that meet operational combat requirements.[218]
- Conducting pilot programs for cyber militia development and implementing mechanisms for cyber emergency response as well as advanced persistent threat (APT) analysis and monitoring for military and local government agencies.[219]
- Engaging in network monitoring, cyber offense and defense, public opinion management, and advancing military-civilian fusion efforts in the field of cybersecurity.[220]

Operationally, the Jiuxianqiao Street Militia has demonstrated sustained deployment capabilities by consistently providing professional technical personnel to support cybersecurity operations.[221] Notable examples include deployments to international conferences such as the All-China Federation of Industry and Commerce gatherings and the Zhongguancun Forum.[222] The unit also supports ancillary tasks such as critical infrastructure protection and direct assistance to law enforcement in combating cyber fraud and information theft.[223]

Figure 18: Beijing Garrison Command leadership members visiting Qihoo headquarters during the founding of the Jiuxianqiao Street Militia. [224]

Figure 19: 360 personnel meeting with Beijing militia representatives [225]

Antiy Labs

Beijing Antian Network Security Technology Co. (北京安天网络安全技术有限公司), colloquially known as Antiy Labs, maintains one of the largest and most operationally advanced cyber militias in China. The unit was founded in 2018 and purportedly boasts over 100 personnel, making it the largest single cyber militia unit in the PRC.[226] Unlike most China cyber militias (which are typically tied to specific districts or sub-districts) Antiy's unit appears to operate at a broader geographic level, providing support across the entire Harbin region.[227]

In addition to its size and advanced capabilities, Antiy maintains unusually close ties to the Party-state. The company has been formally recognized by military authorities and maintains an active role in national cybersecurity policymaking. As detailed earlier in this report, Antiy's founder and Chief Technical Architect Xiao Xinguang provides the firm with a direct channel for influencing high-level cyber policy through his role as a member of the CPPCC National Committee.[228] He appears to have used this access to position the company as a template to showcase political reliability and deeper private-sector integration into defense structures.

Figure 20: Antiy Labs Cyber Militia Members outside company headquarters circa 2018.[229]

Figure 21: Antiy Labs cyber militia unit members circa 2018. [230]

Mission Set and Relationship with the Party-state

Antiy's cyber militia is organized around a mission profile that reflects the Party-state's prioritization of information infrastructure protection in the face of persistent foreign cyber intrusion.[231] Its stated mission set is to "provide security solutions for major national tasks and strengthen emergency support capabilities" (国家重大任务提供安全解决方案，强化应急保障支撑能力).[232] Accordingly, the Antiy militia unit specializes in incident response, threat detection, cyber threat hunting and incident management.[233] Beyond traditional cybersecurity missions, Antiy's cyber militia has historically undertaken additional roles within related operational domains. For instance, during the COVID-19 pandemic it leveraged its big data management platform to assist the Harbin municipal government in monitoring worker health status.[234]

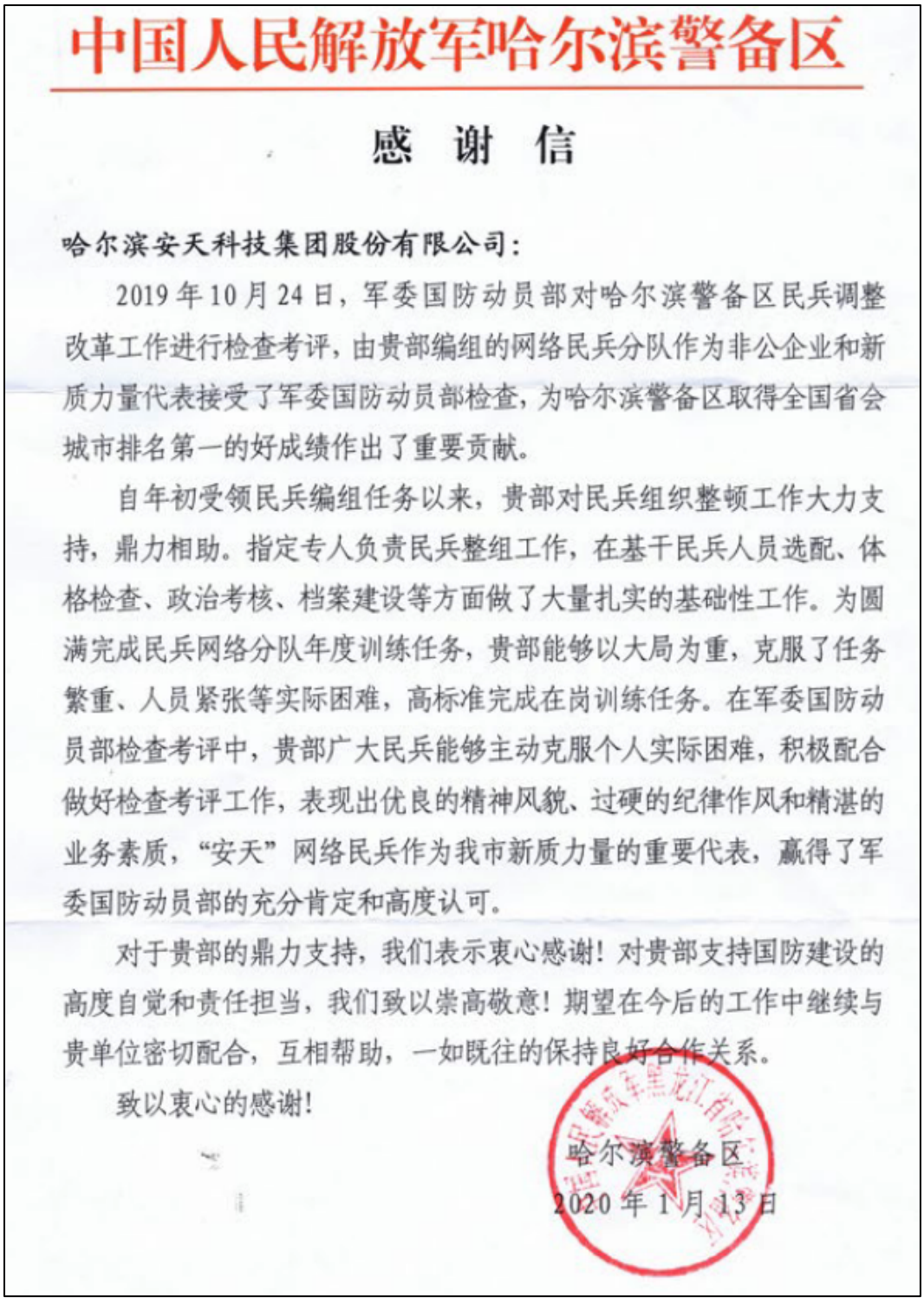
Antiy's leadership and organizational ethos exemplify the deepening linkages between private-sector cybersecurity companies and China's defense establishment. Xiao Xinguang's role as both an interlocutor between the cybersecurity industry and Party leadership, and as the architect of a politically aligned operational model points to the emergence of a new paradigm for private sector participation in national defense.[235] In this context, Antiy's efforts to translate political signaling into institutional practice by standing up a large and operationally capable cyber militia unit demonstrate how support for national security objectives has become not only a marker of patriotism but also a strategic pathway to commercial opportunity and regulatory favor.[236] This approach has been endorsed by other members of the firm's leadership. For example, Miao Chang, Chairman of the Antiy Labor Union and Commander of its cybersecurity militia unit, has emphasized the importance of "seizing the historical opportunities of the current information technology revolution and the new military revolution" to support national defense objectives.[237]

As such, Antiy's mission set cannot be understood solely in terms of force generation; it is also a trusted enterprise whose leaders deeply shape China's national cyber defense mobilization paradigm.[238]

Unit Composition and Organizational Structure

Antiy's cyber militia is primarily composed of the company's emergency response and analysis engineers, reflecting its core competencies in threat intelligence and incident response.[239] The unit appears to chiefly support the PLA's Northern Theater Command by building localized network security capabilities across China's three northeastern provinces to provide defense of critical infrastructure.[*] [240] While not explicitly stated, it is possible that Antiy's mission remit includes countering cyber threats posed by Russian and North Korean APT groups, given its focus on the border provinces most exposed to these adversaries.

[*] The reference to the three northeastern provinces most likely denotes Liaoning, Jilin, and Heilongjiang, which together comprise a large part of the PLA's Northern Theater Command area of responsibility. Given that Antiy is based in Harbin (Heilongjiang's capital) its cyber militia efforts are logically focused on this strategic area, which borders Russia, North Korea, and the Yellow Sea.



中国人民解放军哈尔滨警备区

感 谢 信

哈尔滨安天科技集团股份有限公司：

2019年10月24日，军委国防动员部对哈尔滨警备区民兵调整改革工作进行检查考评，由贵部编组的网络民兵分队作为非公企业和新质力量代表接受了军委国防动员部检查，为哈尔滨警备区取得全国省会城市排名第一的好成绩作出了重要贡献。

自年初受领民兵编组任务以来，贵部对民兵组织整顿工作大力支持，鼎力相助。指定专人负责民兵整组工作，在基干民兵人员选配、体格检查、政治考核、档案建设等方面做了大量扎实的基础性工作。为圆满完成民兵网络分队年度训练任务，贵部能够以大局为重，克服了任务繁重、人员紧张等实际困难，高标准完成在岗训练任务。在军委国防动员部检查考评中，贵部广大民兵能够主动克服个人实际困难，积极配合做好检查考评工作，表现出优良的精神风貌、过硬的纪律作风和精湛的业务素质，“安天”网络民兵作为我市新质力量的重要代表，赢得了军委国防动员部的充分肯定和高度认可。

对于贵部的鼎力支持，我们表示衷心感谢！对贵部支持国防建设的高度自觉和责任担当，我们致以崇高敬意！期望在今后的工作中继续与贵单位密切配合，互相帮助，一如既往的保持良好合作关系。

致以衷心的感谢！

哈尔滨警备区

2020年1月13日

Figure 22: Letter of commendation from the Harbin PLA Garrison Command to the Antiy Militia Network Detachment.[*] [241]

[*] An English translation of the letter is as follows: “On October 24, 2019, the Central Military Commission's National Defense Mobilization Department inspected and evaluated the adjustment and reform of the militia of the Harbin Garrison. The cyber militia detachment organized by your department accepted the inspection as a representative of non-public enterprises and new-type forces, and made important contributions to the Harbin Garrison's achievement

Figure 23: "Outstanding Grassroots Militia Advanced Collective" award presented by the PLA Harbin garrison to Antiy Labs.[242]

Antiy's leadership has articulated a clear ambition to shape the future architecture of China's cyber militia system. For instance, Xiao Xinguang has advocated for inducing provinces with strong cybersecurity industrial bases (such as Heilongjiang) to contribute network infrastructure for national-level cybersecurity initiatives.[243] At the same time, he has called for encouraging more large-scale cybersecurity and internet companies in these regions to establish dedicated cyber militia units that would be stood up in coordination with their respective Theater Commands.[244] Moreover, at the national level Antiy has proposed the development of an integrated cybersecurity emergency and combat-readiness framework that would merge government and enterprise resources.[245] This would entail strengthening coordination through the National Internet Emergency Center and institutionalizing a hybrid readiness system, whereby

of ranking first among provincial capital cities in the country. Since receiving the task of organizing the militia at the beginning of the year, your department has strongly supported and assisted the organization and rectification of the militia. A special person was designated to be responsible for the organization of the militia, and a lot of solid basic work was done in the selection of basic militia personnel, physical examination, political assessment, and archive construction. In order to successfully complete the annual training tasks of the militia network team, your department was able to focus on the overall situation, overcome practical difficulties such as heavy tasks and tight personnel, and complete the on-the-job training tasks with high standards. In the inspection and evaluation of the Military Commission's National Defense Mobilization Department, the majority of militiamen in your department were able to take the initiative to overcome their difficulties and actively cooperate in the inspection and evaluation work, showing excellent spirit, strong discipline and superb professional quality. As an important representative of the new quality of our city, the "Antiy" network militia has won full recognition and high recognition from the Military Commission's National Defense Mobilization Department. We would like to express our sincere gratitude for your strong support! We have the highest respect for your high awareness and sense of responsibility in supporting national defense construction! We hope to continue to work closely with your unit in the future, help each other, and maintain a good cooperative relationship as always. With sincere thanks!" -- Harbin Garrison District, January 13, 2020

large cybersecurity enterprises and key infrastructure operators are placed at the disposal of the PLASSF (now PLACSF and PLAISF) and the national defense mobilization apparatus.[246]

Operational Capabilities and Technical Competencies

Antiy's core technical responsibilities include the detection and analysis of malicious code, as well as tracking APTs, analyzing adversarial infrastructure, and conducting rapid response to major cyber incidents such as zero-day vulnerabilities.[247] Accordingly, its militia maintains a specialized focus on high-risk contingency operations in addition to participating in routine militia training programs organized under the supervision of higher-level military authorities.[248] This entails scenario-based training designed to prepare personnel for foreign cyber intrusions targeting China's critical information infrastructure, as well as broader emergency response requirements associated with high-intensity cyber conflict.[249] To meet the requirements of this mission set, the militia is equipped with a range of portable toolkits such as emergency incident response kits, traffic monitoring platforms, and sandbox analysis environments designed to enable rapid deployment and on-site triage of emerging cyber threats.[250] Antiy militia personnel are also embedded in 24/7 security support teams, often traveling across regions to support high-profile or time-sensitive security operations.[251] During major national events, these personnel conduct monitoring and analysis of inbound and outbound internet traffic in order to assess threat vectors and maintain the integrity of client networks.[252]

Conclusions and Takeaways

Challenges and Future Trends in China's Cyber Militia System

Under Xi Jinping, the PRC has labored to transform its cyber militia forces into a sharper, more potent instrument of state power. Nevertheless, despite over a decade of reform and expansion, the system remains marked by uneven capability development, inconsistent coordination across administrative levels, and serious gaps in mobilization readiness. These challenges, if unresolved, could undercut the militia system's strategic utility during a crisis or conflict.

Structural Fragmentation and Local Infrastructure Dependence

One of the central dilemmas facing the cyber militia system is its dependence on local infrastructure and human capital, which leads to wide disparities in operational effectiveness across regions. Unlike regular forces under the PLACSF and PLAISF, militia cyber units are raised, trained, and partially equipped by local PAFD departments and regional governments. As a result, their capacity correlates strongly with local access to high-tech talent pools and organizational resources.[253] As such, less developed provinces (especially those with strategic relevance like Tibet and Xinjiang) continue to face acute shortfalls in recruitment and capability.[254] According to PAFD leaders, the lack of training sites and equipment and weak training strength are a major

problem affecting the quality and effectiveness of militia training, and ability to generate a high-quality force.[255] This fragmentation also undermines fungibility across units. Cyber operators, despite theoretically being non-location-bound, often maintain loyalty and practical ties to their host regions.[256] These ties, along with the fact that cyber militia personnel are not subject to the same service obligations as uniformed PLA troops, limit central military authority's ability to reassign units flexibly and surge forces where needed during national-level contingencies.[257]

Recruitment, Training, and Retention Challenges

Despite high-profile efforts by the Party to enlist private firms in cyber militia development, the technical demands of cyber operations create high barriers to recruitment and retention. Civilian enterprises with relevant personnel often resist militia recruitment efforts due to the operational costs of releasing scarce, high-value staff.[258] This issue is particularly acute among small- and medium-sized enterprises, whose lean staffing models make them wary of sustained militia commitments.[259] In Suzhou, for instance, a local PAFD struggled to enlist just 20 employees from a communications firm because their absence (even for a 10-day training period) posed a risk to company functions.[260] Such cases are emblematic of a broader trend of the PLA's cyber mobilization ambitions frequently colliding with the realities of enterprise workforce planning.

Moreover, even when skilled recruits are secured, training programs often fail to bridge the gap between civilian technical expertise and battlefield readiness. To illustrate, a cadre overseeing one of Suzhou's aforementioned high-tech militia detachments noted that even among technically capable individuals, few possessed the "battlefield literacy" (i.e. military discipline and attention to operational security protocols) necessary for effective deployment.[261] To wit, many militia members frequently rely on workplace-standard operating procedures during training, rather than military tactics appropriate to a wartime environment.[262] In some instances, this has resulted in serious security violations due to militia members connecting personal laptops, mobile devices, or home computers to sensitive government and enterprise intranet networks.[263] Compounding these problems is the lack of suitable training infrastructure in many localities. In particular, the scarcity of cyber training ranges, live-fire simulation tools, and combat scenario planning still limits the effectiveness of exercises among militia units.[264]

Shortcomings in China's National Defense Mobilization System

Compounding these issues is the lack of a national-level cybersecurity strategic reserve and unified data exchange and sharing system to support national defense mobilization of cyber companies.[265] China currently lacks a unified mechanism for provisioning system platforms, software tools, and personnel during major cyber emergencies.[266] Furthermore, there is no normalized hierarchical national strategic reserve mechanism for the system platforms, technical equipment, software tools, storage carriers, etc. required for emergency response.[267] This gap in national preparedness undermines the PLA's ability to maintain a real-time inventory of

operational capabilities and hampers its efforts to execute the kind of complex joint cyber operations envisioned by military planners. To wit, although a small number of cities and counties have invested in "smart defense mobilization" platforms to facilitate resource mapping and mobilization planning, many still rely on paper records or outdated database management systems.[268]

Future Trends

Despite persistent limitations, China's ongoing investment in the expansion and modernization of its cyber militia system has produced tangible dividends. Moreover, it bears noting the Party-state does not regard this system as a finished product, but rather as an evolving component of broader defense reforms. Future initiatives may further strengthen the system through digitized force management to optimize recruitment pipelines, training programs, and resource allocation.[269] The PLA is also experimenting with new configurations that integrate militia and regular forces. These trial mobilization models entail linking pre-positioned technical equipment with designated militia personnel and conducting joint mobilization exercises with local governments to simulate wartime activation.[270] This hybrid model would enable the PLA to leverage civilian cyber capabilities without requiring full-time integration or direct command subordination.[271]

Implications and Policy Recommendations

The growing strategic operational role of China's cyber militias merits closer scrutiny in U.S. wartime contingency planning and peacetime policymaking. Given the evolution of the cyber militia system over the past decade and its projected trajectory, it is no longer analytically defensible to treat China's cyber militias as peripheral to the PLA's operational architecture. While current force capacity limitations will continue to constrain militia effectiveness in the immediate future, continued Party-state investment and reform efforts point to their potential emergence as a formidable tool for the PRC in the medium- to long-term.

Accordingly, while elite cyber operators within the PLACSF and other uniformed units remain central to Beijing's cyber strategy, these personnel increasingly represent only the most visible component of a much larger force structure. Below this tip of the spear lies a vast and growing ecosystem of militia-affiliated cyber personnel, embedded across state-owned enterprises, research universities, and commercial technology firms. Collectively, these entities provide the PLA with a latent reserve of technically capable operators that can be activated with minimal lead time to support a wide range of missions in the cyber domain.

The operational logic underpinning this system is straightforward. Unlike conventional reserve forces, which typically require extensive training in weapons handling, unit cohesion, and combined arms operations, cyber militia personnel are often drawn from segments of society that already possess relevant technical proficiencies. Many operate daily in roles related to

vulnerability discovery, malware analysis, digital forensics, or network engineering. PLA-affiliated commentary makes clear that, with proper oversight and direction, these individuals can be rapidly converted into a credible auxiliary cyber force.[272] In some cases, the boundary between support functions and offensive operations is intentionally blurred, allowing select militia units to pivot from rear-echelon tasks to frontline missions with little or no latency.

This characteristic has important implications for China's ability to generate cyber mass during high-tempo or prolonged operations. In conflict scenarios such as a Taiwan Strait contingency, the PLA's ability to surge cyber capabilities could depend heavily on the availability of trained reserve forces outside of the standing force structure. In this context, the functional distinction between China's active-duty cyber operators and their militia counterparts may be far narrower than in other warfighting domains, granting the PLA a scalable, adaptable means of sustaining pressure in the information environment. Moreover, cyber militia units increasingly participate in missions beyond technical network defense, including critical infrastructure protection, information control, public opinion guidance, and political warfare, further expanding their strategic utility in both peacetime and wartime contexts.

These developments require U.S. policymakers to revise foundational assumptions about the scope, scale, and composition of China's cyber capabilities. In particular, Western threat intelligence frameworks must move beyond their current fixation on state-directed APT groups to include non-traditional actors, including cyber militia detachments embedded in private industry and research institutions. U.S. operational planning should also account for the fact that cyber militias are likely to play a central role in pre-crisis infrastructure reconnaissance, crisis-era surge operations, and post-conflict resilience activities. Accordingly, U.S. planners should prioritize mapping China's cyber mobilization ecosystem, gaining visibility into dual-use commercial platforms with ties to PLA-affiliated units, and evaluating policy levers such as investment screening and export controls to constrain the Party-state's ability to leverage globally integrated tech firms for coercive purposes. Failure to account for this rapidly maturing component of China's cyber apparatus risks underestimating the scale of adversary capability the United States and its allies may confront in a future conflict.

Sources

[1] People's Liberation Army Dictionary (中国人民解放军语军语), Military Science Press (军事科学出版社), Beijing, 2011, pp. 32-36
[2] Costello, John, and Joe McReynolds. China's Strategic Support Force: A Force for a New Era. Washington, D.C.: National Defense University Press, 2018. https://digitalcommons.ndu.edu/china-strategic-perspectives/6/; Yatsuzuka, Masaaki, "PLA's Intelligentized Warfare: The Politics on China's Military Strategy," Security & Strategy, vol. 1, no. 2, October 2020; Dave Aitel et al, "China's Cyber Operations: The Rising Threat to American Security," Margin Research, 2022, https://margin.re/chinas-cyber-operations-the-rising-threat-to-american-security/.
[3] Joe McReynolds and LeighAnn Luce, "China's Human Capital Ecosystem for Network Warfare," in The People in the PLA 2.0, Roy Kamphausen (ed.), U.S. Army War College Press, Carlisle, PA, 2021; U.S. Department of Defense, "Military and Security Developments Involving the People's Republic of China," Annual Report to Congress, 2023.
[4] "Military-Civil Fusion and the People's Republic of China." Washington, D.C.: U.S. State Department, May 2020. https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf.
[5] People's Liberation Army Dictionary (中国人民解放军语军语), Military Science Press (军事科学出版社), Beijing, 2011pp. 32-33.
[6] People's Liberation Army Dictionary (中国人民解放军语军语), Military Science Press (军事科学出版社), Beijing, 2011, pp. 6-11.
[7] Zheng, Cindy, and Timothy Heath. "China's People's Armed Forces Departments: Developments Under Xi Jinping." Jamestown China Brief 24, no. 9 (April 26, 2024). https://jamestown.org/program/chinas-peoples-armed-forces-departments-developments-under-xi-jinping/; Xu Yonghan (徐永汉), and Zheng Ning (郑宁). "Mission Construction and Application of Militia Cyber Warfare Team (民兵网络战分队的任务建设与运用)." National Defense (国防), no. 8 (December 2006): 39–40; Ma Jianguang (马建光). "Cyber Militia: Every Citizen Is a Soldier in the Information War Era (网络民兵：信息战争时代的全民皆兵)." Guangming Daily (光明日报), August 10, 2016. https://web.archive.org/web/20250703160427/http://www.81.cn/theory/2016-10/08/content_7289960.htm; Hunan University of Humanities, Sciences, and Technology (湖南人科技学院). "Our School's Militia Team Participated in the Assembly and Inspection of the Basic Militia in Louxing District (我校民兵分队参加娄星区基干民兵集合点验)." April 27, 2023. https://web.archive.org/web/20250703161013/https://www.huhst.edu.cn/wbc/info/2018/4257.htm; Rongguang Technology (戎光科技). "Smart Mobilization System: Serving in Peacetime, Responding to Emergencies, and Fighting in Wartime (智慧动员系统：平时服务、急时应急、战时应战)." September 22, 2023. https://web.archive.org/web/20250703161004/https://www.sohu.com/a/722656107_121337322.
[8] Andrew, Martin Kenneth. "Tuo Mao: The Operational History of the People's Liberation Army." Bond University, 2008.
[9] Xiao Tianliang (ed.). In Their Own Words: The Science of Military Strategy. Beijing: PLA Academy of Military Sciences (Translated by the China Aerospace Studies Institute, 2020. pg. 29
[10] Manhas, Neeraj Singh, and Hari Yadav. "China's Military-Civil Fusion from Mao to Xi: A Long Roadmap." Journal of Polity & Society 16, no. 1 (2024): 45–58.
[11] Shu Ke (舒可). "Looking at Milita Force Building From the Perspective of Anti-Epidemic Efforts (从抗疫看民兵力量建设)." China Military Online (中国军网), July 1, 2020. https://web.archive.org/web/20231022175831/http://www.81.cn/gfbmap/content/2020-07/01/content_264897.htm.
[12] Gu Gang (谷钢), A Brief Discussion on the Construction of Combat Capabilities of College Militia Information Units (略论高校民兵信息分队作战能力建设), Central South University (中南大学), Master's Thesis, 2010.
[13] Gu Gang (谷钢), A Brief Discussion on the Construction of Combat Capabilities of College Militia Information Units (略论高校民兵信息分队作战能力建设), Central South University (中南大学), Master's Thesis, 2010.
[14] Gu Gang (谷钢), A Brief Discussion on the Construction of Combat Capabilities of College Militia Information Units (略论高校民兵信息分队作战能力建设), Central South University (中南大学), Master's Thesis, 2010.
[15] Chang, Yu-Ping. "National Defense Mobilization: Toward A Clear Division of Labor between the PLA and Civilian Bureaucracies." Jamestown China Brief 24, no. 6 (March 15, 2024).

[16] Chang, Yu-Ping. “National Defense Mobilization: Toward A Clear Division of Labor between the PLA and Civilian Bureaucracies.” Jamestown China Brief 24, no. 6 (March 15, 2024).
[17] Chang, Yu-Ping. “National Defense Mobilization: Toward A Clear Division of Labor between the PLA and Civilian Bureaucracies.” Jamestown China Brief 24, no. 6 (March 15, 2024).
[18] Chang, Yu-Ping. “National Defense Mobilization: Toward A Clear Division of Labor between the PLA and Civilian Bureaucracies.” Jamestown China Brief 24, no. 6 (March 15, 2024); Shu Ke (舒可). “Looking at Milita Force Building From the Perspective of Anti-Epidemic Efforts (从抗疫看民兵力量建设).” China Military Online (中国军网), July 1, 2020. https://web.archive.org/web/20231022175831/http://www.81.cn/gfbmap/content/2020-07/01/content_264897.htm.
[19] Zhou Ling (周玲). “Strengthening the Militia’s Emergency Response Capabilities (加强民兵应急应战能力建设).” China Military Online (中国军网), June 17, 2024. https://web.archive.org/web/20250703163556/http://www.81.cn/szb_223187/gfbszbxq/index.html?paperName=zggfb&paperDate=2024-06-17&paperNumber=03&articleid=933342.
[20] Zhou Ling (周玲). “Strengthening the Militia’s Emergency Response Capabilities (加强民兵应急应战能力建设).” China Military Online (中国军网), June 17, 2024. https://web.archive.org/web/20250703163556/http://www.81.cn/szb_223187/gfbszbxq/index.html?paperName=zggfb&paperDate=2024-06-17&paperNumber=03&articleid=933342.
[21] Chang, Yu-Ping. “National Defense Mobilization: Toward A Clear Division of Labor between the PLA and Civilian Bureaucracies.” Jamestown China Brief 24, no. 6 (March 15, 2024).
[22] Chang, Yu-Ping. “National Defense Mobilization: Toward A Clear Division of Labor between the PLA and Civilian Bureaucracies.” Jamestown China Brief 24, no. 6 (March 15, 2024).
[23] Zheng, Cindy, and Timothy Heath. “China’s People’s Armed Forces Departments: Developments Under Xi Jinping.” Jamestown China Brief 24, no. 9 (April 26, 2024). https://jamestown.org/program/chinas-peoples-armed-forces-departments-developments-under-xi-jinping/.
[24] Dave Aitel et al, “China’s Cyber Operations: The Rising Threat to American Security,” Margin Research, 2022, https://margin.re/chinas-cyber-operations-the-rising-threat-to-american-security/.
[25] Costello, John, and Joe McReynolds. China’s Strategic Support Force: A Force for a New Era. Washington, D.C.: National Defense University Press, 2018. https://digitalcommons.ndu.edu/china-strategic-perspectives/6/. AND https://jamestown.org/program/a-disturbance-in-the-force-the-reorganization-of-peoples-liberation-army-command-and-elimination-of-chinas-strategic-support-force/
[26] Cary, Dakota, and Kristin Del Rosso. “Sleight of Hand: How China Weaponizes Software Vulnerabilities.” Atlantic Council, September 6, 2023. https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/.
[27] See: attached data sheet.
[28] An Weiping (安卫平). “The People’s Liberation Army Must Have the Courage to Take on the National Responsibility of Guarding the ‘Internet National Gate’ (解放军要勇于承担把守‘网络国门’国家担当).” Huanqiu Net (环球网), April 17, 2017. https://web.archive.org/web/20171014001426/http://www.ce.cn/xwzx/gnsz/gdxw/201704/17/t20170417_22018228.shtml.
[29] An Weiping (安卫平). “The People’s Liberation Army Must Have the Courage to Take on the National Responsibility of Guarding the ‘Internet National Gate’ (解放军要勇于承担把守‘网络国门’国家担当).” Huanqiu Net (环球网), April 17, 2017. https://web.archive.org/web/20171014001426/http://www.ce.cn/xwzx/gnsz/gdxw/201704/17/t20170417_22018228.shtml.
[30] An Weiping (安卫平). “The People’s Liberation Army Must Have the Courage to Take on the National Responsibility of Guarding the ‘Internet National Gate’ (解放军要勇于承担把守‘网络国门’国家担当).” Huanqiu Net (环球网), April 17, 2017. https://web.archive.org/web/20171014001426/http://www.ce.cn/xwzx/gnsz/gdxw/201704/17/t20170417_22018228.shtml.
[31] An Weiping (安卫平). “The People’s Liberation Army Must Have the Courage to Take on the National Responsibility of Guarding the ‘Internet National Gate’ (解放军要勇于承担把守‘网络国门’国家担当).” Huanqiu Net (环球网), April 17, 2017. https://web.archive.org/web/20171014001426/http://www.ce.cn/xwzx/gnsz/gdxw/201704/17/t20170417_22018228.shtml.

[32] An Weiping (安卫平). “The People’s Liberation Army Must Have the Courage to Take on the National Responsibility of Guarding the ‘Internet National Gate’ (解放军要勇于承担把守‘网络国门’国家担当).” Huanqiu Net (环球网), April 17, 2017. https://web.archive.org/web/20171014001426/http://www.ce.cn/xwzx/gnsz/gdxw/201704/17/t20170417_22018228.shtml.

[33] Dongfang Hong Think Tank (东方红智库), “Research on the Mobilization of China's Reserve Forces: Taking the Construction of “Cyber Militias” as an Example,” (中国后备力量动员的研究：以”网络民兵”建设为例), National Defense Mobilization Special Issue (国防动员专刊), June 3, 2024; “To Implement Xi Jinping’s General Requirement of ‘Being Able to Withstand and Get by’ in Cyberspace, We Need to Clearly Understand the Twelve Major Cybersecurity Risks (网络空间落实习近平‘扛得住、过得去’的总要求，需看清十二大网络安全风险).” 2019 2023. https://web.archive.org/web/20250703165426/https://www.secrss.com/articles/7992; “China’s Cybersecurity Industry White Paper (中国网络安全产业白皮书).” China Academy of Information and Communications Technology (中国信息通信研究院), September 2018. https://web.archive.org/web/20250703170001/; China’s Cybersecurity Industry White Paper (中国网络安全产业白皮书).” China Academy of Information and Communications Technology (中国信息通信研究院), September 2018. https://web.archive.org/web/20250703170001/http://www.caict.ac.cn/kxyj/qwfb/bps/201809/P020181022488727633391.pdf; Antiy Labs. “General Secretary Xi Jinping Attended the National Cybersecurity and Informatization Work Conference; Antiy Immediately Organized the Study of the Important Speech of the General Secretary (习近平总书记出席全国网络安全和信息化工作会议 安天第一时间组织学习总书记重要讲话精神).” Antiy Observer (安天周观察), April 23, 2018. https://web.archive.org/web/20240616130341/https://www.antiy.cn/observe_download/observe_132.pdf; “To Implement Xi Jinping’s General Requirement of ‘Being Able to Withstand and Get by’ in Cyberspace, We Need to Clearly Understand the Twelve Major Cybersecurity Risks (网络空间落实习近平‘扛得住、过得去’的总要求，需看清十二大网络安全风险).” 2019 2023. https://web.archive.org/web/20250703165426/https://www.secrss.com/articles/7992.

[34] Dongfang Hong Think Tank (东方红智库), “Research on the Mobilization of China's Reserve Forces: Taking the Construction of “Cyber Militias” as an Example,” (中国后备力量动员的研究：以”网络民兵”建设为例), National Defense Mobilization Special Issue (国防动员专刊), June 3, 2024; “To Implement Xi Jinping’s General Requirement of ‘Being Able to Withstand and Get by’ in Cyberspace, We Need to Clearly Understand the Twelve Major Cybersecurity Risks (网络空间落实习近平‘扛得住、过得去’的总要求，需看清十二大网络安全风险).” 2019 2023. https://web.archive.org/web/20250703165426/https://www.secrss.com/articles/7992; “China’s Cybersecurity Industry White Paper (中国网络安全产业白皮书).” China Academy of Information and Communications Technology (中国信息通信研究院), September 2018. https://web.archive.org/web/20250703170001/; China’s Cybersecurity Industry White Paper (中国网络安全产业白皮书).” China Academy of Information and Communications Technology (中国信息通信研究院), September 2018. https://web.archive.org/web/20250703170001/http://www.caict.ac.cn/kxyj/qwfb/bps/201809/P020181022488727633391.pdf; Antiy Labs. “General Secretary Xi Jinping Attended the National Cybersecurity and Informatization Work Conference; Antiy Immediately Organized the Study of the Important Speech of the General Secretary (习近平总书记出席全国网络安全和信息化工作会议 安天第一时间组织学习总书记重要讲话精神).” Antiy Observer (安天周观察), April 23, 2018. https://web.archive.org/web/20240616130341/https://www.antiy.cn/observe_download/observe_132.pdf; “To Implement Xi Jinping’s General Requirement of ‘Being Able to Withstand and Get by’ in Cyberspace, We Need to Clearly Understand the Twelve Major Cybersecurity Risks (网络空间落实习近平‘扛得住、过得去’的总要求，需看清十二大网络安全风险).” 2019 2023. https://web.archive.org/web/20250703165426/https://www.secrss.com/articles/7992.

[35]Dongfang Hong Think Tank (东方红智库), “Research on the Mobilization of China's Reserve Forces: Taking the Construction of “Cyber Militias” as an Example,” (中国后备力量动员的研究：以”网络民兵”建设为例), National Defense Mobilization Special Issue (国防动员专刊), June 3, 2024; “To Implement Xi Jinping’s General Requirement of ‘Being Able to Withstand and Get by’ in Cyberspace, We Need to Clearly Understand the Twelve

Major Cybersecurity Risks (网络空间落实习近平‘扛得住、过得去’的总要求，需看清十二大网络安全风险).” 2019 2023. https://web.archive.org/web/20250703165426/https://www.secrss.com/articles/7992; “China’s Cybersecurity Industry White Paper (中国网络安全产业白皮书).” China Academy of Information and Communications Technology (中国信息通信研究院), September 2018. https://web.archive.org/web/20250703170001/; China’s Cybersecurity Industry White Paper (中国网络安全产业白皮书).” China Academy of Information and Communications Technology (中国信息通信研究院), September 2018. https://web.archive.org/web/20250703170001/http://www.caict.ac.cn/kxyj/qwfb/bps/201809/P020181022488727633391.pdf; Antiy Labs. “General Secretary Xi Jinping Attended the National Cybersecurity and Informatization Work Conference; Antiy Immediately Organized the Study of the Important Speech of the General Secretary (习近平总书记出席全国网络安全和信息化工作会议 安天第一时间组织学习总书记重要讲话精神).” Antiy Observer (安天周观察), April 23, 2018. https://web.archive.org/web/20240616130341/https://www.antiy.cn/observe_download/observe_132.pdf; “To Implement Xi Jinping’s General Requirement of ‘Being Able to Withstand and Get by’ in Cyberspace, We Need to Clearly Understand the Twelve Major Cybersecurity Risks (网络空间落实习近平‘扛得住、过得去’的总要求，需看清十二大网络安全风险).” 2019 2023.

[36] Dongfang Hong Think Tank (东方红智库), “Research on the Mobilization of China's Reserve Forces: Taking the Construction of “Cyber Militias” as an Example,” (中国后备力量动员的研究：以”网络民兵”建设为例), National Defense Mobilization Special Issue (国防动员专刊), June 3, 2024; “To Implement Xi Jinping’s General Requirement of ‘Being Able to Withstand and Get by’ in Cyberspace, We Need to Clearly Understand the Twelve Major Cybersecurity Risks (网络空间落实习近平‘扛得住、过得去’的总要求，需看清十二大网络安全风险).” 2019 2023. https://web.archive.org/web/20250703165426/https://www.secrss.com/articles/7992; “China’s Cybersecurity Industry White Paper (中国网络安全产业白皮书).” China Academy of Information and Communications Technology (中国信息通信研究院), September 2018. https://web.archive.org/web/20250703170001/; China’s Cybersecurity Industry White Paper (中国网络安全产业白皮书).” China Academy of Information and Communications Technology (中国信息通信研究院), September 2018. https://web.archive.org/web/20250703170001/http://www.caict.ac.cn/kxyj/qwfb/bps/201809/P020181022488727633391.pdf; Antiy Labs. “General Secretary Xi Jinping Attended the National Cybersecurity and Informatization Work Conference; Antiy Immediately Organized the Study of the Important Speech of the General Secretary (习近平总书记出席全国网络安全和信息化工作会议 安天第一时间组织学习总书记重要讲话精神).” Antiy Observer (安天周观察), April 23, 2018. https://web.archive.org/web/20240616130341/https://www.antiy.cn/observe_download/observe_132.pdf; “To Implement Xi Jinping’s General Requirement of ‘Being Able to Withstand and Get by’ in Cyberspace, We Need to Clearly Understand the Twelve Major Cybersecurity Risks (网络空间落实习近平‘扛得住、过得去’的总要求，需看清十二大网络安全风险).” 2019 2023.

[37] Dongfang Hong Think Tank (东方红智库), “Research on the Mobilization of China's Reserve Forces: Taking the Construction of “Cyber Militias” as an Example,” (中国后备力量动员的研究：以”网络民兵”建设为例), National Defense Mobilization Special Issue (国防动员专刊), June 3, 2024; “To Implement Xi Jinping’s General Requirement of ‘Being Able to Withstand and Get by’ in Cyberspace, We Need to Clearly Understand the Twelve Major Cybersecurity Risks (网络空间落实习近平‘扛得住、过得去’的总要求，需看清十二大网络安全风险).” 2019 2023. https://web.archive.org/web/20250703165426/https://www.secrss.com/articles/7992; “China’s Cybersecurity Industry White Paper (中国网络安全产业白皮书).” China Academy of Information and Communications Technology (中国信息通信研究院), September 2018. https://web.archive.org/web/20250703170001/; China’s Cybersecurity Industry White Paper (中国网络安全产业白皮书).” China Academy of Information and Communications Technology (中国信息通信研究院), September 2018. https://web.archive.org/web/20250703170001/http://www.caict.ac.cn/kxyj/qwfb/bps/201809/P020181022488727633391.pdf; Antiy Labs. “General Secretary Xi Jinping Attended the National Cybersecurity and Informatization Work Conference; Antiy Immediately Organized the Study of the Important Speech of the General Secretary (习近平总

书记出席全国网络安全和信息化工作会议 安天第一时间组织学习总书记重要讲话精神).” Antiy Observer (安天周观察), April 23, 2018. https://web.archive.org/web/20240616130341/https://www.antiy.cn/observe_download/observe_132.pdf; “To Implement Xi Jinping’s General Requirement of ‘Being Able to Withstand and Get by’ in Cyberspace, We Need to Clearly Understand the Twelve Major Cybersecurity Risks (网络空间落实习近平‘扛得住、过得去’的总要求，需看清十二大网络安全风险).” 2019 2023.

[38] Cybersecurity Law of the People’s Republic of China (中华人民共和国网络安全法) (2017). https://web.archive.org/web/20230319140804/https://www.miit.gov.cn/ztzl/rdzt/tdzzyyhlwsdrhfzjkjstggyhlwpt/zcfb/art/2020/art_41be9e94ecc5433899ca88a0339a38b6.html.

[39] Hou Jiabin (侯嘉斌), “Paths for Promoting Civil-Military Integration in Cyber National Defense Construction from the Draft Cybersecurity Law” (《从〈网络安全法草案〉看推动网络国防建设军民融合发展的路径》), China Information Security (《中国信息安全》), no. 11 (2015): 119–121.

[40] “Qingshuihe County 2023 Militia Organization Rectification Work Plan (清水河县 2023 年度民兵组织整顿工作方案),” 2023. http://www.huhhot.gov.cn/hhht_zfgb/qsh/qsh2023/202301/202311/t20231122_1623227.html. ; “Notice of the Qingshuihe County People’s Government and the Qingshuihe County People’s Armed Forces Department on the Issuance of the ‘Qingshuihe County 2023 Militia Organization Rectification Work Plan’ (清水河县人民政府清水河县人民武装部关于印发《清水河县 2023 年度民兵组织整顿工作方案》的通知),” December 14, 2023. http://www.qingshuihe.gov.cn/zfxxgkzl/fdzdgknr/zfwj_16168/202312/t20231214_1632233.html; Chen Yu (陈羽). “Qinghai Provincial Military District Organizes Training on Standardized Governance of Grassroots Construction (青海省军区组织基层建设规范化治理集训).” China Military Online (中国军网), August 13, 2023. https://web.archive.org/web/20240910145548/https://military.people.com.cn/n1/2024/0813/c1011-40297863.html.

[41] “Qingshuihe County 2023 Militia Organization Rectification Work Plan (清水河县 2023 年度民兵组织整顿工作方案),” 2023. http://www.huhhot.gov.cn/hhht_zfgb/qsh/qsh2023/202301/202311/t20231122_1623227.html. ; “Notice of the Qingshuihe County People’s Government and the Qingshuihe County People’s Armed Forces Department on the Issuance of the ‘Qingshuihe County 2023 Militia Organization Rectification Work Plan’ (清水河县人民政府清水河县人民武装部关于印发《清水河县 2023 年度民兵组织整顿工作方案》的通知),” December 14, 2023. http://www.qingshuihe.gov.cn/zfxxgkzl/fdzdgknr/zfwj_16168/202312/t20231214_1632233.html; Chen Yu (陈羽). “Qinghai Provincial Military District Organizes Training on Standardized Governance of Grassroots Construction (青海省军区组织基层建设规范化治理集训).” China Military Online (中国军网), August 13, 2023. https://web.archive.org/web/20240910145548/https://military.people.com.cn/n1/2024/0813/c1011-40297863.html.

[42] “Qingshuihe County 2023 Militia Organization Rectification Work Plan (清水河县 2023 年度民兵组织整顿工作方案),” 2023. http://www.huhhot.gov.cn/hhht_zfgb/qsh/qsh2023/202301/202311/t20231122_1623227.html. ; “Notice of the Qingshuihe County People’s Government and the Qingshuihe County People’s Armed Forces Department on the Issuance of the ‘Qingshuihe County 2023 Militia Organization Rectification Work Plan’ (清水河县人民政府清水河县人民武装部关于印发《清水河县 2023 年度民兵组织整顿工作方案》的通知),” December 14, 2023. http://www.qingshuihe.gov.cn/zfxxgkzl/fdzdgknr/zfwj_16168/202312/t20231214_1632233.html; Chen Yu (陈羽). “Qinghai Provincial Military District Organizes Training on Standardized Governance of Grassroots Construction (青海省军区组织基层建设规范化治理集训).” China Military Online (中国军网), August 13, 2023. https://web.archive.org/web/20240910145548/https://military.people.com.cn/n1/2024/0813/c1011-40297863.html.

[43] China Security Science Editorial Department (本刊编辑部). “Selected Security Proposals for the Two Session (两会安全提案选登).” China Information Security (中国信息安全), no. 4 (2018): 85–90; Hou Jianbin (侯嘉斌). “The Path to Promote the Development of Military-Civilian Fusion in Cyber Defense Construction from the Perspective of the ‘Draft Cybersecurity Law’ (从《网络安全法草案》看推动网络国防建设军民融合发展的路径).” China Information Security (中国信息安全), no. 11 (2015): 119–21.

[44] China Security Science Editorial Department (本刊编辑部). “Selected Security Proposals for the Two Session (两会安全提案选登).” China Information Security (中国信息安全), no. 4 (2018): 85–90.

[45] Hou Jianbin (侯嘉斌). “The Path to Promote the Development of Military-Civilian Fusion in Cyber Defense Construction from the Perspective of the ‘Draft Cybersecurity Law’ (从《网络安全法草案》看推动网络国防建设军民融合发展的路径).” China Information Security (中国信息安全), no. 11 (2015): 119–21.
[46] Hou Jianbin (侯嘉斌). “The Path to Promote the Development of Military-Civilian Fusion in Cyber Defense Construction from the Perspective of the ‘Draft Cybersecurity Law’ (从《网络安全法草案》看推动网络国防建设军民融合发展的路径).” China Information Security (中国信息安全), no. 11 (2015): 119–21.
[47] Xiao Jing (晓景). “Strengthen Military-Civilian Fusion in the Field of Cyber Security and Give Full Play to the Strategic Effect of High-Quality Resources (加强网络安全领域军民融合,发挥优质资源的战略效应).” China Information Security (中国信息安全), March 15, 2016, 44–45.
[48] Gu Gang (谷钢), A Brief Discussion on the Construction of Combat Capabilities of College Militia Information Units (略论高校民兵信息分队作战能力建设), Central South University (中南大学), Master’s Thesis, 2010.
[49] Xiao Jing (晓景). “Strengthen Military-Civilian Fusion in the Field of Cyber Security and Give Full Play to the Strategic Effect of High-Quality Resources (加强网络安全领域军民融合,发挥优质资源的战略效应).” China Information Security (中国信息安全), March 15, 2016, 44–45.
[50] An Weiping (安卫平). “The People’s Liberation Army Must Have the Courage to Take on the National Responsibility of Guarding the ‘Internet National Gate’ (解放军要勇于承担把守‘网络国门’国家担当).” Huanqiu Net (环球网), April 17, 2017.
https://web.archive.org/web/20171014001426/http://www.ce.cn/xwzx/gnsz/gdxw/201704/17/t20170417_22018228.shtml.
[51] Yang Jianjun (杨建军), Zhang Ming (张明), and Zhu Feng (朱峰). “Sharpen the Ability to Win the War (向战务战砥砺打赢本领),” 2023.
https://web.archive.org/web/20250704001858/http://www.81.cn/rmjz_203219/zgmb/2023nd6q/zxzc_245365/16243723.html; Political Work Bureau of Henan Provincial Military Region (河南省军区政治工作局). “The Military and Local Governments Work Together to Ensure the Final Implementation of the Militia’s Political Work (军地合力抓好民兵政治工作末端落实).” China Military Online (中国军网), 2023.
https://web.archive.org/web/20241014221150/http://www.81.cn/rmjz_203219/zgmb/2023n10y/gzyj_246619/16271051.html.
[52] Liu Yu (刘宇). “Accurately Match Potential Data with Battlefield Needs (让潜力数据精准对接战场需求).” China Military Online (中国军网), June 24, 2020.
https://web.archive.org/web/20250704004634/http://www.81.cn/gfbmap/content/2020-06/24/content_264502.htm.
[53] Liu Yu (刘宇). “Accurately Match Potential Data with Battlefield Needs (让潜力数据精准对接战场需求).” China Military Online (中国军网), June 24, 2020.
[54] Zhou Ling (周玲). “Strengthening the Militia’s Emergency Response Capabilities (加强民兵应急应战能力建设).” China Military Online (中国军网), June 17, 2024.
https://web.archive.org/web/20250703163556/http://www.81.cn/szb_223187/gfbszbxq/index.html?paperName=zggfb&paperDate=2024-06-17&paperNumber=03&articleid=933342.
[55] Shu Ke (舒可). “Looking at Milita Force Building From the Perspective of Anti-Epidemic Efforts (从抗疫看民兵力量建设).” China Military Online (中国军网), July 1, 2020.
https://web.archive.org/web/20231022175831/http://www.81.cn/gfbmap/content/2020-07/01/content_264897.htm.
[56] Shu Ke (舒可). “Looking at Milita Force Building From the Perspective of Anti-Epidemic Efforts (从抗疫看民兵力量建设).” China Military Online (中国军网), July 1, 2020.
https://web.archive.org/web/20231022175831/http://www.81.cn/gfbmap/content/2020-07/01/content_264897.htm.
[57] Zhou Ling (周玲). “Strengthening the Militia’s Emergency Response Capabilities (加强民兵应急应战能力建设).” China Military Online (中国军网), June 17, 2024.
https://web.archive.org/web/20250703163556/http://www.81.cn/szb_223187/gfbszbxq/index.html?paperName=zggfb&paperDate=2024-06-17&paperNumber=03&articleid=933342.
[58] https://amti.csis.org/directing-chinas-little-blue-men-uncovering-the-maritime-militia-command-structure/ AND Zhou Ling (周玲). “Strengthening the Militia’s Emergency Response Capabilities (加强民兵应急应战能力建设).” China Military Online (中国军网), June 17, 2024.
https://web.archive.org/web/20250703163556/http://www.81.cn/szb_223187/gfbszbxq/index.html?paperName=zggfb&paperDate=2024-06-17&paperNumber=03&articleid=933342.

[59] https://amti.csis.org/directing-chinas-little-blue-men-uncovering-the-maritime-militia-command-structure/ AND Zhou Ling (周玲). "Strengthening the Militia's Emergency Response Capabilities (加强民兵应急应战能力建设)." China Military Online (中国军网), June 17, 2024. https://web.archive.org/web/20250703163556/http://www.81.cn/szb_223187/gfbszbxq/index.html?paperName=zggfb&paperDate=2024-06-17&paperNumber=03&articleid=933342.

[60] Xiao Tianliang (ed.). In Their Own Words: The Science of Military Strategy. Beijing: PLA Academy of Military Sciences (Translated by the China Aerospace Studies Institute, 2020. pp. 436-450.

[61] Zhou Ling (周玲). "Strengthening the Militia's Emergency Response Capabilities (加强民兵应急应战能力建设)." China Military Online (中国军网), June 17, 2024. https://web.archive.org/web/20250703163556/http://www.81.cn/szb_223187/gfbszbxq/index.html?paperName=zggfb&paperDate=2024-06-17&paperNumber=03&articleid=933342.

[62] Gu Gang (谷钢), A Brief Discussion on the Construction of Combat Capabilities of College Militia Information Units (略论高校民兵信息分队作战能力建设), Central South University (中南大学), Master's Thesis, 2010.

[63] Gu Gang (谷钢), A Brief Discussion on the Construction of Combat Capabilities of College Militia Information Units (略论高校民兵信息分队作战能力建设), Central South University (中南大学), Master's Thesis, 2010.

[64] Gu Gang (谷钢), A Brief Discussion on the Construction of Combat Capabilities of College Militia Information Units (略论高校民兵信息分队作战能力建设), Central South University (中南大学), Master's Thesis, 2010.

[65] Gu Gang (谷钢), A Brief Discussion on the Construction of Combat Capabilities of College Militia Information Units (略论高校民兵信息分队作战能力建设), Central South University (中南大学), Master's Thesis, 2010.

[66] Gu Gang (谷钢), A Brief Discussion on the Construction of Combat Capabilities of College Militia Information Units (略论高校民兵信息分队作战能力建设), Central South University (中南大学), Master's Thesis, 2010.

[67] Gu Gang (谷钢), A Brief Discussion on the Construction of Combat Capabilities of College Militia Information Units (略论高校民兵信息分队作战能力建设), Central South University (中南大学), Master's Thesis, 2010. AND Xu Yonghan (徐永汉), and Zheng Ning (郑宁). "Mission Construction and Application of Militia Cyber Warfare Team (民兵网络战分队的任务建设与运用)." National Defense (国防), no. 8 (December 2006): 39–40; Zhou Ling (周玲). "Strengthening the Militia's Emergency Response Capabilities (加强民兵应急应战能力建设)." China Military Online (中国军网), June 17, 2024. https://web.archive.org/web/20250703163556/http://www.81.cn/szb_223187/gfbszbxq/index.html?paperName=zggfb&paperDate=2024-06-17&paperNumber=03&articleid=933342.

[68] Gu Gang (谷钢), A Brief Discussion on the Construction of Combat Capabilities of College Militia Information Units (略论高校民兵信息分队作战能力建设), Central South University (中南大学), Master's Thesis, 2010; Zhou Ling (周玲). "Strengthening the Militia's Emergency Response Capabilities (加强民兵应急应战能力建设)." China Military Online (中国军网), June 17, 2024. https://web.archive.org/web/20250703163556/http://www.81.cn/szb_223187/gfbszbxq/index.html?paperName=zggfb&paperDate=2024-06-17&paperNumber=03&articleid=933342.

[69] Gu Gang (谷钢), A Brief Discussion on the Construction of Combat Capabilities of College Militia Information Units (略论高校民兵信息分队作战能力建设), Central South University (中南大学), Master's Thesis, 2010.

[70] Yuan Yi 袁艺 To build a strong cyber power, we must plan to win the cyber war 建设网络强国必须谋划打赢网络战争

[71] Gu Gang (谷钢), A Brief Discussion on the Construction of Combat Capabilities of College Militia Information Units (略论高校民兵信息分队作战能力建设), Central South University (中南大学), Master's Thesis, 2010.

[72] Yuan Yi 袁艺 To build a strong cyber power, we must plan to win the cyber war 建设网络强国必须谋划打赢网络战争

[73] Dongfang Hong Think Tank (东方红智库), "Research on the Mobilization of China's Reserve Forces: Taking the Construction of "Cyber Militias" as an Example," (中国后备力量动员的研究：以"网络民兵"建设为例), National Defense Mobilization Special Issue (国防动员专刊), June 3, 2024.

[74] Yuan Yi 袁艺 To build a strong cyber power, we must plan to win the cyber war 建设网络强国必须谋划打赢网络战争

[75] Liu Weihua (刘卫华), Xu Qiang (徐强), and Zhang Ning (张宁). "How Do Military Branches and Militia Professional Units Connect? (军种主建，民兵专业分队如何对接？)." China National Defense News (中国国防

报), January 27, 2016. https://web.archive.org/web/20210418123038/http://www.81.cn/mb/2016-01/27/content_7071697.htm; Jian Tianbo (姜天波). “Strive to Achieve New Breakthroughs in Militia Construction in the New Era (努力谋求新时代民兵建设实现新突破).” China Military Online (中国军网), 2023. https://web.archive.org/web/20241014222726/http://www.81.cn/rmjz_203219/zgmb/2023nd9q/dysjhgf_246488/16258411.html.; Yang Jianjun (杨建军), Zhang Ming (张明), and Zhu Feng (朱峰). “Sharpen the Ability to Win the War (向战务战砥砺打赢本领),” 2023. https://web.archive.org/web/20250704001858/http://www.81.cn/rmjz_203219/zgmb/2023nd6q/zxzc_245365/16243723.html.

[76] Liu Weihua (刘卫华), Xu Qiang (徐强), and Zhang Ning (张宁). “How Do Military Branches and Militia Professional Units Connect? (军种主建，民兵专业分队如何对接？).” China National Defense News (中国国防报), January 27, 2016. https://web.archive.org/web/20210418123038/http://www.81.cn/mb/2016-01/27/content_7071697.htm; Jian Tianbo (姜天波). “Strive to Achieve New Breakthroughs in Militia Construction in the New Era (努力谋求新时代民兵建设实现新突破).” China Military Online (中国军网), 2023. https://web.archive.org/web/20241014222726/http://www.81.cn/rmjz_203219/zgmb/2023nd9q/dysjhgf_246488/16258411.html. ; Yang Jianjun (杨建军), Zhang Ming (张明), and Zhu Feng (朱峰). “Sharpen the Ability to Win the War (向战务战砥砺打赢本领),” 2023. https://web.archive.org/web/20250704001858/http://www.81.cn/rmjz_203219/zgmb/2023nd6q/zxzc_245365/16243723.html.

[77] Zhou Ling (周玲). “Strengthening the Militia’s Emergency Response Capabilities (加强民兵应急应战能力建设).” China Military Online (中国军网), June 17, 2024. https://web.archive.org/web/20250703163556/http://www.81.cn/szb_223187/gfbszbxq/index.html?paperName=zggfb&paperDate=2024-06-17&paperNumber=03&articleid=933342.

[78] Lu Shijun (吕世军), Yang Yajun (杨亚军), and Wang Lingshuo (王凌硕). “Qinghai Provincial Military District Organizes Training on Standardized Governance of Grassroots Force Construction (青海省军区组织基层建设规范化治理集训).” China National Defense News (中国国防报), August 13, 2024. https://web.archive.org/web/20250413070809/https://www.mod.gov.cn/gfbw/gfdy/zzdy/16330879.html.

[79] Song Hui (宋辉). “Training the Target Range Construction by the Militiaman Network Attack and Defense for the Security Problem (论民兵网络攻防训练靶场建设的安全问题).” Science Technology and Engineering (科学技术与工程), 2008; “The Live-Fire Shooting Training of Military Trainees Was Successfully Completed (军训师实弹射击训练圆满结束).” Chang’an University Military Training Division Political Department (长安大学军训师政治部), 2012. https://web.archive.org/web/20250704020330/https://rmwzb.chd.edu.cn/_upload/article/files/e3/45/8376fcd24eca868b9654f141067f/fdf6819a-ec5e-4a80-bfde-34a26152a88e.pdf.

[80] “The Live-Fire Shooting Training of Military Trainees Was Successfully Completed (军训师实弹射击训练圆满结束).” Chang’an University Military Training Division Political Department (长安大学军训师政治部), 2012. https://web.archive.org/web/20250704020330/https://rmwzb.chd.edu.cn/_upload/article/files/e3/45/8376fcd24eca868b9654f141067f/fdf6819a-ec5e-4a80-bfde-34a26152a88e.pdf.

[81] “The Live-Fire Shooting Training of Military Trainees Was Successfully Completed (军训师实弹射击训练圆满结束).” Chang’an University Military Training Division Political Department (长安大学军训师政治部), 2012. https://web.archive.org/web/20250704020330/https://rmwzb.chd.edu.cn/_upload/article/files/e3/45/8376fcd24eca868b9654f141067f/fdf6819a-ec5e-4a80-bfde-34a26152a88e.pdf.

[82] Gu Gang (谷钢), A Brief Discussion on the Construction of Combat Capabilities of College Militia Information Units (略论高校民兵信息分队作战能力建设), Central South University (中南大学), Master’s Thesis, 2010.

[83] Dakota Cary. “Downrange: A Survey of China’s Cyber Ranges.” Center for Security and Emerging Technology, September 2022. https://cset.georgetown.edu/publication/downrange-a-survey-of-chinas-cyber-ranges/.

[84] Song Hui (宋辉). “Training the Target Range Construction by the Militiaman Network Attack and Defense for the Security Problem (论民兵网络攻防训练靶场建设的安全问题).” Science Technology and Engineering (科学技术与工程), 2008.

[85] Song Hui (宋辉). “Training the Target Range Construction by the Militiaman Network Attack and Defense for the Security Problem (论民兵网络攻防训练靶场建设的安全问题).” Science Technology and Engineering (科学技术与工程), 2008.

[86] Long Libin (龙礼彬). “The Network Operations and Maintenance Team Opens Up the Information Link (网络运维分队打通信息链路).” China Military Online (中国军网), May 11, 2022. https://web.archive.org/web/20250704020800/http://www.81.cn/gfbmap/content/2022-05/17/content_315696.htm; Wang Jin (王进), Zhu Feng (朱峰), and Li Hongfei (李弘非). “Building a ‘Big Stage’ for Talent Cultivation - Record of the Joint Training and Cultivation of Talents Implemented by the Jiangsu Provincial Military Region Relying on Military and Local Resources (搭建人才培养‘大舞台’——江苏省军区依托军地资源实施人才联训联育工作纪实).” China Military Online (中国军网), 2023. https://web.archive.org/web/20241014222619/http://www.81.cn/rmjz_203219/zgmb/2023nd4q/xxgcesd/16225105.html.

[87] Wang Xiaoming (王晓明), ed. Introduction to Cyberspace Operations (网络空间作战概论). PLA National Defense Information Academy (中国人民解放军国防信息学院), 2017. pg. 297

[88] Xiao Tianliang (ed.). In Their Own Words: The Science of Military Strategy. Beijing: PLA Academy of Military Sciences (Translated by the China Aerospace Studies Institute, 2020. pg. 208

[89] Gu Gang (谷钢), A Brief Discussion on the Construction of Combat Capabilities of College Militia Information Units (略论高校民兵信息分队作战能力建设), Central South University (中南大学), Master’s Thesis, 2010.

[90] John Chen, Joe McReynolds, and Kieran Green, “The PLA Strategic Support Force: A ‘Joint’ Force for Information Operations,” in The PLA Beyond Borders: Chinese Military Operations in Regional and Global Context, Joel Wuthnow et al (ed.), Washington D.C., 2021.

[91] Shu Ke (舒可). “Looking at Milita Force Building From the Perspective of Anti-Epidemic Efforts (从抗疫看民兵力量建设).” China Military Online (中国军网), July 1, 2020. https://web.archive.org/web/20231022175831/http://www.81.cn/gfbmap/content/2020-07/01/content_264897.htm.

[92] Shu Ke (舒可). “Looking at Milita Force Building From the Perspective of Anti-Epidemic Efforts (从抗疫看民兵力量建设).” China Military Online (中国军网), July 1, 2020. https://web.archive.org/web/20231022175831/http://www.81.cn/gfbmap/content/2020-07/01/content_264897.htm.

[93] “The Milita Showed Their Style During the Inspection and Promoted Training to Forge the Military Spirit (民兵点验展风采 以验促练铸军魂).”Sohu, May 22, 2024. https://web.archive.org/web/20250704022046/https://www.sohu.com/a/780736245_121106854.

[94] “The Milita Showed Their Style During the Inspection and Promoted Training to Forge the Military Spirit (民兵点验展风采 以验促练铸军魂).”Sohu, May 22, 2024.

[95] “The District People’s Armed Forces Department Investigated the Construction of the New-Type Enterprise at Xiaoguwei Street (区人武部调研小谷围街新质企业民兵分队建设).” Guangzhou Panyu District People’s Government (广州市番禺区人民政府), August 7, 2024. https://web.archive.org/web/20250704022720/https://www.panyu.gov.cn/jgzy/zzfjdbsc/fzqrmzfxgwjdbsc/xgwgkml/zwdt/content/post_9803667.html.

[96] Dongfang Hong Think Tank (东方红智库), “Research on the Mobilization of China's Reserve Forces: Taking the Construction of “Cyber Militias” as an Example,” (中国后备力量动员的研究：以”网络民兵”建设为例), National Defense Mobilization Special Issue (国防动员专刊), June 3, 2024.

[97] Citation Available Upon Request.

[98] Citation Available Upon Request.

[99] Dongfang Hong Think Tank (东方红智库), “Research on the Mobilization of China's Reserve Forces: Taking the Construction of “Cyber Militias” as an Example,” (中国后备力量动员的研究：以”网络民兵”建设为例), National Defense Mobilization Special Issue (国防动员专刊), June 3, 2024.

[100] Shu Ke (舒可). “Looking at Milita Force Building From the Perspective of Anti-Epidemic Efforts (从抗疫看民兵力量建设).” China Military Online (中国军网), July 1, 2020. https://web.archive.org/web/20231022175831/http://www.81.cn/gfbmap/content/2020-07/01/content_264897.htm.

[101] Shu Ke (舒可). “Looking at Milita Force Building From the Perspective of Anti-Epidemic Efforts (从抗疫看民兵力量建设).” China Military Online (中国军网), July 1, 2020. https://web.archive.org/web/20231022175831/http://www.81.cn/gfbmap/content/2020-07/01/content_264897.htm.

[102] Shu Ke (舒可). “Looking at Milita Force Building From the Perspective of Anti-Epidemic Efforts (从抗疫看民兵力量建设).” China Military Online (中国军网), July 1, 2020. https://web.archive.org/web/20231022175831/http://www.81.cn/gfbmap/content/2020-07/01/content_264897.htm.

[103] Liu Yangyue (刘杨钺). "On the In-Depth Development of Military-Civilian Integration of Cyber Security in the Context of a Strong Cyber Province (论网络强省背景下的网络安全军民融合深度发展)." Journal of Huaihua University (怀化学院学报), 2018.
[104] Cui Guangyao (崔光耀). "Current Security Hotspots From the Perspective of the Two Sessions (从两会声音看当前安全热点)." China Information Security (中国信息安全), no. 4 (2018): 56–57.
[105] Guo Yuandan (郭媛丹). "Members of the National Committee of the Chinese People's Political Consultative Conference Suggested Improving the Coordinated Assessment and Command Mechanism for Major Social Risks and Called for the Establishment of a 'Cyber Security Militia' System (全国政协委员建议完善重大社会风险协同研判指挥机制 呼吁建设'网信民兵'体系)." Global Times (环球时报), May 23, 2020. https://web.archive.org/web/20250704150815/https://lianghui.huanqiu.com/article/9CaKrnKr620?from=timeline&isappinstalled=0.
[106] Cui Guangyao (崔光耀). "Current Security Hotspots From the Perspective of the Two Sessions (从两会声音看当前安全热点)." China Information Security (中国信息安全), no. 4 (2018): 56–57.
[107] Cui Guangyao (崔光耀). "Current Security Hotspots From the Perspective of the Two Sessions (从两会声音看当前安全热点)." China Information Security (中国信息安全), no. 4 (2018): 56–57.
[108] Camille Boullenois, Agatha Kratz, and Laura Gormley. "Spread Thin: China's Science and Technology Spending in an Economic Slowdown," Rhodium Group, December 15, 2023. https://rhg.com/research/spread-thin-chinas-science-and-technology-spending-in-an-economic-slowdown/.
[109] Citation Available Upon Request.
[110] Citation Available Upon Request.
[111] Citation Available Upon Request.
[112] Zhou Ling (周玲). "Strengthening the Militia's Emergency Response Capabilities (加强民兵应急应战能力建设)." China Military Online (中国军网), June 17, 2024. https://web.archive.org/web/20250703163556/http://www.81.cn/szb_223187/gfbszbxq/index.html?paperName=zggfb&paperDate=2024-06-17&paperNumber=03&articleid=933342.
[113] Wang Tao (吴涛). "A Meritorious Official Married a Meritorious Official. The Good News of Meritorious Service Testifies to the Story of Sichuan Girl Zhang Hui and the Military Camp, University and Yibin. (功臣嫁给功臣 立功喜报作证川妹子张慧与军营、大学、宜宾的故事)," March 1, 2022. http://tyjrswj.yibin.gov.cn.http.80.3422207674.ipv6.whsw.edu.cn/xwzx_87/sydt/202203/t20220302_1706486.html.
[114] Dongfang Hong Think Tank (东方红智库), "Research on the Mobilization of China's Reserve Forces: Taking the Construction of "Cyber Militias" as an Example," (中国后备力量动员的研究：以"网络民兵"建设为例), National Defense Mobilization Special Issue (国防动员专刊), June 3, 2024.
[115] Dongfang Hong Think Tank (东方红智库), "Research on the Mobilization of China's Reserve Forces: Taking the Construction of "Cyber Militias" as an Example," (中国后备力量动员的研究：以"网络民兵"建设为例), National Defense Mobilization Special Issue (国防动员专刊), June 3, 2024.
[116] Global Communications (环球通信). "Central State-Owned Enterprises Have Set Up Armed Departments One After Another, and the Operators' Armed Departments Are Here! (央国企纷纷设立武装部，运营商武装部来了！)." November 2, 2023. https://web.archive.org/web/20250704024017/https://www.163.com/dy/article/IIIGOQTI0511DFSC.html; Gu Gang (谷钢), A Brief Discussion on the Construction of Combat Capabilities of College Militia Information Units (略论高校民兵信息分队作战能力建设), Central South University (中南大学), Master's Thesis, 2010.
[117] Xu Yonghan (徐永汉), and Zheng Ning (郑宁). "Mission Construction and Application of Militia Cyber Warfare Team (民兵网络战分队的任务建设与运用)." National Defense (国防), no. 8 (December 2006): 39–40
[118] See: attached data set; "The District People's Armed Forces Department Investigated the Construction of the New-Type Enterprise at Xiaoguwei Street (区人武部调研小谷围街新质企业民兵分队建设)." Guangzhou Panyu District People's Government (广州市番禺区人民政府), August 7, 2024. https://web.archive.org/web/20250704022720/https://www.panyu.gov.cn/jgzy/zzfjdbsc/fzqrmzfxgwjdbsc/xgwgkml/zwdt/content/post_9803667.html.
[119] China's Cybersecurity Industry White Paper (中国网络安全产业白皮书)." China Academy of Information and Communications Technology (中国信息通信研究院), September 2018.

https://web.archive.org/web/20250703170001/http://www.caict.ac.cn/kxyj/qwfb/bps/201809/P020181022488727633391.pdf
[120] See: attached data set
[121] See: attached data set
[122] Zhou Ling (周玲). “Strengthening the Militia’s Emergency Response Capabilities (加强民兵应急应战能力建设).” China Military Online (中国军网), June 17, 2024. https://web.archive.org/web/20250703163556/http://www.81.cn/szb_223187/gfbszbxq/index.html?paperName=zggfb&paperDate=2024-06-17&paperNumber=03&articleid=933342.
[123] Zhou Ling (周玲). “Strengthening the Militia’s Emergency Response Capabilities (加强民兵应急应战能力建设).” China Military Online (中国军网), June 17, 2024. https://web.archive.org/web/20250703163556/http://www.81.cn/szb_223187/gfbszbxq/index.html?paperName=zggfb&paperDate=2024-06-17&paperNumber=03&articleid=933342.
[124] Hantai District 2018 Basic Militia Organization Task List (Professional Force) (汉台区 2018 年基干民兵编组任务表（专业力量）), Full text available upon request.
[125] Hantai District 2017 Emergency Force Task Allocation Table (汉台区 2017 年基干民兵编组任务分配表), Full text available upon request.
[126] See: attached data sheet.
[127] See: attached data sheet.
[128] Zhou Ling (周玲). “Strengthening the Militia’s Emergency Response Capabilities (加强民兵应急应战能力建设).” China Military Online (中国军网), June 17, 2024. https://web.archive.org/web/20250703163556/http://www.81.cn/szb_223187/gfbszbxq/index.html?paperName=zggfb&paperDate=2024-06-17&paperNumber=03&articleid=933342.
[129] Zhou Ling (周玲). “Strengthening the Militia’s Emergency Response Capabilities (加强民兵应急应战能力建设).” China Military Online (中国军网), June 17, 2024. https://web.archive.org/web/20250703163556/http://www.81.cn/szb_223187/gfbszbxq/index.html?paperName=zggfb&paperDate=2024-06-17&paperNumber=03&articleid=933342.
[130] Dongfang Hong Think Tank (东方红智库), “Research on the Mobilization of China's Reserve Forces: Taking the Construction of “Cyber Militias” as an Example,” (中国后备力量动员的研究：以”网络民兵”建设为例), National Defense Mobilization Special Issue (国防动员专刊), June 3, 2024.
[131] Dongfang Hong Think Tank (东方红智库), “Research on the Mobilization of China's Reserve Forces: Taking the Construction of “Cyber Militias” as an Example,” (中国后备力量动员的研究：以”网络民兵”建设为例), National Defense Mobilization Special Issue (国防动员专刊), June 3, 2024. Robert Sheldon and Joe McReynolds, “Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias,” in China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York: Oxford University Press, 2015), 188–222.
[132] Xu Yonghan (徐永汉), and Zheng Ning (郑宁). “Mission Construction and Application of Militia Cyber Warfare Team (民兵网络战分队的任务建设与运用).” National Defense (国防), no. 8 (December 2006): 39–40; Dongfang Hong Think Tank (东方红智库), “Research on the Mobilization of China's Reserve Forces: Taking the Construction of “Cyber Militias” as an Example,” (中国后备力量动员的研究：以”网络民兵”建设为例), National Defense Mobilization Special Issue (国防动员专刊), June 3, 2024.
[133] Dongfang Hong Think Tank (东方红智库), “Research on the Mobilization of China's Reserve Forces: Taking the Construction of “Cyber Militias” as an Example,” (中国后备力量动员的研究：以”网络民兵”建设为例), National Defense Mobilization Special Issue (国防动员专刊), June 3, 2024.
[134] Xu Yonghan (徐永汉), and Zheng Ning (郑宁). “Mission Construction and Application of Militia Cyber Warfare Team (民兵网络战分队的任务建设与运用).” National Defense (国防), no. 8 (December 2006): 39–40; Hong Think Tank (东方红智库), “Research on the Mobilization of China's Reserve Forces: Taking the Construction of “Cyber Militias” as an Example,” (中国后备力量动员的研究：以”网络民兵”建设为例), National Defense Mobilization Special Issue (国防动员专刊), June 3, 2024.
[135] Jiang Yanchuan (蒋研川) and Zhao Lin (赵林). “Our School Participated in the 2020 Basic Militia Inspection of the Shapingba District(我校参加沙坪坝区 2020 基干民兵点验).” CQU News (重大新闻网), June 12, 2020. https://web.archive.org/web/20250704025350/https://news.cqu.edu.cn/archives/news2/content/2020/06/12/3d810f84

ca9e37b83ea62c09da7c919d1113b139.html; Jixi No. 18 Middle School Held the Founding Meeting of the Basic Militia Network Protection Team (鸡西市第十八中学召开基干民兵网络防护分队成立大会), https://edu.jixi.gov.cn/Article/21852.html.

[136] Baidu News. "Jiuxianqiao Subdistrict Holds Flag-Raising Ceremony for the Cyber Security Militia (酒仙桥街道举行网络安全民兵分队授旗仪式)." December 16, 2020. https://web.archive.org/web/20250704030035/https://wappass.baidu.com/static/captcha/tuxing.html?ak=572be823e2f50ea759a616c060d6b9f1&backurl=https%3A%2F%2Fmbd.baidu.com%2Fnewspage%2Fdata%2Flandingsuper%3Fid%3D1686222420624511090%26wfr%3Dspider%26for%3Dpc%26third%3Dbaijiahao%26baijiahao_id%3D1686222420624511090%26c_source%3Dkunlun%26c_score%3D0.999000&timestamp=1751597946&signature=b26d914fdc08d0d2789133568937af1c; Xu Yonghan (徐永汉), and Zheng Ning (郑宁). "Mission Construction and Application of Militia Cyber Warfare Team (民兵网络战分队的任务建设与运用)." National Defense (国防), no. 8 (December 2006): 39–40; Banyuetan (半月谈网). "360 Group's Cyber Security Militia Team Guards the 'Fifth Dimension' (360 集团网络安全民兵分队守护'第五维空间')." May 18, 2021. https://web.archive.org/web/20250704030657/http://www.banyuetan.org/hzjh/detail/20210518/1000200033138981621298012850799816_1.html.

[137] "Decision of the CCP Central Committee on Several Major Issues Concerning Upholding and Improving the Socialist System with Chinese Characteristics and Promoting the Modernization of the National Governance System and Governance Capacity (中共中央关于坚持和完善中国特色社会主义制度 推进国家治理体系和治理能力现代化若干重大问题的决定)." Fourth Plenary Session of the 19th Central Committee of the Communist Party of China (中国共产党第十九届中央委员会第四次全体会议), November 5, 2019. https://web.archive.org/web/20200310064934/https://www.gov.cn/zhengce/2019-11/05/content_5449023.htm; Niu Baoming (牛保明). "Our School Carried Out Military Training Activities for the Network Attack and Defense Militia Team (我校开展网络攻防民兵分队军事训练活动)." Yan'an University Party Committee Propaganda Department (延安大学党委宣传部), May 15, 2018. https://web.archive.org/web/20250124150821/https://www.yau.edu.cn/info/1120/330617.htm.

[138] Zhou Ling (周玲). "Strengthening the Militia's Emergency Response Capabilities (加强民兵应急应战能力建设)." China Military Online (中国军网), June 17, 2024. https://web.archive.org/web/20250703163556/http://www.81.cn/szb_223187/gfbszbxq/index.html?paperName=zggfb&paperDate=2024-06-17&paperNumber=03&articleid=933342.

[139] Gu Gang (谷钢), A Brief Discussion on the Construction of Combat Capabilities of College Militia Information Units (略论高校民兵信息分队作战能力建设), Central South University (中南大学), Master's Thesis, 2010.

[140] "Our School Carried Out Military Training Activities for the Network Attack and Defense Militia Team (我校开展网络攻防民兵分队军事训练活动)." Yan'an University Party Committee Propaganda Department (延安大学党委宣传部), May 15, 2018. https://web.archive.org/web/20250124150821/https://www.yau.edu.cn/info/1120/330617.htm Zhou Ling (周玲). "Strengthening the Militia's Emergency Response Capabilities (加强民兵应急应战能力建设)." China Military Online (中国军网), June 17, 2024. https://web.archive.org/web/20250703163556/http://www.81.cn/szb_223187/gfbszbxq/index.html?paperName=zggfb&paperDate=2024-06-17&paperNumber=03&articleid=933342.

[141] Citation Available Upon Request.

[142] Dongfang Hong Think Tank (东方红智库), "Research on the Mobilization of China's Reserve Forces: Taking the Construction of "Cyber Militias" as an Example," (中国后备力量动员的研究：以"网络民兵"建设为例), National Defense Mobilization Special Issue (国防动员专刊), June 3, 2024.

[143] Xu Yonghan (徐永汉), and Zheng Ning (郑宁). "Mission Construction and Application of Militia Cyber Warfare Team (民兵网络战分队的任务建设与运用)." National Defense (国防), no. 8 (December 2006): 39–40

[144] Xu Yonghan (徐永汉), and Zheng Ning (郑宁). "Mission Construction and Application of Militia Cyber Warfare Team (民兵网络战分队的任务建设与运用)." National Defense (国防), no. 8 (December 2006): 39–40

[145] Dongfang Hong Think Tank (东方红智库), "Research on the Mobilization of China's Reserve Forces: Taking the Construction of "Cyber Militias" as an Example," (中国后备力量动员的研究：以"网络民兵"建设为例), National Defense Mobilization Special Issue (国防动员专刊), June 3, 2024.

[146] Dongfang Hong Think Tank (东方红智库), “Research on the Mobilization of China's Reserve Forces: Taking the Construction of “Cyber Militias” as an Example,” (中国后备力量动员的研究：以”网络民兵”建设为例), National Defense Mobilization Special Issue (国防动员专刊), June 3, 2024.
[147] Dongfang Hong Think Tank (东方红智库), “Research on the Mobilization of China's Reserve Forces: Taking the Construction of “Cyber Militias” as an Example,” (中国后备力量动员的研究：以”网络民兵”建设为例), National Defense Mobilization Special Issue (国防动员专刊), June 3, 2024.
[148] See: attached data set.
[149] Gu Gang (谷钢), A Brief Discussion on the Construction of Combat Capabilities of College Militia Information Units (略论高校民兵信息分队作战能力建设), Central South University (中南大学), Master’s Thesis, 2010.
[150] Citation Available Upon Request.
[151] Shu Ke (舒可). “Looking at Milita Force Building From the Perspective of Anti-Epidemic Efforts (从抗疫看民兵力量建设).” China Military Online (中国军网), July 1, 2020. https://web.archive.org/web/20231022175831/http://www.81.cn/gfbmap/content/2020-07/01/content_264897.htm.
[152] Shu Ke (舒可). “Looking at Milita Force Building From the Perspective of Anti-Epidemic Efforts (从抗疫看民兵力量建设).” China Military Online (中国军网), July 1, 2020. https://web.archive.org/web/20231022175831/http://www.81.cn/gfbmap/content/2020-07/01/content_264897.htm.
[153] Gu Gang (谷钢), A Brief Discussion on the Construction of Combat Capabilities of College Militia Information Units (略论高校民兵信息分队作战能力建设), Central South University (中南大学), Master’s Thesis, 2010.
[154] Jin Ling (金灵) ed. “Hunan Holds a Meeting to Inspect the Basic Militia Network Squad (湖南召开基干民兵网络分队点验大会).” Huasheng Online (华声在线), June 8, 2018. https://web.archive.org/web/20180610200214/https://hunan.voc.com.cn/article/201806/201806081020423835.html.html AND https://www.yau.edu.cn/info/1121/27339.htm; Xu Yonghan (徐永汉), and Zheng Ning (郑宁). “Mission Construction and Application of Militia Cyber Warfare Team (民兵网络战分队的任务建设与运用).” National Defense (国防), no. 8 (December 2006): 39–40.
[155] Xiao Xinguang (肖新光). “Improve Cybersecurity Emergency Response Capabilities to Address Major Social Emergencies (提升网络安全应急能力，应对社会重大突发事件).” China Information Security (中国信息安全), no. 6 (2020): 30–31; Xiao Jing (晓景). “Strengthen Military-Civilian Fusion in the Field of Cyber Security and Give Full Play to the Strategic Effect of High-Quality Resources (加强网络安全领域军民融合,发挥优质资源的战略效应).” China Information Security (中国信息安全), March 15, 2016, 44–45.
China Security Science Editorial Department (本刊编辑部). “Selected Security Proposals for the Two Session (两会安全提案选登).” China Information Security (中国信息安全), no. 4 (2018): 85–90.
[156] “The Demonstration of the ‘Militia Activity Day’ in Chenzhou City has Ignited the Enthusiasm for Improving Capabilities and Inspiring Honor” (郴州市”民兵活动日”活动课目演示燃爆了提升能力，激发荣誉) ICSWB, 2024. https://web.archive.org/web/20250704043338/https://www.icswb.com/newspaper_article-detail-1790727.html; “Hainan Military Region Strengthens Joint Exercises Between Militia and Troops to Forge Reserve Forces to Defend the South China Sea,” China National Defense News (中国国防报), 2016https://web.archive.org/web/20160225092651/http://military.people.com.cn/n1/2016/0224/c1011-28145851.html; “CPPCC National Committee member: Set up special funds to upgrade Northeast cybersecurity facilities,” Security Internal Reference (安全内参), 3/6/2018 https://www.secrss.com/articles/1251; Solving New Problems with New Perspectives: I Am a Member of the Communist Party (用新视角解新课题：我是共产党员), Gwyoo.com, December 5, 2022. https://web.archive.org/web/20250704151343/https://www.gwyoo.com/article/lidaojianhua/dwdangjian/200712/102881.html.
[157] Long Libin (龙礼彬). “The Network Operations and Maintenance Team Opens Up the Information Link (网络运维分队打通信息链路).” China Military Online (中国军网), May 11, 2022. https://web.archive.org/web/20250704020800/http://www.81.cn/gfbmap/content/2022-05/17/content_315696.htm. AND http://www.81.cn/rmjz_203219/zgmb/2023nd4q/xxgcesd/16225105.html
[158] Citation Available Upon Request.
[159] Wang Xiaoming (王晓明), ed. Introduction to Cyberspace Operations (网络空间作战概论). PLA National Defense Information Academy (中国人民解放军国防信息学院), 2017., Zhou Ling (周玲). “Strengthening the Militia’s Emergency Response Capabilities (加强民兵应急应战能力建设).” China Military Online (中国军网),

June 17, 2024.
https://web.archive.org/web/20250703163556/http://www.81.cn/szb_223187/gfbszbxq/index.html?paperName=zggfb&paperDate=2024-06-17&paperNumber=03&articleid=933342.
[160] "The Demonstration of the 'Militia Activity Day' in Chenzhou City has Ignited the Enthusiasm for Improving Capabilities and Inspiring Honor" (郴州市"民兵活动日"活动课目演示燃爆了提升能力，激发荣誉) ICSWB, 2024. https://web.archive.org/web/20250704043338/https://www.icswb.com/newspaper_article-detail-1790727.html; "Hainan Military Region Strengthens Joint Exercises Between Militia and Troops to Forge Reserve Forces to Defend the South China Sea," China National Defense News (中国国防报), 2016https://web.archive.org/web/20160225092651/http://military.people.com.cn/n1/2016/0224/c1011-28145851.html; "CPPCC National Committee member: Set up special funds to upgrade Northeast cybersecurity facilities," Security Internal Reference (安全内参), 3/6/2018 https://www.secrss.com/articles/1251 Solving New Problems with New Perspectives: I Am a Member of the Communist Party (用新视角解新课题：我是共产党员), Gwyoo.com, December 5, 2022.
https://web.archive.org/web/20250704151343/https://www.gwyoo.com/article/lidaojianhua/dwdangjian/200712/102881.html.
[161] Wang Xiaoming (王晓明), ed. Introduction to Cyberspace Operations (网络空间作战概论). PLA National Defense Information Academy (中国人民解放军国防信息学院), 2017.pp. 121, 206-255.
[162] Wang Xiaoming (王晓明), ed. Introduction to Cyberspace Operations (网络空间作战概论). PLA National Defense Information Academy (中国人民解放军国防信息学院), 2017.pg. 206
[163] Citation Available Upon Request.
[164] John Chen, Joe McReynolds, and Kieran Green, "The PLA Strategic Support Force: A 'Joint' Force for Information Operations," in The PLA Beyond Borders: Chinese Military Operations in Regional and Global Context, Joel Wuthnow et al (ed.), Washington D.C., 2021.
[165] See: attached data sheet.
[166] Gu Gang (谷钢), A Brief Discussion on the Construction of Combat Capabilities of College Militia Information Units (略论高校民兵信息分队作战能力建设), Central South University (中南大学), Master's Thesis, 2010; Xu Yonghan (徐永汉), and Zheng Ning (郑宁). "Mission Construction and Application of Militia Cyber Warfare Team (民兵网络战分队的任务建设与运用)." National Defense (国防), no. 8 (December 2006): 39–40
[167] China National Defense News (中国国防报). "Hainan Military Region Strengthens Joint Exercises Between Miltia and Soldiers to Forge Reserve Forces to Defend the South China Sea (海南军区加强民兵与部队联演 锻造保卫南海后备力量)." February 24, 2016. http://military.people.com.cn/n1/2016/0224/c1011-28145851.html.
[168] China National Defense News (中国国防报). "Hainan Military Region Strengthens Joint Exercises Between Miltia and Soldiers to Forge Reserve Forces to Defend the South China Sea (海南军区加强民兵与部队联演 锻造保卫南海后备力量)." February 24, 2016. http://military.people.com.cn/n1/2016/0224/c1011-28145851.html.
[169] From a New Starting Point, Toward New Capability Concentration: Henan Provincial Military District Explores Potential in Emerging Domains to Build Strong Civilian-Military Specialist Teams (从"新"出发 向"新"聚能——河南省军区深挖新兴领域潜力编实建强民兵专业分队纪实), People's Armed Forces (人民武装), May 20, 2024.
[170] China National Defense News (中国国防报). "Hainan Military Region Strengthens Joint Exercises Between Miltia and Soldiers to Forge Reserve Forces to Defend the South China Sea (海南军区加强民兵与部队联演 锻造保卫南海后备力量)." February 24, 2016. http://military.people.com.cn/n1/2016/0224/c1011-28145851.html.
[171] Xiao Tianliang (ed.). In Their Own Words: The Science of Military Strategy. Beijing: PLA Academy of Military Sciences (Translated by the China Aerospace Studies Institute, 2020. pg. 231
[172] Song Hui (宋辉). "Training the Target Range Construction by the Militiaman Network Attack and Defense for the Security Problem (论民兵网络攻防训练靶场建设的安全问题)." Science Technology and Engineering (科学技术与工程), 2008.
[173] Dongfang Hong Think Tank (东方红智库), "Research on the Mobilization of China's Reserve Forces: Taking the Construction of "Cyber Militias" as an Example," (中国后备力量动员的研究：以"网络民兵"建设为例), National Defense Mobilization Special Issue (国防动员专刊), June 3, 2024.
[174] Xu Yonghan (徐永汉), and Zheng Ning (郑宁). "Mission Construction and Application of Militia Cyber Warfare Team (民兵网络战分队的任务建设与运用)." National Defense (国防), no. 8 (December 2006): 39–40

[175] Dongfang Hong Think Tank (东方红智库), “Research on the Mobilization of China's Reserve Forces: Taking the Construction of “Cyber Militias” as an Example,” (中国后备力量动员的研究：以”网络民兵”建设为例), National Defense Mobilization Special Issue (国防动员专刊), June 3, 2024. https://www.uscc.gov/sites/default/files/2024-02/Censorship_Practices_of_the_Peoples_Republic_of_China.pdf
[176] Kieran Green et al, “Censorship Practices of the People’s Republic of China, Exovera via the U.S.-China Economic and Security Review Commission (USCC), 2024, https://www.uscc.gov/sites/default/files/2024-02/Censorship_Practices_of_the_Peoples_Republic_of_China.pdf.
[177] Kieran Green et al, “Censorship Practices of the People’s Republic of China, Exovera via the U.S.-China Economic and Security Review Commission (USCC), 2024, https://www.uscc.gov/sites/default/files/2024-02/Censorship_Practices_of_the_Peoples_Republic_of_China.pdf.
[178] Kieran Green et al, “Censorship Practices of the People’s Republic of China, Exovera via the U.S.-China Economic and Security Review Commission (USCC), 2024, https://www.uscc.gov/sites/default/files/2024-02/Censorship_Practices_of_the_Peoples_Republic_of_China.pdf.
[179] https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Other-Topics/2025-01-06%20PLA%20view%20of%20the%20Information%20Domain.pdf?ver=MqTu69vXJ41zUkJV0cY6Jg%3d%3d
[180] Zhenping County Convenes 2020 Military-Civilian Joint Conference on National Defense Mobilization (镇平县召开 2020 年国防动员军地联席会议), Zhenping County People’s Government (镇平县人民政府), April 24, 2020. https://web.archive.org/web/20250704040804/https://www.zhenping.gov.cn/2020/04-24/587483.html.
[181] Citation Available Upon Request.
[182] Hunan Electronic Information Industry Institute (湖南电子信息产业学院). “Maintaining Network Security, Monitoring and Guiding Public Opinion: Our Hospital’s Basic Militia Network Team Receives Instruction (维护网络安全 监控引导舆情——我院基干民兵网络分队接受点验).” June 8, 2018. https://gxt.hunan.gov.cn/gxt/hnxcy/xcyxwzx/xcygzdt/202209/t20220923_29014809.html.
[183] “Our School Carried Out Military Training Activities for the Network Attack and Defense Militia Team (我校开展网络攻防民兵分队军事训练活动).” Yan’an University Party Committee Propaganda Department (延安大学党委宣传部), May 15, 2018. https://web.archive.org/web/20250124150821/https://www.yau.edu.cn/info/1120/330617.htm
[184] Shu Ke (舒可). “Looking at Milita Force Building From the Perspective of Anti-Epidemic Efforts (从抗疫看民兵力量建设).” China Military Online (中国军网), July 1, 2020. https://web.archive.org/web/20231022175831/http://www.81.cn/gfbmap/content/2020-07/01/content_264897.htm.
[185] The District People’s Armed Forces Department Organized Militia to Fight the Epidemic (区人武部组织民兵抗击疫情), Tianjin Jinnan District Double Support Office (天津市津南区双拥办), January 2022, https://web.archive.org/save/https://www.tjjn.gov.cn/ztzl/ztzl_65015/jnsy/202202/W020220218574508924227.pdf.
[186] Veterans Tell the Story of the Harbin Militia’s Anti-Epidemic Efforts (老兵讲述哈尔滨民兵抗疫故事), Sohu (搜狐), August 8, 2020. https://web.archive.org/web/20250704041202/https://www.sohu.com/a/412069948_99962390.
[187] Nearly 700 Party Members and Cadres Gathered and the Party Flag Fluttered on the Front Line of Songshan Lake’s Anti-Epidemic Work (近 700 名党员干部集结，松山湖抗疫一线党旗飘扬), Sohu (搜狐), December 12, 2022. Shu Ke (舒可). “Looking at Milita Force Building From the Perspective of Anti-Epidemic Efforts (从抗疫看民兵力量建设).” China Military Online (中国军网), July 1, 2020. https://web.archive.org/web/20231022175831/http://www.81.cn/gfbmap/content/2020-07/01/content_264897.htm.
[188] Citation Available Upon Request.
[189] Chinese Hacking Competitions Fuel the Country’s Broad Cyber Ambitions, Bloomberg, April 30, 2025. https://www.bloomberg.com/news/articles/2025-04-30/chinese-hacking-competitions-fuel-the-country-s-broad-cyber-ambitions
[190] China National Radio (央广网). “Approaching the ‘National Model Veterans’ (Part 3) (走近‘全国模范退役军人’（三）).” August 17, 2024. https://web.archive.org/web/20241005122805/http://www.cnr.cn/gd/nyhkt/20240817/t20240817_526857045.shtml; Liang Lisheng (梁力升). “‘Be a Good Soldier of the Era, Become the Most Outstanding Baise Serviceman’ Campaign Launch Ceremony Held (‘当时代好战士 做最美百色兵’专题活动启动仪式举行).” Youjiang Daily (右江日报), March 1, 2023. https://web.archive.org/web/20250704041649/https://www.gxbszx.gov.cn/html/news-view-153370.html; 广东省退役军人事务厅. “Mao Yifeng｜Deputy Director of the People’s Armed Forces

Department of Nancheng Subdistrict, Dongguan City (毛以锋丨东莞市南城街道人民武装部副部长).” August 29, 2024. https://web.archive.org/web/20250704041710/https://dva.gd.gov.cn/ztzl/qgmf/mftyjr/content/post_4485109.html.

[191] Citation Available Upon Request.

[192] Wu'an City, Hebei Province Held a Mobilization Meeting for Militia Emergency Team Training (河北省武安市举行民兵应急分队开训动员大会), Sohu (搜狐), July 23, 2020.

[193]Hacker 7 Master (黑客 7 师傅), “Video Courseware + Supporting Materials + Cyber Range Training,” Bilibili (哔哩哔哩), March 15, 2022. https://www.bilibili.com/read/cv33432603/

[194] https://web.archive.org/save/https://www.sohu.com/a/808924966_121888494

[195] China National Radio (央广网). “Approaching the ‘National Model Veterans’ (Part 3) (走近‘全国模范退役军人’（三）).” August 17, 2024. https://web.archive.org/web/20241005122805/http://www.cnr.cn/gd/nyhkt/20240817/t20240817_526857045.shtml.

[196] 360 Group’s Cybersecurity Militia Project Wins Nomination for 2021 Digital Economy Party-Building Innovation Award (360 集团网络安全民兵分队项目荣获 2021 数字经济党建优秀创新项目提名奖), Party Committee of 360 Group (360 集团党委), August 2, 2021. Party Committee of the Capital Internet Association (首都互联网协会党委). https://web.archive.org/save/https://www.sohu.com/a/481010011_99981118; 360 15th Anniversary Special Program - 01-Talk Show Conference Wei Ruochen Visited the Jiuxianqiao Street Network Security Militia Team (【360 十五周年特别节目】01-脱口秀大会韦若琛做客酒仙桥街道网络安全民兵分队), 2020. https://web.archive.org/web/20250704142420/https://www.bilibili.com/video/BV1HK411G732/.

[197] China Unveils Its First Civil-Military Cybersecurity Innovation Center. People’s Daily Online , December 28, 2017. https://web.archive.org/web/20210613123606/http://en.people.cn/n3/2017/1228/c90000-9309428.html

[198] China Unveils Its First Civil-Military Cybersecurity Innovation Center. People’s Daily Online , December 28, 2017. https://web.archive.org/web/20210613123606/http://en.people.cn/n3/2017/1228/c90000-9309428.html

[199] 360 Group’s Cybersecurity Militia Project Wins Nomination for 2021 Digital Economy Party-Building Innovation Award (360 集团网络安全民兵分队项目荣获 2021 数字经济党建优秀创新项目提名奖), Party Committee of 360 Group (360 集团党委), August 2, 2021. Party Committee of the Capital Internet Association (首都互联网协会党委). https://web.archive.org/save/https://www.sohu.com/a/481010011_99981118

[200] Baidu News. “Jiuxianqiao Subdistrict Holds Flag-Raising Ceremony for the Cyber Security Militia (酒仙桥街道举行网络安全民兵分队授旗仪式).” December 16, 2020. https://web.archive.org/web/20250704030035/https://wappass.baidu.com/static/captcha/tuxing.html?ak=572be823e2f50ea759a616c060d6b9f1&backurl=https%3A%2F%2Fmbd.baidu.com%2Fnewspage%2Fdata%2Flandingsuper%3Fid%3D1686222420624511090%26wfr%3Dspider%26for%3Dpc%26third%3Dbaijiahao%26baijiahao_id%3D1686222420624511090%26c_source%3Dkunlun%26c_score%3D0.999000&timestamp=1751597946&signature=b26d914fdc08d0d2789133568937af1c.

[201] Baidu News. “Jiuxianqiao Subdistrict Holds Flag-Raising Ceremony for the Cyber Security Militia (酒仙桥街道举行网络安全民兵分队授旗仪式).” December 16, 2020. https://web.archive.org/web/20250704030035/https://wappass.baidu.com/static/captcha/tuxing.html?ak=572be823e2f50ea759a616c060d6b9f1&backurl=https%3A%2F%2Fmbd.baidu.com%2Fnewspage%2Fdata%2Flandingsuper%3Fid%3D1686222420624511090%26wfr%3Dspider%26for%3Dpc%26third%3Dbaijiahao%26baijiahao_id%3D1686222420624511090%26c_source%3Dkunlun%26c_score%3D0.999000&timestamp=1751597946&signature=b26d914fdc08d0d2789133568937af1c.

[202] Baidu News. “Jiuxianqiao Subdistrict Holds Flag-Raising Ceremony for the Cyber Security Militia (酒仙桥街道举行网络安全民兵分队授旗仪式).” December 16, 2020. https://web.archive.org/web/20250704030035/https://wappass.baidu.com/static/captcha/tuxing.html?ak=572be823e2f50ea759a616c060d6b9f1&backurl=https%3A%2F%2Fmbd.baidu.com%2Fnewspage%2Fdata%2Flandingsuper%3Fid%3D1686222420624511090%26wfr%3Dspider%26for%3Dpc%26third%3Dbaijiahao%26baijiahao_id%3D1686222420624511090%26c_source%3Dkunlun%26c_score%3D0.999000&timestamp=1751597946&signature=b26d914fdc08d0d2789133568937af1c.

[203] Editorial Department (本刊编辑部). “Actively Promote Vulnerability Warning and Risk Control Work (积极促进开展漏洞预警及风险消控工作).” China Information Security (中国信息安全), no. 5 (2023): 84–90.

[204] Smartmore Technology (思谋科技). “360 Undertakes the Establishment of the Cyberspace Security Military-Civil Fusion Innovation Center (360 承建网络空间安全军民融合创新中心成立收藏).” 2024. https://web.archive.org/web/20250704143427/https://cn.smartmore.com/article/post/19202.html.
[205] Smartmore Technology (思谋科技). “360 Undertakes the Establishment of the Cyberspace Security Military-Civil Fusion Innovation Center (360 承建网络空间安全军民融合创新中心成立收藏).” 2024. https://web.archive.org/web/20250704143427/https://cn.smartmore.com/article/post/19202.html.
[206] Smartmore Technology (思谋科技). “360 Undertakes the Establishment of the Cyberspace Security Military-Civil Fusion Innovation Center (360 承建网络空间安全军民融合创新中心成立收藏).” 2024. https://web.archive.org/web/20250704143427/https://cn.smartmore.com/article/post/19202.html.
[207] Actively promote vulnerability warning and risk control work 积极促进开展漏洞预警及风险消控工作 ; Banyuetan (半月谈网). “360 Group’s Cyber Security Militia Team Guards the ‘Fifth Dimension’ (360 集团网络安全民兵分队守护‘第五维空间’).” May 18, 2021. https://web.archive.org/web/20250704030657/http://www.banyuetan.org/hzjh/detail/20210518/1000200033138981621298012850799816_1.html.
[208] “360 Group’s Cyber Security Militia Team Guards the ‘Fifth Dimension’ (360 集团网络安全民兵分队守护‘第五维空间’).” May 18, 2021. https://web.archive.org/web/20250704030657/http://www.banyuetan.org/hzjh/detail/20210518/1000200033138981621298012850799816_1.html.
[209] “360 Group’s Cyber Security Militia Team Guards the ‘Fifth Dimension’ (360 集团网络安全民兵分队守护‘第五维空间’).” May 18, 2021. https://web.archive.org/web/20250704030657/http://www.banyuetan.org/hzjh/detail/20210518/1000200033138981621298012850799816_1.html.
[210] “360 Group’s Cyber Security Militia Team Guards the ‘Fifth Dimension’ (360 集团网络安全民兵分队守护‘第五维空间’).” May 18, 2021. https://web.archive.org/web/20250704030657/http://www.banyuetan.org/hzjh/detail/20210518/1000200033138981621298012850799816_1.html.
[211] “360 Group’s Cyber Security Militia Team Guards the ‘Fifth Dimension’ (360 集团网络安全民兵分队守护‘第五维空间’).” May 18, 2021. https://web.archive.org/web/20250704030657/http://www.banyuetan.org/hzjh/detail/20210518/1000200033138981621298012850799816_1.html.
[212] “360 Group’s Cyber Security Militia Team Guards the ‘Fifth Dimension’ (360 集团网络安全民兵分队守护‘第五维空间’).” May 18, 2021. https://web.archive.org/web/20250704030657/http://www.banyuetan.org/hzjh/detail/20210518/1000200033138981621298012850799816_1.html.
[213] “360 Group’s Cyber Security Militia Team Guards the ‘Fifth Dimension’ (360 集团网络安全民兵分队守护‘第五维空间’).” May 18, 2021. https://web.archive.org/web/20250704030657/http://www.banyuetan.org/hzjh/detail/20210518/1000200033138981621298012850799816_1.html; Tongxin e-Bridade (同心 e 桥). “Wang Weimin, Member of the Standing Committee of the Chaoyang District Committee and Minister of the Armed Forces, Went to Jiuxianqiao Subdistrict for Research and Guidance (朝阳区委常委、武装部部长王维民到酒仙桥街道调研指导).” WeChat (blog), July 14, 2022. https://web.archive.org/web/20250704140801/https://mp.weixin.qq.com/s?__biz=Mzk0NjI1MjI2Mg==&mid=2247558720&idx=1&sn=74a8906cc30d90740f8407244186f02b&chksm=c30b56c9f47cdfdf00c13348c956898600e76292c35d5b687fd70bee27426779f9bd20a03fa9&scene=27; Constitution of the Communist Party of China. International Department, Central Committee of the Communist Party of China, December 21, 2018. https://www.idcpc.gov.cn/english2023/tjzl/cpcjj/PartyConstitution/.
[214] “360 Group’s Cyber Security Militia Team Guards the ‘Fifth Dimension’ (360 集团网络安全民兵分队守护‘第五维空间’).” May 18, 2021. https://web.archive.org/web/20250704030657/http://www.banyuetan.org/hzjh/detail/20210518/1000200033138981621298012850799816_1.html; Tongxin e-Bridade (同心 e 桥). “Wang Weimin, Member of the Standing Committee of the Chaoyang District Committee and Minister of the Armed Forces, Went to Jiuxianqiao Subdistrict for Research and Guidance (朝阳区委常委、武装部部长王维民到酒仙桥街道调研指导).” WeChat (blog), July 14,

2022.
https://web.archive.org/web/20250704140801/https://mp.weixin.qq.com/s?__biz=Mzk0NjI1MjI2Mg==&mid=2247558720&idx=1&sn=74a8906cc30d90740f8407244186f02b&chksm=c30b56c9f47cdfdf00c13348c956898600e76292c35d5b687fd70bee27426779f9bd20a03fa9&scene=27; 360 Internet Security Center (360 互联网安全中心). “360 Group Launched a Series of Party-Building Activities to Become a Company Truly Owned by the Chinese People! (360 集团开展系列党建活动，做真正的中国人自己的公司！).” October 17, 2017.
https://web.archive.org/web/20180224095410/http://www.360.cn/newslist/zxzx/360jtkzxldjhdzzzdzgrzjdgs.html.

[215] http://www.360.cn/newslist/zxzx/360jtkzxldjhdzzzdzgrzjdgs.html.

[216] “360 Group’s Cyber Security Militia Team Guards the ‘Fifth Dimension’ (360 集团网络安全民兵分队守护‘第五维空间’).” May 18, 2021.
https://web.archive.org/web/20250704030657/http://www.banyuetan.org/hzjh/detail/20210518/1000200033138981621298012850799816_1.html.

[217] China Unveils Its First Civil-Military Cybersecurity Innovation Center (中国首个军民融合网络安全创新中心揭幕), People’s Daily Online (人民网), December 28, 2017.
https://web.archive.org/web/20250118111709/http://en.people.cn/n3/2017/1228/c90000-9309428.html.

[218] China Unveils Its First Civil-Military Cybersecurity Innovation Center (中国首个军民融合网络安全创新中心揭幕), People’s Daily Online (人民网), December 28, 2017.
https://web.archive.org/web/20250118111709/http://en.people.cn/n3/2017/1228/c90000-9309428.html.

[219] China Unveils Its First Civil-Military Cybersecurity Innovation Center (中国首个军民融合网络安全创新中心揭幕), People’s Daily Online (人民网), December 28, 2017.
https://web.archive.org/web/20250118111709/http://en.people.cn/n3/2017/1228/c90000-9309428.html.

[220] Tongxin e-Bridade (同心 e 桥). “Wang Weimin, Member of the Standing Committee of the Chaoyang District Committee and Minister of the Armed Forces, Went to Jiuxianqiao Subdistrict for Research and Guidance (朝阳区委常委、武装部部长王维民到酒仙桥街道调研指导).” WeChat (blog), July 14, 2022.
https://web.archive.org/web/20250704140801/https://mp.weixin.qq.com/s?__biz=Mzk0NjI1MjI2Mg==&mid=2247558720&idx=1&sn=74a8906cc30d90740f8407244186f02b&chksm=c30b56c9f47cdfdf00c13348c956898600e76292c35d5b687fd70bee27426779f9bd20a03fa9&scene=27.

[221] “360 Group’s Cyber Security Militia Team Guards the ‘Fifth Dimension’ (360 集团网络安全民兵分队守护‘第五维空间’).” May 18, 2021.
https://web.archive.org/web/20250704030657/http://www.banyuetan.org/hzjh/detail/20210518/1000200033138981621298012850799816_1.html.

[222] “360 Group’s Cyber Security Militia Team Guards the ‘Fifth Dimension’ (360 集团网络安全民兵分队守护‘第五维空间’).” May 18, 2021.
https://web.archive.org/web/20250704030657/http://www.banyuetan.org/hzjh/detail/20210518/1000200033138981621298012850799816_1.html.

[223] “360 Group’s Cyber Security Militia Team Guards the ‘Fifth Dimension’ (360 集团网络安全民兵分队守护‘第五维空间’).” May 18, 2021.
https://web.archive.org/web/20250704030657/http://www.banyuetan.org/hzjh/detail/20210518/1000200033138981621298012850799816_1.html.

[224] Tongxin e-Bridade (同心 e 桥). “Wang Weimin, Member of the Standing Committee of the Chaoyang District Committee and Minister of the Armed Forces, Went to Jiuxianqiao Subdistrict for Research and Guidance (朝阳区委常委、武装部部长王维民到酒仙桥街道调研指导).” WeChat (blog), July 14, 2022.
https://web.archive.org/web/20250704140801/https://mp.weixin.qq.com/s?__biz=Mzk0NjI1MjI2Mg==&mid=2247558720&idx=1&sn=74a8906cc30d90740f8407244186f02b&chksm=c30b56c9f47cdfdf00c13348c956898600e76292c35d5b687fd70bee27426779f9bd20a03fa9&scene=27.

[225] Tongxin e-Bridade (同心 e 桥). “Wang Weimin, Member of the Standing Committee of the Chaoyang District Committee and Minister of the Armed Forces, Went to Jiuxianqiao Subdistrict for Research and Guidance (朝阳区委常委、武装部部长王维民到酒仙桥街道调研指导).” WeChat (blog), July 14, 2022.
https://web.archive.org/web/20250704140801/https://mp.weixin.qq.com/s?__biz=Mzk0NjI1MjI2Mg==&mid=2247558720&idx=1&sn=74a8906cc30d90740f8407244186f02b&chksm=c30b56c9f47cdfdf00c13348c956898600e76292c35d5b687fd70bee27426779f9bd20a03fa9&scene=27.

[226] Antiy Innovation (安天创造). “New Youth Pursuing Dreams, We Are Young (逐梦新青年，我们正青春).” July 2022. https://web.archive.org/web/20250103173659/https://www.antiy.cn/observe_download/observe_302.pdf.
[227] Veterans Tell the Story of the Harbin Militia’s Anti-Epidemic Efforts (老兵讲述哈尔滨民兵抗疫故事), Sohu (搜狐), August 8, 2020.
https://web.archive.org/web/20250704041202/https://www.sohu.com/a/412069948_99962390.
[228] https://www.secrss.com/articles/1251; Cui Guangyao (崔光耀). “Current Security Hotspots From the Perspective of the Two Sessions (从两会声音看当前安全热点).” China Information Security (中国信息安全), no. 4 (2018): 56–57.
[229] Antiy (安天). “On the Second Anniversary of General Secretary Xi’s ‘4.19’ Important Speech, the Antiy Cyber Militia Team Was Established (习总书记‘4·19’重要讲话两周年之际 安天网络民兵分队成立).” Antiy Labs (安天), April 20, 2018.
https://web.archive.org/web/20250704145552/https://www.antiy.cn/About/news/2018042001.html.
[230] Antiy (安天). “On the Second Anniversary of General Secretary Xi’s ‘4.19’ Important Speech, the Antiy Cyber Militia Team Was Established (习总书记‘4·19’重要讲话两周年之际 安天网络民兵分队成立).” Antiy Labs (安天), April 20, 2018.
https://web.archive.org/web/20250704145552/https://www.antiy.cn/About/news/2018042001.html.
[231] Antiy (安天). “Relevant Personnel from the Militia Reserve Bureau of the Ministry of National Defense Mobilization Visited Antiy Headquarters for Research (国防动员部民兵预备役局有关人员莅临安天总部调研).” Antiy Labs (安天), May 11, 2019.
https://web.archive.org/web/20250704145922/https://www.antiy.cn/About/news/20191105.html.
[232] China’s Cybersecurity Industry White Paper (中国网络安全产业白皮书).” China Academy of Information and Communications Technology (中国信息通信研究院), September 2018.
https://web.archive.org/web/20250703170001/http://www.caict.ac.cn/kxyj/qwfb/bps/201809/P020181022488727633391.pdf
[233] Antiy (安天). “Relevant Personnel from the Militia Reserve Bureau of the Ministry of National Defense Mobilization Visited Antiy Headquarters for Research (国防动员部民兵预备役局有关人员莅临安天总部调研).” Antiy Labs (安天), May 11, 2019.
https://web.archive.org/web/20250704145922/https://www.antiy.cn/About/news/20191105.html.
[234] Veterans Tell the Story of the Harbin Militia’s Anti-Epidemic Efforts (老兵讲述哈尔滨民兵抗疫故事), Sohu (搜狐), August 8, 2020.
https://web.archive.org/web/20250704041202/https://www.sohu.com/a/412069948_99962390.
[235] Antiy (安天). “To Commemorate the Sixth Anniversary of the ‘April 19’ Important Speech, Antiy Launched the 'Overall National Security Concept Monthly Public Activities (纪念”4·19”重要讲话六周年 安天开展‘总体国家安全观’宣传月活动).” Antiy Labs (安天), April 19, 2022.
https://web.archive.org/web/20230804030052/https://www.antiy.cn/About/news/20220419-1.html; Antiy (安天). “Antiy Received a Letter of Thanks from the Harbin Garrison (安天收到哈尔滨警备区感谢信).” Antiy Innovation (安天创造), March 30, 2020.
https://web.archive.org/web/20240616110236/https://www.antiy.cn/observe_download/observe_224.pdf; Cui Guangyao (崔光耀). “Current Security Hotspots From the Perspective of the Two Sessions (从两会声音看当前安全热点).” China Information Security (中国信息安全), no. 4 (2018): 56–57; Guo Yuandan (郭媛丹). “Members of the National Committee of the Chinese People’s Political Consultative Conference Suggested Improving the Coordinated Assessment and Command Mechanism for Major Social Risks and Called for the Establishment of a ‘Cyber Security Militia’ System (全国政协委员建议完善重大社会风险协同研判指挥机制 呼吁建设‘网信民兵’体系).” Global Times (环球时报), May 23, 2020.
https://web.archive.org/web/20250704150815/https://lianghui.huanqiu.com/article/9CaKrnKr620?from=timeline&isappinstalled=0.
[236] Antiy (安天). “To Commemorate the Sixth Anniversary of the ‘April 19’ Important Speech, Antiy Launched the 'Overall National Security Concept Monthly Public Activities (纪念”4·19”重要讲话六周年 安天开展‘总体国家安全观’宣传月活动).” Antiy Labs (安天), April 19, 2022.
https://web.archive.org/web/20230804030052/https://www.antiy.cn/About/news/20220419-1.html

[237] Antiy (安天). “To Commemorate the Sixth Anniversary of the ‘April 19’ Important Speech, Antiy Launched the 'Overall National Security Concept Monthly Public Activities (纪念”4・19”重要讲话六周年 安天开展‘总体国家安全观’宣传月活动).” Antiy Labs (安天), April 19, 2022. https://web.archive.org/web/20230804030052/https://www.antiy.cn/About/news/20220419-1.html

[238] “Antiy Received a Letter of Thanks from the Harbin Garrison (安天收到哈尔滨警备区感谢信).” Antiy Innovation (安天创造), March 30, 2020. https://web.archive.org/web/20240616110236/https://www.antiy.cn/observe_download/observe_224.pdf

[239] Antiy (安天). “On the Second Anniversary of General Secretary Xi’s ‘4.19’ Important Speech, the Antiy Cyber Militia Team Was Established (习总书记‘4・19’重要讲话两周年之际 安天网络民兵分队成立).” Antiy Labs (安天), April 20, 2018. https://web.archive.org/web/20250704145552/https://www.antiy.cn/About/news/2018042001.html.

[240] Antiy (安天). “On the Second Anniversary of General Secretary Xi’s ‘4.19’ Important Speech, the Antiy Cyber Militia Team Was Established (习总书记‘4・19’重要讲话两周年之际 安天网络民兵分队成立).” Antiy Labs (安天), April 20, 2018. https://web.archive.org/web/20250704145552/https://www.antiy.cn/About/news/2018042001.html.

[241] “Antiy Received a Letter of Thanks from the Harbin Garrison (安天收到哈尔滨警备区感谢信).” Antiy Innovation (安天创造), March 30, 2020. https://web.archive.org/web/20240616110236/https://www.antiy.cn/observe_download/observe_224.pdf

[242] “Antiy Received a Letter of Thanks from the Harbin Garrison (安天收到哈尔滨警备区感谢信).” Antiy Innovation (安天创造), March 30, 2020. https://web.archive.org/web/20240616110236/https://www.antiy.cn/observe_download/observe_224.pdf

[243] Security Internal Reference (安全内参). “CPPCC National Committee Member: Set Up Special Funds to Upgrade Northeast Cybersecurity Facilities (全国政协委员：设专项资金升级东北网络安全设施).” March 6, 2018. https://web.archive.org/web/20250704145643/https://www.secrss.com/articles/1251.

[244] Security Internal Reference (安全内参). “CPPCC National Committee Member: Set Up Special Funds to Upgrade Northeast Cybersecurity Facilities (全国政协委员：设专项资金升级东北网络安全设施).” March 6, 2018. https://web.archive.org/web/20250704145643/https://www.secrss.com/articles/1251.

[245] Guo Yuandan (郭媛丹). “Members of the National Committee of the Chinese People’s Political Consultative Conference Suggested Improving the Coordinated Assessment and Command Mechanism for Major Social Risks and Called for the Establishment of a ‘Cyber Security Militia’ System (全国政协委员建议完善重大社会风险协同研判指挥机制 呼吁建设‘网信民兵’体系).” Global Times (环球时报), May 23, 2020. https://web.archive.org/web/20250704150815/https://lianghui.huanqiu.com/article/9CaKrnKr620?from=timeline&isappinstalled=0.

[246] Guo Yuandan (郭媛丹). “Members of the National Committee of the Chinese People’s Political Consultative Conference Suggested Improving the Coordinated Assessment and Command Mechanism for Major Social Risks and Called for the Establishment of a ‘Cyber Security Militia’ System (全国政协委员建议完善重大社会风险协同研判指挥机制 呼吁建设‘网信民兵’体系).” Global Times (环球时报), May 23, 2020. https://web.archive.org/web/20250704150815/https://lianghui.huanqiu.com/article/9CaKrnKr620?from=timeline&isappinstalled=0.

[247] Antiy Innovation (安天创造). “New Youth Pursuing Dreams, We Are Young (逐梦新青年，我们正青春).” July 2022. https://web.archive.org/web/20250103173659/https://www.antiy.cn/observe_download/observe_302.pdf.

[248] “Antiy Received a Letter of Thanks from the Harbin Garrison (安天收到哈尔滨警备区感谢信).” Antiy Innovation (安天创造), March 30, 2020. https://web.archive.org/web/20240616110236/https://www.antiy.cn/observe_download/observe_224.pdf

[249] “Antiy Received a Letter of Thanks from the Harbin Garrison (安天收到哈尔滨警备区感谢信).” Antiy Innovation (安天创造), March 30, 2020. https://web.archive.org/web/20240616110236/https://www.antiy.cn/observe_download/observe_224.pdf

[250] “Antiy Received a Letter of Thanks from the Harbin Garrison (安天收到哈尔滨警备区感谢信).” Antiy Innovation (安天创造), March 30, 2020. https://web.archive.org/web/20240616110236/https://www.antiy.cn/observe_download/observe_224.pdf

[251] “Antiy Received a Letter of Thanks from the Harbin Garrison (安天收到哈尔滨警备区感谢信).” Antiy Innovation (安天创造), March 30, 2020.
https://web.archive.org/web/20240616110236/https://www.antiy.cn/observe_download/observe_224.pdf
[252]“Antiy Received a Letter of Thanks from the Harbin Garrison (安天收到哈尔滨警备区感谢信).” Antiy Innovation (安天创造), March 30, 2020.
https://web.archive.org/web/20240616110236/https://www.antiy.cn/observe_download/observe_224.pdf
[253] Solving New Problems with New Perspectives: I Am a Member of the Communist Party (用新视角解新课题：我是共产党员), Gwyoo.com, December 5, 2022.
https://web.archive.org/web/20250704151343/https://www.gwyoo.com/article/lidaojianhua/dwdangjian/200712/102881.html.
[254] China Security Science Editorial Department (本刊编辑部). “Selected Security Proposals for the Two Session (两会安全提案选登).” China Information Security (中国信息安全), no. 4 (2018): 85–90.
[255] PRC Ministry of National Defense (中华人民共和国国防部). “Jiangxi Province Ji’an Military Sub-District Organizes Joint Training for Militia and Garrison Troops (江西省吉安军分区组织民兵与驻军部队联合训练).” November 26, 2024.
https://web.archive.org/web/20250223102419/http://www.mod.gov.cn/gfbw/gfdy/wzdy/16354174.html.
[256] Nanjing Daily (南京日报). “Nanjing Daily Shicheng National Defense Issue 21: A Side Contingent of Nanjing-Based Troops Visiting the Nanjing Development Photo Exhibition to Celebrate the 40th Anniversary of Reform and Opening Up.” November 26, 2018.
https://web.archive.org/web/20250704152139/https://njsy.nanjing.gov.cn/syxw/201912/t20191226_1923350.html.
[257] Nanjing Daily (南京日报). “Nanjing Daily Shicheng National Defense Issue 21: A Side Contingent of Nanjing-Based Troops Visiting the Nanjing Development Photo Exhibition to Celebrate the 40th Anniversary of Reform and Opening Up.” November 26, 2018.
https://web.archive.org/web/20250704152139/https://njsy.nanjing.gov.cn/syxw/201912/t20191226_1923350.html.
[258] Henan Provincial Military District Explores Potential in Emerging Domains to Strengthen Specialized Militia Units (河南省军区深挖新兴领域潜力编实建强民兵专业分队记事). Xuexi Juntuan (学习军团), May 19, 2024.
[259] Henan Provincial Military District Explores Potential in Emerging Domains to Strengthen Specialized Militia Units (河南省军区深挖新兴领域潜力编实建强民兵专业分队记事). Xuexi Juntuan (学习军团), May 19, 2024.
[260] Zhou Ling (周玲). “Strengthening the Militia’s Emergency Response Capabilities (加强民兵应急应战能力建设).” China Military Online (中国军网), June 17, 2024.
https://web.archive.org/web/20250703163556/http://www.81.cn/szb_223187/gfbszbxq/index.html?paperName=zggfb&paperDate=2024-06-17&paperNumber=03&articleid=933342.
[261] Zhou Ling (周玲). “Strengthening the Militia’s Emergency Response Capabilities (加强民兵应急应战能力建设).” China Military Online (中国军网), June 17, 2024.
https://web.archive.org/web/20250703163556/http://www.81.cn/szb_223187/gfbszbxq/index.html?paperName=zggfb&paperDate=2024-06-17&paperNumber=03&articleid=933342.
[262] Henan Provincial Military District Explores Potential in Emerging Domains to Strengthen Specialized Militia Units (河南省军区深挖新兴领域潜力编实建强民兵专业分队记事). Xuexi Juntuan (学习军团), May 19, 2024.
[263] Xiao Xinguang (肖新光). “Improve Cybersecurity Emergency Response Capabilities to Address Major Social Emergencies (提升网络安全应急能力，应对社会重大突发事件).” China Information Security (中国信息安全), no. 6 (2020): 30–31.
[264] Cai Zhengyang (蔡政洋), Sun Bin (孙彬), and Jiao Jinghong (焦景宏). “Zhengzhou City, Henan Province, Vigorously Develops New-Type Militia Forces to Support Economic and Social Development (河南省郑州市倾力打造民兵新质力量助力经济社会发展).” China National Defense News (中国国防报), n.d.
https://web.archive.org/web/20250704152628/http://www.mod.gov.cn/gfbw/gfdy/jjdy/4899086.html.
[265] Guo Yuandan (郭媛丹). “Members of the National Committee of the Chinese People’s Political Consultative Conference Suggested Improving the Coordinated Assessment and Command Mechanism for Major Social Risks and Called for the Establishment of a ‘Cyber Security Militia’ System (全国政协委员建议完善重大社会风险协同研判指挥机制 呼吁建设‘网信民兵’体系).” Global Times (环球时报), May 23, 2020.
https://web.archive.org/web/20250704150815/https://lianghui.huanqiu.com/article/9CaKrnKr620?from=timeline&isappinstalled=0; Liu Yu (刘宇). “Accurately Match Potential Data with Battlefield Needs (让潜力数据精准对接战

场需求).” China Military Online (中国军网), June 24, 2020. https://web.archive.org/web/20250704004634/http://www.81.cn/gfbmap/content/2020-06/24/content_264502.htm.

[266] Guo Yuandan (郭媛丹). “Members of the National Committee of the Chinese People’s Political Consultative Conference Suggested Improving the Coordinated Assessment and Command Mechanism for Major Social Risks and Called for the Establishment of a ‘Cyber Security Militia’ System (全国政协委员建议完善重大社会风险协同研判指挥机制 呼吁建设‘网信民兵’体系).” Global Times (环球时报), May 23, 2020. https://web.archive.org/web/20250704150815/https://lianghui.huanqiu.com/article/9CaKrnKr620?from=timeline&isappinstalled=0.

[267] “Solving New Problems with New Perspectives: I Am a Member of the Communist Party” (用新视角解新课题：我是共产党员), Gwyoo.com, December 5, 2022. https://web.archive.org/web/20250704151343/https://www.gwyoo.com/article/lidaojianhua/dwdangjian/200712/102881.html.

[268] “Solving New Problems with New Perspectives: I Am a Member of the Communist Party” (用新视角解新课题：我是共产党员), Gwyoo.com, December 5, 2022. https://web.archive.org/web/20250704151343/https://www.gwyoo.com/article/lidaojianhua/dwdangjian/200712/102881.html; Rongguang Technology (戎光科技). “Smart Mobilization System: Serving in Peacetime, Responding to Emergencies, and Fighting in Wartime (智慧动员系统：平时服务、急时应急、战时应战).” September 22, 2023. https://web.archive.org/web/20250703161004/https://www.sohu.com/a/722656107_121337322; AND Jian Tianbo (姜天波). “Strive to Achieve New Breakthroughs in Militia Construction in the New Era (努力谋求新时代民兵建设实现新突破).” China Military Online (中国军网), 2023. https://web.archive.org/web/20241014222726/http://www.81.cn/rmjz_203219/zgmb/2023nd9q/dysjhgf_246488/16258411.html.

[269] Cui Guangyao (崔光耀). “Current Security Hotspots From the Perspective of the Two Sessions (从两会声音看当前安全热点).” China Information Security (中国信息安全), no. 4 (2018): 56–57.

[270] Guo Yuandan (郭媛丹). “Members of the National Committee of the Chinese People’s Political Consultative Conference Suggested Improving the Coordinated Assessment and Command Mechanism for Major Social Risks and Called for the Establishment of a ‘Cyber Security Militia’ System (全国政协委员建议完善重大社会风险协同研判指挥机制 呼吁建设‘网信民兵’体系).” Global Times (环球时报), May 23, 2020. https://web.archive.org/web/20250704150815/https://lianghui.huanqiu.com/article/9CaKrnKr620?from=timeline&isappinstalled=0.

[271] Guo Yuandan (郭媛丹). “Members of the National Committee of the Chinese People’s Political Consultative Conference Suggested Improving the Coordinated Assessment and Command Mechanism for Major Social Risks and Called for the Establishment of a ‘Cyber Security Militia’ System (全国政协委员建议完善重大社会风险协同研判指挥机制 呼吁建设‘网信民兵’体系).” Global Times (环球时报), May 23, 2020. https://web.archive.org/web/20250704150815/https://lianghui.huanqiu.com/article/9CaKrnKr620?from=timeline&isappinstalled=0.

[272] Ma Jianguang (马建光). “Cyber Militia: Every Citizen Is a Soldier in the Information War Era (网络民兵：信息战争时代的全民皆兵).” Guangming Daily (光明日报), August 10, 2016. https://web.archive.org/web/20250703160427/http://www.81.cn/theory/2016-10/08/content_7289960.htm