ONLINE ISSN: 3007-3197 | PRINT ISSN: 3007-3189

http://amresearchreview.com/index.php/Journal/about

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 7 (2025)

Weaponizing Algorithms: China's Strategic AI Ecosystem and the Erosion of U.S. Informational Hegemony

[1]Izba Zaheer, [2]Dr. Ali Abbas, [3]Noorulain

Article Details

Keywords: China AI Strategy; Informational Hegemony; Algorithmic Propaganda; Civil-Military Fusion; Ai Governance; Digital Authoritarianism; Cognitive Warfare; Ai Transparency; Global Standard-Setting; u.s.–China Rivalry

Izba Zaheer
PhD Scholar , Muslim Youth University, Islamabad. izbazaheerofficial@gmail.com

Dr. Ali Abbas
College of Politics and Public Administration, Henan Normal University Xinxiang China. 2024064@htu.edu.cn

Noorulain
MS in Peace and Conflict Studies, National University of Sciences and Technology (NUST), Islamabad. noorulain125@gmail.com

ABSTRACT

The advent of artificial intelligence (AI) has inaugurated a new arena of geopolitical competition, wherein informational dominance, historically held by the United States, is being increasingly contested. This paper explores how the People's Republic of China has constructed a strategically integrated AI ecosystem that fuses state, military, and private sector capabilities to systematically challenge U.S. informational hegemony. Leveraging doctrines of civil-military fusion, centralized governance, and global technology outreach, China is not only developing advanced AI capabilities but also exporting its algorithmic governance model to reshape global information flows and norms. We argue that the weaponization of algorithms, manifested through surveillance systems, disinformation operations, and infrastructure control, constitutes a form of cognitive warfare aimed at undermining liberal-democratic influence globally. Through a comparative analysis of the U.S. and Chinese AI ecosystems, and case studies of digital authoritarianism and influence operations, the paper illustrates how informational asymmetries are shifting in China's favor. This shift heralds a transition from a unipolar digital order to a contested multipolar system, with profound implications for global governance, cyber sovereignty, and democratic resilience. The paper concludes with policy recommendations for the U.S. and allied democracies to recalibrate AI strategy, enhance normative leadership, and safeguard the integrity of the global information environment.

DOI: Availability

INTRODUCTION

Artificial Intelligence (AI) has rapidly become a cornerstone of global power projection, with its transformative potential shaping everything from economic systems to military capabilities. In this unfolding landscape, China has emerged as a formidable actor, constructing a state-directed AI ecosystem that fuses military, industrial, and political power. This development directly challenges the long-standing informational hegemony of the United States, whose dominance in global knowledge production and digital governance has underpinned the liberal international order since the Cold War.

Unlike the decentralized, market-driven model of the United States, China's AI strategy is deeply embedded in statecraft through a doctrine of civil-military fusion and authoritarian digital control (Bareis & Katzenbach, 2022; Rikap & Lundvall, 2021). Key policy instruments, including the 2017 Next Generation AI Development Plan, the Digital Silk Road, and China's growing leadership in international standard-setting bodies, reflect a coherent vision to not only achieve AI supremacy but also export a model of algorithmic governance that reinforces illiberalism (Cheney, 2019; Pardesi, 2023; Wang, 2020).

At the same time, the United States faces a crisis of digital leadership. Internal fragmentation, weak AI regulation, and waning influence in international institutions are eroding its ability to maintain normative and infrastructural dominance in the global AI order (Taghizade & Ahmadov, 2025; Vázquez Rojo, 2023). As Chinese platforms like TikTok and Huawei extend their reach, Washington's informational primacy is being overtaken by what some have termed a "Digital Cold War" (Taghizade & Ahmadov, 2025).

This paper argues that China is effectively weaponizing algorithms, not just for domestic control but also for external influence. Through strategic integration of data, surveillance, and influence operations, China is actively reshaping the rules of the global digital game. By situating this AI ecosystem within broader theories of techno-nationalism and hegemonic transition, the study contributes a novel analytical framework for understanding how AI is recoding the balance of international power.

CONCEPTUAL FRAMEWORK AND LITERATURE REVIEW

HISTORICAL CONTEXT: FROM SILICON VALLEY SUPREMACY TO SINO-TECH REALIGNMENT

Throughout the post-Cold War period, the United States leveraged its economic clout, military superiority, and dominance over global digital infrastructure to sustain what scholars have termed

"informational hegemony" a system where norms, technologies, and platforms mirrored liberal democratic values (GL Network et al., 2023). U.S.-based corporations like Google, Facebook, and Amazon projected American cultural and informational values globally, backed by institutions such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the IEEE.

However, the past decade has witnessed the emergence of a formidable challenger: China. By embedding artificial intelligence (AI) into the core of its national rejuvenation strategy, China has positioned AI not merely as an economic growth driver, but as a tool of geopolitical disruption. At the center of this strategy is a fusion of technological innovation, authoritarian control, and international norm-building, which collectively aim to erode U.S. supremacy in the digital domain (Pardesi, 2023).

TECHNO-NATIONALISM AND CIVIL-MILITARY FUSION

China's AI policy architecture is inseparable from the concept of techno-nationalism, the fusion of national identity with technological development and strategic autonomy (Loo & Char, 2024). This approach manifests through several overlapping initiatives: The *Made in China 2025* policy, the *Next Generation AI Plan*, and the strategic application of *civil-military fusion*, which erases traditional boundaries between private firms, state entities, and the military-industrial complex (Zhao, 2025). These policies enable Beijing to mobilize data, capital, and talent toward dual-use AI systems that support both governance and military capabilities.

Unlike Western liberal democracies where corporate independence and ethical AI governance are frequently debated, China's governance model relies on centralized control and political loyalty. The Chinese Communist Party (CCP) actively channels AI development toward reinforcing ideological narratives, suppressing dissent, and promoting a highly orchestrated model of "cyber sovereignty" (Willnat, Tang, & Martin, 2025). This weaponization of AI for domestic stability and international projection distinguishes China's strategy from traditional Western innovation pathways.

INFORMATIONAL HEGEMONY: CONCEPT AND EROSION

Informational hegemony refers to a state's ability to dominate the global flow of information through infrastructure, platforms, and values. Historically, this hegemony has rested on U.S. ownership of key internet infrastructure, technological standards, and platform ecosystems. However, the emergence of China as a tech power challenges this architecture in both normative and operational terms (Mengüaslan, 2025).

China's export of AI-based governance systems, ranging from facial recognition and predictive policing to surveillance-enabled smart cities, has created a rival digital ecosystem particularly attractive to illiberal regimes (Thussu, 2025). This diffusion is facilitated through the Digital Silk Road**,** a subcomponent of the Belt and Road Initiative (BRI), which allows Beijing to provide infrastructural support to developing nations while simultaneously exporting its algorithmic governance norms.

Moreover, Beijing has increasingly contested Western control in international digital institutions. Its successful lobbying within the International Telecommunication Union (ITU) to normalize internet fragmentation, via the *New IP* protocol, and its growing presence in the Global South illustrate how China is building an alternative normative order (Su, 2022). This shift from a universalist to a multipolar internet severely undermines the U.S.'s ability to enforce global digital standards and ethics.

ALGORITHMIC SOVEREIGNTY AND GLOBAL NORM REENGINEERING

Beyond hardware and policy, the core of China's challenge lies in its model of algorithmic sovereignty, the use of proprietary algorithms not only for domestic social control but for global influence. While the U.S. promotes ethical and inclusive AI, Chinese platforms like TikTok, WeChat, and Alibaba Cloud serve as proxies for Chinese influence, enabling data extraction, narrative shaping, and disinformation campaigns outside its borders (Bjola & Kornprobst, 2023).

According to Can (2024), China's mobilization strategy treats AI as a resource, integrating algorithmic models with infrastructure projects and trade agreements. These efforts enable a high degree of influence in emerging markets while simultaneously creating dependencies on Chinese technology stacks. As algorithmic systems become embedded in governance processes abroad, China gains normative leverage**,** reshaping how states conceptualize privacy, surveillance, and political control.

Furthermore, China's strategic investments in semiconductors, AI chips, and cloud infrastructure show that this is not simply a passive diffusion of technology, it is a calculated reengineering of the digital world order (Su, 2022; Mengüaslan, 2025). Beijing's global AI strategy thus goes beyond technological leadership; it aims to redefine the ethical and institutional frameworks through which digital futures are governed.

COMPARATIVE GOVERNANCE MODELS: U.S. VS. CHINA

The contrast between U.S. and Chinese AI strategies is not merely institutional but epistemological. The United States emphasizes a liberal-democratic epistemology in which data

privacy, transparency, and accountability are essential. Governance is fragmented across agencies, with ethical AI often subordinated to market incentives and regulatory inertia (Milhaupt, 2025).

Conversely, China's governance logic prioritizes efficiency, control, and political alignment. Its AI strategy is coordinated across ministries, firms, and security organs, making it capable of deploying complex technologies at scale with remarkable speed (Pardesi, 2023). Hine and Floridi (2024) argue that Chinese governance embodies a "technocratic authoritarianism," wherein the legitimacy of the state is derived from its perceived technological prowess and capacity to deliver order. This divergence is crucial in shaping global AI norms. U.S.-based institutions have struggled to retain leadership in the face of China's systematic entry into global fora, offering low-cost surveillance infrastructure, digital diplomacy, and capacity-building programs to non-Western states. The hegemonic transition in AI governance thus appears not only probable but already underway.

TABLE 1: GOVERNANCE AND STRATEGIC COMPARISON – CHINA VS. UNITED STATES

Dimension	China	United States
Governance Model	Technocratic, centralized, state-controlled	Democratic, decentralized, private-sector-led
Policy Instruments	Made in China 2025, Next Gen AI Plan, Digital Silk Road	National AI Initiative, AI Bill of Rights
Data Regime	State-mandated access, surveillance-centric	Privacy-first, fragmented (GDPR-influenced)
Military Integration	Civil-Military Fusion	DARPA-led innovation partnerships
Norm Export	Cyber sovereignty, digital authoritarianism	Digital democracy, ethics-first AI norms
Infrastructure Influence	Huawei, BeiDou, Alibaba Cloud	AWS, Google, Starlink

IMPLICATIONS FOR GLOBAL ORDER

The implications of this strategic divergence are profound. First, informational multipolarity is becoming a structural feature of the international system, with the U.S. no longer the uncontested custodian of digital norms. Second, the diffusion of China's AI ecosystem among authoritarian and hybrid regimes suggests that algorithmic governance is becoming a tool of soft coercion, enabling

regimes to emulate China's control model without its economic capacity (Pardesi, 2023; Thussu, 2025).

Third, the erosion of U.S. hegemony creates governance vacuums in domains such as surveillance law, AI safety, and data localization. While Western alliances are attempting to counteract this trend through initiatives like the Global Partnership on AI (GPAI), their impact remains limited due to internal disunity and a lack of enforceable norms (Mengüaslan, 2025). Ultimately, as the global digital order splinters, a key question emerges: can liberal democracies formulate a compelling alternative to China's AI-centric authoritarianism, or will the future of information be defined by centralized, opaque, and strategically weaponized algorithms?

CHINA'S STRATEGIC AI ECOSYSTEM

China's strategic AI ecosystem is a deeply integrated architecture that brings together military modernization, surveillance infrastructure, international diplomacy, and technological standard-setting. At the heart of this ecosystem is the doctrine of civil-military fusion (CMF), which tightly integrates research institutions, commercial tech giants, and the People's Liberation Army (PLA) to leverage AI for both state control and global influence.

CIVIL-MILITARY FUSION: INSTITUTIONALIZING DUAL-USE INNOVATION

Civil-Military Fusion (CMF) is not a policy in isolation but a defining structural feature of China's AI ecosystem. Enshrined in the 14th Five-Year Plan and reinforced through the Next Generation Artificial Intelligence Development Plan**,** CMF mandates that civilian innovations be designed for military utility from inception (Manhas & GX, 2024). Under this framework, national champions like Huawei, SenseTime, and Hikvision are both commercial entities and strategic military partners.

As Sharma (2024) notes, CMF facilitates resource sharing between universities, state laboratories, and PLA research centers, creating a system where AI projects in facial recognition, drone swarming, and natural language processing are seamlessly transferred into military deployment. This convergence reflects Xi Jinping's broader vision of "informatized warfare," in which future conflicts will be won not only on land or sea, but in the algorithmic and cognitive domains.

In practice, this has enabled rapid development of autonomous weapons systems, unmanned aerial surveillance networks, and AI-assisted decision-making tools for battlefield command. Such developments raise critical concerns for global arms control, as China's opaque R&D ecosystem

blurs the lines between civilian and military applications (Papageorgiou, Can, & Vieira, 2024; Banerjee, 2023).

SURVEILLANCE INFRASTRUCTURE: DOMESTIC CONTROL, GLOBAL REPLICATION

One of the most consequential outputs of China's AI ecosystem is its mass surveillance architecture**,** which now encompasses facial recognition, biometric tracking, predictive policing algorithms, and social credit systems. These technologies, while primarily justified as tools for domestic stability, have been deployed in tandem with repressive policies in Xinjiang, Tibet, and among dissident populations (Mirrlees, 2024).

AI surveillance systems are supported by vast public-private data partnerships, where companies like Megvii and Yitu Technologies provide real-time surveillance feeds to municipal security bureaus. These capabilities are not only unmatched in scale but also form the basis of China's AI exports to other authoritarian-leaning states.

According to Banerjee (2023), Chinese firms have replicated this model abroad through "smart city" contracts in Africa, Southeast Asia, and Latin America, exporting not just hardware, but also algorithmic governance templates. The underlying goal is to establish infrastructural dependencies while normalizing China's model of digitally enhanced authoritarianism.

DIGITAL SILK ROAD: EXPORTING ALGORITHMIC GOVERNANCE

The Digital Silk Road (DSR)**,** a sub-initiative of the Belt and Road Initiative (BRI), serves as China's key channel for exporting AI capabilities. Originally envisioned as a strategy for ICT development in the Global South, the DSR has evolved into a geopolitical instrument, delivering fiber-optic cables, data centers, and e-governance platforms embedded with AI tools (Hussain, Imran, & Hussain, 2023).

Through DSR projects, China offers bundled packages, surveillance systems, cloud computing, and AI training programs, that are cost-competitive and politically appealing to non-Western regimes. Sharma (2024) observes that this bundling also includes the export of legal-technical standards favoring cyber sovereignty, thereby undermining the liberal, open internet paradigm championed by the United States and Europe.

A notable example is Ethiopia's partnership with ZTE and Alibaba Cloud to develop a centralized digital identity and payment system, effectively locking the country into China's technological orbit. This deepens dependencies and facilitates long-term data extraction and influence.

DIPLOMACY AND STANDARD-SETTING: AI GOVERNANCE WITH CHINESE CHARACTERISTICS

Parallel to its infrastructure efforts, China has become increasingly active in international AI diplomacy and standard-setting. In forums such as the International Telecommunication Union (ITU), China has advocated for technical protocols that facilitate state monitoring and internet fragmentation. These proposals, such as the "New IP" protocol, have raised alarm among digital rights groups and democratic states (Pardesi, 2023).

China's standard-setting strategy is rooted in the idea of governing AI globally through state sovereignty rather than multilateral liberalism. As Manning (2024) argues, Beijing's normative push focuses on reshaping global AI ethics from Western-style transparency and human rights toward state efficiency and social stability.

At the United Nations and other intergovernmental forums, Chinese diplomats have successfully rallied support from countries with similar political structures or dependency relationships. This creates a multipolar AI governance environment in which China's model of control gains legitimacy, particularly in the absence of unified Western alternatives.

China's strategic AI ecosystem is a symbiotic complex of domestic control mechanisms, military innovations, infrastructural exports, and diplomatic engagement. Through civil-military fusion, the regime blurs distinctions between civilian tech and strategic defense; through surveillance infrastructure, it perfects population control; through the Digital Silk Road, it exports technological and normative systems; and through AI diplomacy, it actively rewrites the global governance script. This ecosystem is not a reactive measure but a proactive geopolitical architecture designed to contest and ultimately supplant U.S. informational hegemony.

EROSION OF U.S. INFORMATIONAL HEGEMONY

The informational dominance historically enjoyed by the United States, rooted in its global media architecture, normative leadership in digital governance, and control over internet infrastructure, is increasingly under pressure from a strategic and systemic challenge: China's algorithmically-enabled statecraft. The weaponization of artificial intelligence, algorithmic propaganda, and global infrastructure influence have significantly shifted the balance of soft power and information sovereignty. This section analyzes four key drivers of this erosion: algorithmic propaganda, AI-powered infrastructure control, regulatory asymmetry, and declining normative leadership.

ALGORITHMIC PROPAGANDA AND EPISTEMIC ENGINEERING

One of the most potent instruments of China's digital strategy is its capacity to engineer narratives through algorithmic propaganda. Unlike classical propaganda reliant on state-owned media, China now leverages personalized content delivery systems, such as TikTok, WeChat, and news aggregators like Toutiao, to shape perceptions both domestically and globally.

These platforms operate using AI-enhanced content recommendation algorithms that can amplify state-approved narratives, suppress dissent, and subtly manipulate user engagement to align with Party objectives (Willnat, Tang, & Martin, 2025). This phenomenon, referred to as "epistemic hegemony" by Amundson et al. (2025), describes the systematic shaping of what populations believe to be true, achieved not through censorship alone but through the strategic curation of algorithmic exposure.

In international contexts, these tactics are deployed to blur the line between fact and fiction, flooding information ecosystems with distraction, distortion, and disinformation. For example, JLM Sánchez (2025) draws comparisons between China's digital influence campaigns and Cold War-era disinformation by authoritarian regimes, noting a shift from persuasion to disruption.

The consequences are dire: democracies that depend on open information flows are left vulnerable to coordinated manipulation, especially during critical periods such as elections and civil unrest (Gunnarsdóttir, 2024). This use of AI for cognitive influence has become a central component of China's broader strategy to undermine liberal consensus and disrupt Western political cohesion.

INFRASTRUCTURE CONTROL AND TECHNOLOGICAL LOCK-IN

Parallel to its algorithmic reach, China is consolidating informational influence through control of digital infrastructure**.** By exporting AI-integrated surveillance systems, cloud platforms, and mobile networks under the Digital Silk Road, China establishes long-term technical dependencies with developing countries. This infrastructure not only collects data but also shapes how information is filtered, monetized, and governed.

Taghizade and Ahmadov (2025) describe this strategy as part of a broader "techno-feudalist realignment," in which informational sovereignty is traded for technological access. These infrastructural arrangements serve as vectors for influence**,** embedding Chinese norms and technical standards in host countries' governance systems. Moreover, infrastructure agreements often include closed software ecosystems, creating what Xiao (2025) calls "algorithmic lock-in" a

condition where adopting nations become structurally tied to China's digital governance model and data flows.

This extends beyond physical networks. Chinese companies increasingly control core algorithmic patents, surveillance architectures, and biometric databases, allowing Beijing to scale its influence while gathering sensitive geopolitical intelligence under the guise of commercial expansion (Bazavluk & Kovalev, 2025).

REGULATORY ASYMMETRIES AND INSTITUTIONAL PARALYSIS IN THE U.S.

While China enacts increasingly precise algorithmic regulations tailored to its political goals, including state content filters, real-name policies, and predictive policing, the United States has been slow to respond with coherent countermeasures. The U.S. federal system, fragmented across agencies and legal jurisdictions, has produced regulatory inertia at a time when coordinated governance is essential.

Xiao (2025) notes that the asymmetry in governance is not merely institutional but ideological: while China regulates to enforce alignment, the U.S. debates regulation as a threat to freedom of expression. This mismatch gives China a strategic edge in controlling both domestic and foreign platforms while undermining U.S. credibility in digital rights advocacy.

The result is that U.S.-based platforms, although economically dominant, are normatively fragmented, vulnerable to both internal polarization and external interference. In contrast, China's platforms act as arms of statecraft, their alignment ensured by law, Party committees, and corporate compliance mechanisms.

DECLINING NORMATIVE POWER IN GLOBAL DIGITAL GOVERNANCE

Perhaps the most fundamental indicator of U.S. decline is its waning normative power in the global arena. While Washington was once the architect of internet freedom, net neutrality, and multistakeholder governance, China has aggressively promoted an alternative normative model centered on cyber sovereignty, algorithmic paternalism, and information discipline (Burchell et al., 2025).

China's growing bloc of sympathetic states, including Russia, Iran, Ethiopia, and parts of Southeast Asia, has endorsed these principles through forums like the United Nations Group of Governmental Experts (GGE) and the International Telecommunication Union (ITU). As Thussu (2024) argues, the "geopolitics of global communication" are shifting toward regional models of information control, with Beijing leading efforts to redefine sovereignty as absolute state control over data and discourse.

This is reinforced by China's strategic capture of standard-setting bodies, where it uses its commercial and diplomatic leverage to promote proprietary norms around AI ethics, cybersecurity, and cross-border data flows (Taghizade & Ahmadov, 2025). In contrast, the U.S. has struggled to mount a cohesive normative campaign, often hampered by domestic divisions and limited coalition-building in the Global South.

The erosion of U.S. informational hegemony is not the product of a single technological disruption, but the result of a multi-domain strategy by China, encompassing cognitive, infrastructural, legal, and normative terrains. By combining algorithmic propaganda, strategic infrastructure exports, regulatory asymmetries, and normative entrepreneurship, Beijing has systematically dismantled key pillars of U.S. digital influence.

What emerges is a fragmented digital world order, where influence is no longer monopolized by liberal democracies but contested through the strategic deployment of data, code, and networks. Unless countered through coherent policy, international collaboration, and ethical AI leadership, the United States risks becoming a legacy power in the domain it once dominated.

WEAPONIZATION OF AI IN PRACTICE

While China's AI strategy is deeply institutional and geopolitical in nature, its operational character is increasingly visible in the realm of hybrid warfare, algorithmic propaganda, and digital infrastructure dominance. These mechanisms represent the tactical translation of national policy into real-world applications that blur the boundary between peace and conflict. This section outlines how China has weaponized artificial intelligence in practical terms, using it as a multi-domain force multiplier for global influence and strategic disruption.

COGNITIVE WARFARE AND AI-ENHANCED DISINFORMATION CAMPAIGNS

China's deployment of AI-enhanced disinformation constitutes a powerful method of conducting cognitive warfare, a tactic focused on altering target audiences' perceptions, behaviors, and decision-making processes. AI enables the automation of botnets, content amplification, and targeted narrative shaping at scale. Unlike earlier information operations, today's campaigns use natural language generation and real-time sentiment analysis to dynamically tailor content to manipulate emotions and sow distrust.

According to Singh (2024), China has tested these methods extensively in Taiwan, where AI-generated content has been used to disseminate confusion and pro-Beijing sentiment, particularly around elections and national defense debates (Singh, 2024). The campaigns often rely

on deepfake technology and synthetic personas, leveraging platforms like TikTok and WeChat for mass-scale influence in Southeast Asia.

Similarly, Matsehora (2024) describes how Chinese and Russian influence operations overlap through coordinated disinformation campaigns, where algorithms detect divisive issues and flood digital spaces with engineered content to sabotage democratic coherence (Matsehora, 2024).

INFRASTRUCTURE DOMINANCE AND STRATEGIC DIGITAL ENTRAPMENT

Beyond content manipulation, China has weaponized AI by embedding it in critical digital infrastructure worldwide. Through initiatives like the Digital Silk Road and cloud partnerships with authoritarian-leaning regimes, Beijing exports AI surveillance systems that serve dual purposes: helping regimes entrench control while giving China long-term influence over foreign data and communication networks.

Saccone (2024) highlights how Huawei's 5G infrastructure includes AI backdoors designed for real-time traffic analysis and content filtering, offering the Chinese state situational awareness across foreign cyber-terrain (Saccone, 2024). The strategic goal is not only commercial dominance but techno-political entrapment, where states become reliant on opaque AI ecosystems engineered in Beijing. These dependencies undermine local data sovereignty, allowing China to extend its algorithmic governance model under the guise of economic partnership and technological modernization.

AI IN HYBRID WARFARE AND POLITICAL DESTABILIZATION

AI also plays a direct role in hybrid warfare, where conventional and irregular tactics are blended with digital disruption. Chinese strategies increasingly involve gray-zone operations, such as AI-enabled cyber-attacks, infrastructure probing, and AI-powered influence ops targeting military cohesion or civic trust in adversary nations.

Correal (2025) analyzes how AI has transformed cyberwarfare into a persistent low-intensity conflict environment, where adversaries can target logistical systems, elections, or media without kinetic escalation (Correal, 2025). This is particularly evident in Southeast Asia and parts of Central Asia, where China's AI assets are used to erode strategic confidence in Western-aligned states.

Chin (2023) contextualizes this within a broader Western military view of "informational battlespaces," where controlling perception and communication rhythms is as important as

physical territory (Chin, 2023). Chinese cyber-AI tools serve as precision-guided information weapons in this domain, blurring the lines between peacetime engagement and active hostilities.

TIKTOK AS A CASE STUDY: FROM ENTERTAINMENT TO COGNITIVE VECTOR

A particularly salient example of China's algorithmic influence is TikTok, owned by Byte Dance, whose recommendation algorithm has become a focal point in debates about algorithmic bias, content steering, and national security. Unlike Western platforms, which are driven by ad-centric engagement metrics, TikTok's algorithm is believed to reflect geopolitical priorities of the Chinese state through subtle manipulations of virality and visibility.

Wright (2021) and Singh (2024) both note that TikTok's moderation systems differ dramatically by region, with pro-PRC narratives downranking critical content in foreign markets and suppressing pro-democracy messaging within diaspora communities (Wright, 2021; Singh, 2024). This selective exposure contributes to an environment of perceptual asymmetry, where younger audiences are incrementally aligned with China's soft power goals.

While U.S. legislation has sought to counter this influence, the complexity of **algorithmic sovereignty** and content transparency challenges the ability of liberal democracies to effectively regulate foreign platforms operating under opaque AI logic.

SUMMARY OF AI WEAPONIZATION VECTORS

Weaponization Vector	Operational Example	Strategic Impact
Disinformation & Deepfakes	AI-generated political content in Taiwan and U.S.	Electoral destabilization, trust erosion
Infrastructure Surveillance	Huawei 5G, Hikvision smart cities	Long-term data access, strategic vulnerability
Hybrid Warfare (Cyber-AI Ops)	Military targeting disruption, social cohesion sabotage	Persistent gray-zone aggression
Algorithmic Propaganda	TikTok virality manipulation, censorship in diaspora platforms	Cognitive alignment, soft power projection

China's weaponization of AI is not merely conceptual, it is operational, transnational, and asymmetric. Through disinformation, infrastructure dominance, and algorithmic manipulation, Beijing is deploying AI as an instrument of digital coercion and strategic subversion. These applications represent an evolved threat landscape, where traditional deterrence models fail to address persistent, low-visibility AI-enabled operations.

As this paradigm of algorithmic warfare expands, it raises urgent questions for AI governance, international law, and strategic resilience in democracies. Future conflict may be decided less by tanks and missiles than by whose algorithm shapes perception faster, deeper, and more invisibly.

POLICY RECOMMENDATIONS AND COUNTERMEASURES

The intensifying strategic rivalry between the United States and China in the AI domain has catalyzed a pressing need for a coherent, multilateral response to the weaponization of artificial intelligence. China's approach, marked by authoritarian algorithmic governance, opaque surveillance exports, and influence over infrastructure, has exposed structural vulnerabilities in the liberal international order. This section offers four key policy recommendations: (1) strengthening multilateral AI governance; (2) countering infrastructural dependence; (3) institutionalizing algorithmic transparency and standards; and (4) building democratic resilience through strategic technological alignment.

STRENGTHENING MULTILATERAL AI GOVERNANCE AND NORM LEADERSHIP

To counteract China's normative expansion in global standard-setting bodies like the International Telecommunication Union (ITU), the U.S. and its allies must reinvest in multilateral AI governance frameworks that reaffirm democratic values. Rebolledo (2025) argues that international cooperation grounded in shared principles of transparency, fairness, and accountability is essential to reducing the asymmetry between authoritarian and democratic AI regimes (Rebolledo, 2025).

Coalitions such as the Global Partnership on Artificial Intelligence (GPAI) and the OECD AI Principles should be expanded to include Global South partners, offering both technical support and normative leadership as alternatives to China's cyber-sovereignty model. Ishkhanyan (2025) stresses the urgency of reconciling digital sovereignty with international cooperation, proposing a "digital federalism" approach to preserve local control without ceding ethical leadership to authoritarian states (Ishkhanyan, 2025).

REDUCING STRATEGIC DEPENDENCE ON AUTHORITARIAN INFRASTRUCTURE

Given China's growing presence in global ICT and AI-enabled infrastructure, through initiatives like the Digital Silk Road, U.S. policy must prioritize strategic technological decoupling and infrastructure diversification. This involves offering alternatives to Huawei, ZTE, and Alibaba Cloud by subsidizing trusted tech providers and investing in open-access digital systems.

Lucero (2025) proposes incentives for U.S. firms to enter underserved markets with interoperable AI platforms, allowing partner countries to avoid dependence on authoritarian surveillance

architectures (Lucero, 2025). A comprehensive strategy would also include cyber capacity-building in developing countries to reduce the influence of opaque foreign systems.

ESTABLISHING BINDING FRAMEWORKS FOR ALGORITHMIC TRANSPARENCY

The erosion of U.S. informational influence is in part due to regulatory asymmetries that leave democratic societies vulnerable to opaque AI systems. Addressing this requires harmonizing national and international legal frameworks that enforce algorithmic transparency, particularly in recommender systems, biometric tracking, and autonomous decision-making.

Radanliev (2025) and Lund et al. (2025) both advocate for mandatory algorithmic disclosure laws**,** independent auditing regimes, and transparency-by-design standards (Radanliev, 2025; Lund et al., 2025). These measures are essential not only for public trust but also to outcompete China's opaque AI offerings on normative grounds. The U.S. and EU can jointly develop "algorithmic non-proliferation standards" paralleling arms control protocols to limit the export of unethical AI systems and offer transparency-enforcing alternatives to the international market.

ENHANCING DEMOCRATIC RESILIENCE THROUGH PUBLIC-AI ALIGNMENT

Finally, the durability of liberal democracy in the AI age depends on aligning emerging technologies with public values. This includes proactive investment in **civic** AI education, public-interest algorithm development**,** and participatory digital governance. Hine (2024) and Mukherjee (2025) emphasize that building resilient democratic ecosystems requires not only regulatory safeguards but also technological innovation rooted in public legitimacy (Hine, 2024; Mukherjee, 2025).

Open-source AI models, ethical development frameworks, and domestic data stewardship practices can help rebuild institutional trust and differentiate democratic digital governance from China's model of centralized control. Additionally, democratic states should collaborate on a "resilience index" for AI technologies, identifying vulnerabilities to disinformation, surveillance misuse, or regulatory arbitrage.

The future of global AI governance, and by extension, the ideological character of the 21st-century international order, hinges on whether liberal democracies can formulate a coherent, enforceable, and value-driven AI strategy. China's systematic use of AI as a tool of surveillance, soft coercion, and norm diffusion demands an equally strategic response. By building coalitions, shaping standards, enhancing transparency, and fortifying democratic resilience, the United States

and its allies can preserve their normative leadership and prevent authoritarian consolidation in the algorithmic age.

CONCLUSION

This study has examined how China's strategic artificial intelligence (AI) ecosystem, shaped by civil-military fusion, surveillance exports, algorithmic propaganda, and infrastructural dominance, has emerged as a systemic challenge to U.S. informational hegemony. Unlike the open, market-driven innovation ethos historically led by the United States, China's AI strategy is state-orchestrated, norm-shifting, and intentionally disruptive. It is not only a technological program but a geopolitical doctrine of algorithmic statecraft.

Through its weaponization of AI, China is operationalizing a new form of hybrid power: projecting influence without kinetic warfare, controlling information ecosystems without occupying territory, and reshaping global norms without conventional diplomacy. Its strategies have proven effective in blurring lines between civilian and military tech, exporting authoritarian surveillance systems, and exploiting regulatory asymmetries in liberal democracies.

Meanwhile, the U.S. and its allies face a strategic inflection point. Without coherent, value-driven AI governance, liberal democracies risk ceding not only technological dominance but also the epistemic legitimacy required to shape global perceptions, regulations, and digital ethics. The erosion of informational hegemony manifests in weakened normative power, fragmented cyber alliances, and growing vulnerabilities to authoritarian cognitive warfare.

The broader implication is that the struggle over AI is not just technical it is civilizational. It involves competing visions of how societies should be organized, how decisions should be made, and how truths should be constructed. China's model centers the state, secrecy, and surveillance; the liberal democratic model must center the public, transparency, and trust.

If the 20th century was defined by nuclear deterrence, the 21st will be defined by algorithmic governance. Whichever system, authoritarian or democratic, more effectively governs the algorithm will command not just markets or militaries, but the minds and moral structures of the digital age.

REFERENCES

Amundson, J., Forgacs, L. D. T. H., Kindarji, V., & Korotaev, R. (2025). *Beyond Disinformation.* University of Toronto.

Banerjee, M. A. (2023). *Collaboration in AI Between China & Its Partners: A Prognosis.* CENJOWS.

Bareis, J., & Katzenbach, C. (2022). Talking AI into being: The narratives and imaginaries of national AI strategies and their performative politics. *Science, Technology & Human Values, 47*(4), 642–673. https://doi.org/10.1177/01622439211030007

Bazavluk, S. V., & Kovalev, A. A. (2025). Information warfare in a multipolar world. *RUDN Journal of International Relations, 25*(2), 236–250. https://doi.org/10.22363/2313-0660-2025-25-2-236-250

Bjola, C., & Kornprobst, M. (2023). *Digital International Relations*. Taylor & Francis. https://doi.org/10.4324/9781003437963

Burchell, K., Ross, J., Tolz, V., Yu, S., & Amundson, J. (2025). *Beyond Disinformation: Identarian Narratives and Authoritarian Marketcraft*. University of Toronto.

Can, M. (2024). Artificial intelligence as a resource: An appraisal of China's mobilization and extraction strategies. https://repositorium.sdum.uminho.pt/handle/1822/93221

Cheney, C. (2019). *China's Digital Silk Road: Strategic technological competition and exporting political illiberalism*. Pacific Forum.

Chin, W. (2023). *The Western Military Vision of Future War*. Bristol University Press.

Correal, K. J. (2025). *AI and strategic power: An analysis of AI in cyberwarfare*. Eastern Michigan University.

Ehdaee, A. (2024). The impact of 21st-century emerging technologies on the shift of power in the international system. *Law, Society and Developmental Affairs, 3*(2). https://doi.org/10.61838/kman.lsda.3.2.13

GL Network, Berghofer, J., Futter, A., Häusler, C., & Hoell, M. (2023). *The Implications of Emerging Technologies in the Euro-Atlantic Space*. Springer.

Gunnarsdóttir, G. B. (2024). *From Persuasion to Disruption: Russian Influence and Democratic Vulnerabilities in the 2024 US Election*. Skemman.

Hine, E., & Floridi, L. (2024). Artificial intelligence with American values and Chinese characteristics. *AI & Society*. https://link.springer.com/article/10.1007/s00146-022-01499-8

Hussain, F., Imran, A., & Hussain, Z. (2023). Infrastructure development for the Digital Silk Road and its implications for China. *Asia-Pacific Social Science Review*.

Ishkhanyan, A. (2025). The sovereignty-internationalism paradox in AI governance: Digital federalism and global algorithmic control. *AI and Ethics*. https://link.springer.com/article/10.1007/s44163-025-00374-x

Khan, D., Mehmood, W., & Shah, H. (2025). Hybrid warfare between India and Pakistan: Cyber threats, disinformation, and strategic stability. *RC Archive*.

Loo, B. F. W., & Char, J. (2024). *Strategic Currents: China and U.S. Competition for Influence*. Palgrave Macmillan.

Lucero, K. (2025). *Artificial Intelligence Regulation and China's Future*. Columbia Academic Commons. https://academiccommons.columbia.edu/doi/10.7916/gt4n-1421/download

Manhas, N. S., & GX, H. Y. (2024). China's military-civil fusion from Mao to Xi: A long roadmap. *Journal of Political Science*.

Manning, C. (2024). *Targeted and Precise: Innovation Versus Regulation in the Critical Technology Sector*. Newlines Institute.

Matsehora, P. (2024). *Understanding AI Arms Race*. Charles University Repository.

Mengüaslan, H. (2025). Offensive mercantilism and the crisis of liberal international order. https://dergipark.org.tr/en/pub/adusobed/issue/92578/1677331

Milhaupt, C. J. (2025). *Corporate Governance in an Era of Geoeconomics*. SSRN. https://ssrn.com/abstract=4888623

Mirrlees, T. (2024). *The US and China's Digital Tech War: A New Rivalry*. ResearchGate.

Mukherjee, B. N. (2025). *Navigating AI Governance: National and International Legal and Regulatory Frameworks*. IGI Global. https://www.igi-global.com/chapter/navigating-ai-governance/382021

Papageorgiou, M., Can, M., & Vieira, A. (2024). *China as a Threat and Balancing Behavior in Emerging Technologies*. Springer.

Pardesi, M. S. (2023). *Sino-American Rivalry and the Framework for AI Governance*. World Scientific. https://doi.org/10.1142/13726

Radanliev, P. (2025). AI ethics: Integrating transparency, fairness, and privacy in AI development. *Applied Artificial Intelligence*. https://www.tandfonline.com/doi/pdf/10.1080/08839514.2025.2463722

Rebolledo, V. G. (2025). Impact of the artificial intelligence on international relations: Towards a global algorithms governance. *UNISCI Discussion Papers*, 67. https://www.unisci.es/wp-content/uploads/2025/01/UNISCIDP67-1GARRIDO.pdf

Rikap, C., & Lundvall, B. Å. (2021). AI policies and politics in China and the US between techno-globalism and techno-nationalism. In *The Elgar Companion to Innovation and Knowledge Creation*.

Saccone, G. (2024). *A Japanese Perspective of the China Threat in Cyberspace*. Lund University.

Sánchez, J. L. M. (2025). *How Disinformation Ruins Public Diplomacy: Unfair Competition*. Routledge.

Schneider Rasador, G., & Moreira Cunha, A. (2025). The new security grey zone: Export controls, emerging technologies and US-China technological rivalry. *The Pacific Review*. https://doi.org/10.1080/09512748.2025.2470222

Sharma, M. (2024). *Building China into a Cyber Superpower: Desires, Drivers, and Devices*. Taylor & Francis.

Singh, S. (2024). *Cognitive Warfare Capabilities and Threat to Southeast Asia*. CORE.

Singh, N. K., Jash, A., & Nanjappa, Y. (2025). Navigating the nexus: Geopolitical, international relations and technical dimensions of US-China cyber strategic competition. *Cogent Social Sciences*. https://doi.org/10.1080/23311886.2025.2499171

Su, A. (2022). The promise and perils of international human rights law for AI governance. https://search.informit.org/doi/abs/10.3316/informit.917575001580715

Taghizade, E., & Ahmadov, E. (2025). Techno feudalism and the new global power struggle. *International Journal of Research and Innovation in Social Science*, *9*(2), 1144–1170. https://doi.org/10.47772/IJRISS.2025.9020093

Thussu, D. (2024). *Changing Geopolitics of Global Communication*. Routledge.

Thussu, D. K. (2025). China's deepening digital presence in the global South. *The Round Table*. https://doi.org/10.1080/00358533.2025.2514777

Vassallo, K. J. (2025). *Great Power Competition Between the US and China in South America*. Johns Hopkins University Repository.

Vázquez Rojo, J. (2023). *The US-China Race for Economic Hegemony in the World-System: Individual and Structural Power from a Network Perspective*. Universidad Camilo José Cela.

Wang, D. (2020). *Reigning the Future: AI, 5G, Huawei, and the Next 30 Years of US-China Rivalry*.

Willnat, L., Tang, S., & Martin, J. A. (2025). *Digital Media and Politics in China*. Routledge.

Wright, N. D. (2021). *Intelligent Biology: The Future Character of Information in Strategy*. DTIC.

Xiao, J. W. (2025). *Three Papers on the International Political Economy of AI*. Columbia University. https://academiccommons.columbia.edu/doi/10.7916/bdmh-qj68/download

Zhao, S. (2025). *The Making of China's Artificial Intelligence and Cybersecurity Policy*. Palgrave Macmillan.