Proceedings of ICILLP 2025 Symposium: Property Law and Blockchain Applications in International Law and Legal Policy
DOI: 10.54254/2753-7048/2025.LD29690

Global Governance of Artificial Intelligence and Great Power Rivalry: The Conflict Between Market Logic and Security Logic

Aiyu Yang

College of St Hild and St Bede, Durham University, Durham, United Kingdom
frjr72@durham.ac.uk

Abstract. Artificial intelligence is reshaping the global economy, security, and governance, with the United States and China holding dominant positions. Their rivalry reflects the conflict between market logic, emphasizing efficiency and innovation, and security logic, prioritizing risk management and strategic control. Both powers exercise strong normative influence in multilateral platforms, yet domestic incorporation of norms remains limited. Market rationality accelerates diffusion of technologies such as Large Language Models but aggravates risks of inequality, whereas security rationality mitigates threats but constrains cooperation. Divergences appear in domains including quantum AI, data governance, and military–civil fusion, where strategic confrontation delays regulatory adaptation. Balanced and inclusive frameworks are required for effective global governance, as highlighted by initiatives such as the Bletchley Declaration, with institutions like the United Nations serving a bridging role. Progress depends on cultivating reciprocal trust, avoiding zero-sum dynamics, and achieving mutually beneficial outcomes in AI governance. The persistence of these tensions illustrates the structural challenges inherent in aligning technological development with coherent global regulatory mechanisms.

Keywords: Artificial intelligence, US–China rivalry, market logic, security logic, global governance

1. Introduction

With the rapid rise of the artificial intelligence technology, it has undoubtedly impacted the worldwide economy, security, and society. In total, the AI market still expanding in existence, in which the United States and China are at the top positions. The estimated value of the global AI market crossed 150 billion dollars in the year 2023 and it is expected to reach 1.8 trillion dollars by the year of 2030, where 60% plus is contributed by United states and China [1]. However, this tool's double-edged nature has created demands for international governance: on one side is AI that fuels economic growth and innovation and, on the other is AI that increases the risks of surrendering autonomy and possible abuses. The U.S. and China, two of the world's leading players in AI research and development, have increasingly come to be considered an essential part of the governance competition.While the United States elevates the importance of AI with bodies such as the National Security Council, China ranks AI as one of the top areas in its Fourteenth Five-Year Development Plan. This competition expands beyond the realm of technology to include who has authority in establishing norms and framing the international discourse; that itself is indicative of the underlying conflict between market logic, oriented toward efficiency and profit, and security logic, oriented toward the avoidance of threats and the preservation of national interests.

This study focuses on examining how the US-China rivalry exemplifies the tension between market and security logics in the evolution of AI, with market logic emphasizing efficiency and economic growth driven by AI industrialization, while security logic emphasizes prevention and management through vigilance against the potential militarization of AI. It also addresses the broader issues of how great powers exercise norm-setting capacity—for instance, the United States through G7 and OECD initiatives and China through the Belt and Road Initiative and United Nations mechanisms—how international norms are incorporated into domestic legal frameworks, such as attempts to translate AI ethics guidelines into national legislation despite cultural barriers to standardization, and how the lag between technological advancement and regulatory response becomes manifest.

2. Literature review

Numerous studies have addressed the global challenges associated with AI regulation. The global nature of AI should call forth the need for multilateral structures, but geopolitics challenges coalescence of agreement. The discourse can be divided into three types: the deconstructions of the U.S.–China conflict, the comparisons between different governance structures, and the research into the norm-shaping.

One line of research has focused on the strategic rivalry between China and the United States in the field of AI, particularly in global arenas of technical standardization, where the United States underscores its interpretation of democratic values derived from Western narratives, while China foregrounds cyber sovereignty as a countervailing principle. According to Johnson, this competition should not be understood as zero-sum; instead, it manifests through overlapping memberships and raises the risk of fragmenting global governance [2]. Imbrie et al. argue that the bidirectional dependence between China and the United States in AI supply chains has generated deep mutual distrust [3]. On the U.S. side, concerns are heightened that Chinese actors may exploit U.S. hardware for AI computation, given the extensive entanglement of companies across the bilateral chip manufacturing supply chain. Conversely, China worries that U.S. firms might employ foreign-developed algorithms to process or store Chinese data, which could expose them to risks of surveillance or retaliation. Furthermore, prior research questions the "AI Cold War" framing of China–US relations and contends that geoeconomic dynamics heighten techno-spatial competition [4]. Zeng argues that although the United States and China share concerns about certain AI-related risks, such as existential threats, they diverge significantly in their regulatory approaches [5]. The United States advocates for an open network and emphasizes its interpretation of democratic and multistakeholder approaches, whereas China supports UN-negotiated institutional regulation and prioritizes fairness and equality for developing nations.

Another strand of literature examines the tension between market and security logics. Market logic accelerates the commoditization of AI, exemplified by the development of Large Language Models(LLMs), whereas security logic drives regulatory oversight such as U.S. export bans on China and China's data security measures. The dual-use nature of AI further exacerbates frictions, as both sides accuse each other of vulnerabilities in their supply chains [6]. Brynjolfsson et al. argue that market logic drives global labour division while remaining largely indifferent to the side effects of joblessness and social inequality [7]. Kania points out that security logic is oriented around strategic dominance, with the United States incorporating AI into warfare under the “third offset strategy” and China advancing Military–Civil Fusion (MCF) [8]. Creemers observes that hostilities emerge in the regulatory domain, citing the U.S. “offshore balance of power” policy—implemented through immigration constraints and trade restrictions such as the “fair and reciprocal trade” tariffs—and China’s “technological development blueprint,” which has curtailed access to foreign technology, expanded the entity list, and tightened data outflow through the Data Security Law [9].

A further body of work highlights the role of great-power normative influence. The United States promotes its interpretation of democratic norms through alliance formations, while China exerts influence via the Belt and Road Initiative (BRI) and the United Nations. Standards venues such as the OECD, G20, ITU, and ISO have become prominent arenas for agenda-setting. Mokry debates China’s “Global AI Governance Initiative” with a focus on sovereignty-based modality contrasted against the U.S. multi-stakeholder model [10]. A further body of work highlights the role of great-power normative influence.

Previous studies have shown that governance incongruity between China and the United States persists, with a market-oriented U.S. and a security-focused China generating frictions and making norm-setting the core of contention. While the existing literature is abundant, it lacks in-depth analysis of how the mismatch between technological advancement and regulatory response is manifested; this paper seeks to address that gap.

3. Theoretical framework: the conflict between market logic and security logic

According to market logic, AI is seen as a driver of the economy and thus focused on creativity, competition, and geographic division of labor. In the US, the Silicon Valley ecosystem is relied upon, and in China, data advantages such as mobile payments and monitoring systems are leveraged to incentivize applied research. Market logic promotes the diffusion of technology but overlooks externalities such as unemployment and social inequality [11]. For instance, US.Most AI investments come from the private sector where Venture Capital(VC) raised $50bn in 2023 to develop AI application such as ChatGPT [12]. Meanwhile, the Chinese government uses public subsidies to realize AI in commerce and transport where its market share is 70% in Asia.On the other hand, market rationality fosters chaotic competition, for example, data breach and algorithmic fueling of social divisions [13].

China and the United States both securitize the AI question—the U.S. by way of a “disentanglement” strategy and China by way of blurring the distinction between MCF. The divide is seen in the control of dualuse technology; the United States fears connections between the Chinese military and companies, whereas China sees U.S. limitations as imperialism. As a case in point, the U.S. Export Control Reform Act limits the export of AI technologies to China, while China responded with “Unreliable Entities List” as counterattacks. Such a reasoning strengthens sovereignty protection, but it may inhibit the world collaboration.

Security logic fosters conflict while market logic drives cooperation, in global governance. I In the U.S.–China conflict, security prevails in the United States through measures such as entity lists, whereas China seeks to balance market diffusion with localization, resulting in misalignments that further widen governance gaps [14]. This divergence reflects differing payoff logics between cooperation and competition. Empirically, U.S.–China AI patent conflict exemplifies this: the U.S. accuses China of intellectual property theft, and China accuses the U.S. of tyranny. Besides, Anderljung et al. characterize that out-of-control AI risks – particularly scenarios of uncontrollable

AI escalation – amplify the force of security-dominant logic and narrow the scope of market innovation [15].

The inspection of the system leads us to conclude that Sino-American relations are enmeshed in a deconstructionist logic: markets drive diffusion and neglect hazards, while security constraints combat threats and suppress efficiency. The solution requires balancing the two.

4. The Sino-U.S. game in global AI governance

The motive of this Sino-U.S. AI confrontation is technological domination. The U.S. is market-oriented, and China is powered by state-owned companies. Correspondingly, competition between China and the United States can also be observed in areas such as talent and data. The United States has constrained China through sanctions such as those on Huawei and SenseTime, and China has responded by advocating for autarky through measures like indigenous chip fabrication [6]. This inimical rapport extends to global bazaars: China disseminates technology via the Belt and Road Initiative, and the U.S. forges democratic coalitions in rejoinder.

China and the U.S. governance models also differ significantly: the U.S. places emphasis on multi-stakeholder models, while China adopts a state-guided approach. The misalignment manifests in support of U.N. resolutions, but differences also include weaponised AI. China prioritizes justice, the U.S.focuses on geopolitical security, which hinders consensus [5]. The divergence may give rise to a multi-polar management landscape, which in turn could heighten global risks related to the loss of autonomous control of AI or the emergence of harmful practices [16].

The leading countries China and United States have powerful persuasion capabilities. The U.S. advances governance approaches through platforms such as the OECD and G20, while China, in stewardship roles at organizations like the ITU and ISO, promotes a sovereignty-based modality. China’s “China Standards 2035” sets out a vision for international standards, while the U.S. aligns with allies such as the EU and Japan to counter it. China’s current influence is rooted in normative principles rather than natural resources, and it leverages partnerships with rising powers and Global South cooperation frameworks to enhance its role in international affairs.

At the national level of rules, existing frameworks such as AI ethics guidelines need to be adapted into domestic contexts. While the U.S. “Blueprint for an AI Bill of Rights” introduced in 2022 incorporates democratic principles aligned with Western value systems, China’s “Ethical Norms for the New Generation of AI” issued in 2021 focuses on social harmony. Variability in adoption is rooted in cultural differences, as the US emphasizes personal privacy while China values public security, resulting in nonuniform implementation of principles [17]. Conflicting U.S.–China dynamics accelerate regulatory fragmentation, leading to the coexistence of distinct regional frameworks, such as the EU’s General Data Protection Regulation(GDPR) and China’s Data Law [18].

All in all, the U.S.-China dynamics reveal divergences in governance approaches: the balance between market and safety generates differing narratives, norm-making unfolds as a process of contestation, and the risk of fragmentation poses challenges to international relations.

5. The contradictions between technological development and norms

Machine learning is advancing rapidly, through hybrids like quantum computing and biology. The US and China dominate, with China leading in quantum communication exemplified by the Micius satellite, while the US leads in computation. Policies have a hard time keeping up with maturation when LLMs raise challenges for surveillance. Differences in data governance approaches may affect algorithmic efficacy, while U.S. export controls place constraints on the global flow of innovation.

Technological strides are outpacing regulation, as AI risks such as AGI necessitate proactive governance, yet U.S.–China discordances slow the development of regulatory frameworks [15]. For exemplar, quantum AI could fracture encryption; security logic impels restraints but represses market utilizations. China's "quantum leap" initiative has channeled tens of billions, and the US Quantum Internet endeavor counters it. Conflicts emerge in data governance, as China's Personal Information Protection Law of 2021 highlights localized data while the US CCPA of 2018 focuses on transborder flows, and the latter creates a world data walled garden [18].

Arms Race Escalation arises from the US Defense AI Strategy of 2018, the need for Ethics Assessment, and the uncertainty between military uses and civilian ones caused by China's civil–military fusion. Risks of Dual Use for misuse of military AI drones in accordance with international treaties, whose implementation, in the face of conflicts, US–China hostilities have been impeding. The supply chain frictions brought to the fore by the COVID-19 pandemic have been attributed to a certain degree to the United States and China, blaming each other for having made themselves dependent upon one another.

However, an equilibrium between innovation and regulation is necessary, with multilateral structures to address risks, although differences between the U.S. and China make the process complex. For example, the 2023 Bletchley Declaration committed signatory states to cooperate on the safe design, deployment, and evaluation of "frontier AI" while recognizing their national approaches might differ, but its implementation has remained partial in practice due to unresolved disagreements over risk definitions, safety standards, and the scope of oversight [19]. This technology–policy misfit ultimately stems from the tension between market acceleration and security constraints.

6. Conclusion

AI regulation remains shaped by the broader U.S.–China technological rivalry, in which the interplay of market-driven efficiency and security-driven controls has been most visible. Both powers exert strong normative influence in international arenas, yet domestic incorporation of global norms remains limited. Market rationality stimulates innovation but simultaneously generates systemic risks, whereas security rationality seeks to mitigate dangers but often constrains collaboration. These divergent logics contribute to persistent fragmentation in governance [14]. During norm-setting processes, U.S. alignment with coalitions and China's emphasis on sovereignty-based frameworks generate competing pressures, leaving institutional development constrained [5]. Even in areas such as quantum AI, where technological breakthroughs outpace existing frameworks and require multilateral responses, strategic confrontation slows the establishment of balanced mechanisms [15].

Looking ahead, constructive channels such as the US–China AI Safety Dialogue in 2024 illustrate that dialogue is possible when focused on catastrophic risks. Multilateral initiatives, exemplified by the Bletchley Declaration in 2023, highlight the potential for international coordination on the safe development and deployment of frontier AI, although differences in national approaches have so far limited comprehensive implementation. Global governance will therefore require an inclusive framework, where institutions such as the United Nations play a bridging role. Ultimately, progress depends on cultivating reciprocal trust, avoiding zero-sum dynamics, and building pathways toward collaborative and mutually beneficial outcomes.

References

[1] Statista (2024). Outlook for Artificial Intelligence worldwide. Retrieved from https: //www.statista.com/outlook/tmo/artificial-intelligence/worldwide

[2] Sullivan, R. (2021). The U.S., China, and Artificial Intelligence Competition Factors. China Aerospace Studies Institute.

[3] Imbrie, A., Kania, E. B., & Laskai, L. (2020, January). The Question of Comparative Advantage in Artificial Intelligence: Enduring Strengths and Emerging Challenges for the United States. Center for Security and Emerging Technology.

[4] D Heeks, R., & He, Y. (2024). Analysing the US–China "AI Cold War" Narrative. Centre for Digital Development Working Paper No.110, University of Manchester. Retrieved from https: //www.researchgate.net/publication/385206168_Analysing_the_US-China_AI_Cold_War_Narrative

[5] Cheng, J., & Zeng, J. (2023). Shaping AI's future? China in global AI governance. Journal of Contemporary China, 32(143), 794–810.

[6] U.S.-China Economic and Security Review Commission. (2024). Annual Report to Congress. https: //www.uscc.gov/sites/default/files/2024-11/2024_Annual_Report_to_Congress.pdf

[7] Brynjolfsson, E., Rock, D., & Syverson, C. (2017). Artificial Intelligence and the Modern Productivity Paradox: A Clash of Expectations and Statistics. NBER Working Paper No. 24001. https: //www.nber.org/papers/w24001

[8] Kania, E. B. (2017). Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power. Center for a New American Security. https: //www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power

[9] Creemers, R. (2021). China's Emerging Data Protection Framework. SSRN. https: //ssrn.com/abstract=3964684

[10] Mokry, S. and Gurol, J. (2024) Competing Ambitions regarding the Global Governance of Artificial Intelligence: China, the US, and the EU. Global Policy, 15(5), 955–968. https: //doi.org/10.1111/1758-5899.13444

[11] Autor, D., Dorn, D., Katz, L. F., Patterson, C. and Van Reenen, J. (2020) The Fall of the Labor Share and the Rise of Superstar Firms. Quarterly Journal of Economics, 135(2), 645–709.

[12] CB Insights. (2024) State of AI Report. Retrieved from https: //www.cbinsights.com/research/report/ai-trends-2024/

[13] Zuboff, S. (2019) The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs.

[14] Stango, A. (2024) The Geopolitical Competition Between China and the U.S. in New Technologies. Luiss School of Government Working Paper Series, SOG-WP12/2024. Retrieved from https: //sog.luiss.it/sites/sog.luiss.it/files/stango%20AS%20REV%20The%20geopolitical%20competition%20between%20China%20and%20the%20U.S.%20in%20new%20technologies.pdf

[15] Anderljung, M., Bengtsson, R., Beard, S., Belfield, H., Dafoe, A., Dreksler, N., McCauley, C., Trager, E. and Zhang, B. (2024) US–China Perspectives on Extreme AI Risks and Global Governance. arXiv. Retrieved from https: //arxiv.org/abs/2407.16903

[16] Bostrom, N. (2014) Superintelligence: Paths, Dangers, Strategies. Oxford University Press.

[17] Whittaker, M., Crawford, K., Dobbe, R., Fried, G., Kaziunas, E., Mathur, V., West, S., Richardson, R. and Schultz, J. (2018) AI Now Report 2018. AI Now Institute. Retrieved from https: //ainowinstitute.org/wp-content/uploads/2023/04/AI_Now_2018_Report.pdf

[18] Bradford, A. (2020) The Brussels Effect: How the European Union Rules the World. Oxford University Press.

[19] Government of the United Kingdom. (2023) The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023. Retrieved from https: //www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023