cogitatio

POLITICS AND GOVERNANCE

Volume 13

2025

# Technology and Governance in the Age of Web 3.0

Open Access Journal

ISSN: 2183-2463

**Edited by** Chang Zhang, Zichen Hu, and Denis Galligan

Politics and Governance, 2025, Volume 13
Technology and Governance in the Age of Web 3.0

Published by Cogitatio Press
Rua Fialho de Almeida 14, 2º Esq.,
1070–129 Lisbon
Portugal

Design by Typografia®
http://www.typografia.pt/en/

Cover image: © Tara Winstead from pexels



Available online at: www.cogitatiopress.com/politicsandgovernance

# Table of Contents

Politics and Governance
2025 • Volume 13 • Article 10.17645
https://doi.org/10.17645/pag.11743

EDITORIAL

Open Access Journal

# Technology as Statecraft: Remaking Sovereignty, Security, and Leadership in a Multipolar Age

Zichen Hu [1], Chang Zhang [2], and Denis Galligan [3]

[1] Department of Media and Communications, London School of Economics and Political Science, UK
[2] School of Government and Public Affairs, Communication University of China, China
[3] Department of Law, University of Oxford, UK

**Correspondence:** Zichen Hu (z.hu24@lse.ac.uk)

**Submitted:** 7 November 2025 **Published:** 27 November 2025

**Issue:** This editorial is part of the issue "Technology and Governance in the Age of Web 3.0" edited by Chang Zhang (Communication University of China), Zichen Hu (London School of Economics and Political Science), and Denis Galligan (University of Oxford), fully open access at https://doi.org/10.17645/pag.i443

## Abstract

This thematic issue examines how artificial intelligence, metaverse imaginaries, and decentralized Web3 systems have become arenas for states to build infrastructures, set technical standards, and project geopolitical power. It reconceptualizes technology not merely as an object of regulation but as a medium of statecraft through which sovereignty, security, and leadership are contested and remade in a multipolar digital order. This issue analyzes three interconnected dimensions: (a) the impact of global AI competition on state-making processes, enhancing coercive, extractive, delivery, and informational capacities similar to earlier state formation phases; (b) the nature of technological leadership as a relational and dynamic process influenced by interactions between leading and following states; and (c) the role of security logics in transforming external rivalry and internal governance through securitization. Through comparative analysis of the US, China, the EU, and emerging economies, this issue explores how diverse political systems encode openness, sovereignty, and accountability into their technological regimes, demonstrating that technological governance is inseparable from state-making. The contributions map competing logics—sovereign, liberal, entrepreneurial—showing that digital governance emerges not as convergence toward a singular model but as recursive entanglements of imagination and infrastructure.

## Keywords

China; digital sovereignty; EU; generative AI; infrastructural power; metaverse policy; technological governance; United States; Web3

## 1. Introduction

Artificial intelligence, metaverse imaginaries, and decentralised Web3 systems have moved from the periphery of technological discourse to the centre of global governance agendas. They have become arenas of geopolitical rivalry, state-building, and contested social imaginaries. Most accounts of technological governance view the state as a stable entity that applies rules to neutral tools, contrasting with this thematic issue's perspective that sees technology as a medium through which the state governs and evolves. This thematic issue takes a different view: technology is not only governed by the state; it is also a medium through which the state governs, competes, and remakes itself. In other words, technology has become statecraft—i.e., more than industrial policy or regulatory intervention, it is the strategic deployment of technological capabilities to consolidate sovereignty, project power, and shape the terms of international order. In the sovereign AI race now underway, states are not simply fostering innovation; they are building infrastructures, technical standards, data protocols, epistemic norms, and governance templates that will define economic production, social surveillance, and geopolitical influence for decades to come. Infrastructure, in this context, refers to the layered systems through which digital power is constructed, projected, and contested.

This thematic issue examines how technology operates as statecraft across three interconnected dimensions: sovereignty, security, and leadership. How does global competition over digital technologies reshape state capacity and the meaning of sovereignty itself? How do security logics, especially securitization, reconfigure both external rivalry and internal governance? And how does technological leadership operate as a relational and contested process, mediated by follower states and nonstate actors? We answer these questions by moving from theory to empirics, and from the longue durée of governance genealogies to the comparative politics of the present. The result is a multiscalar map of how technology, geopolitics, and governance coevolve in a multipolar digital order.

## 2. Sovereign AI and the Return of State-Making

This thematic issue begins by situating the global competition over artificial intelligence within classical theories of state formation. As Zhenyu Wang (2025) demonstrates, generative AI is not just a driver of industrial policy but a crucible for remaking state capacity and sovereignty. Drawing on theories of coercive, extractive, delivery, and informational capacities, the article shows how intensifying global competition compels governments to upgrade these capacities in ways reminiscent of earlier phases of state-building.

The article examines case studies of the US, France, Brazil, and Singapore, revealing a clear pattern: where elites perceive stronger transboundary technological rivalry, states invest more heavily in AI infrastructures that serve both domestic governance and geopolitical signalling. Predictive policing reconfigures coercive power; AI-assisted taxation and welfare systems remake extractive and delivery capacities; and large language models extend informational power into new domains of meaning management. Yet this is not a neutral process. As states build AI infrastructures in response to rivalry, they also import security logics into domains once framed as innovation or welfare. The language of a "race" in AI development securitises the technology, influencing investment choices, oversight mechanisms, and even the moral vocabulary of technological progress. Sovereignty becomes both a goal and a justification, blurring the line between nurturing innovation and building digital fortresses.

This reconceptualization is crucial because it highlights that technology is not merely a tool wielded by preexisting state power, but a medium through which state power itself is continually remade. Sovereignty, in the digital age, is less about territorial control than about the capacity to script technological futures by constructing rule regimes, infrastructural templates, and epistemic norms that guide innovation, surveillance, and collaboration across transnational ecosystems.

## 3. Technological Leadership as Relational Governance

If AI drives state-making, who leads this process? While the sovereign AI race highlights the state-making dimension of technology, Fang and Zhang (2025) challenge the assumption that leadership equals technological superiority. Instead, leadership is a relational and dynamic process of norm-setting, standards-writing, and infrastructural agenda-building, shaped by the interactions between leaders and followers.

In their article, Fang and Zhang (2025) emphasize that leadership is a process shaped by interactions and not merely a position of superiority. States do not exercise technological power in a vacuum; their strategies are continually mediated by how "follower" states align, resist, or adapt to competing models. Technological leadership is not a static position of superiority, but a relational, dynamic, and infrastructural process through which states assert normative and material influence. This perspective departs from traditional economic views that equate leadership with metrics like innovation output or patent counts. Instead, as Fang and Zhang (2025) argue, we must understand leadership as a contested terrain shaped by interaction between leading and following states, standard-setting and norm adaptation, and infrastructures and the actors who govern them. This makes technological governance a fluid and contested field rather than a static hierarchy of leaders and laggards. Norms, infrastructures, and standards become key arenas in which influence is negotiated and legitimacy claimed.

The US–China rivalry in AI illustrates the relational and dynamic nature of technological leadership. The US combines technological prowess with value-oriented governance frameworks, while China emphasises infrastructural development and standard-setting. But neither operates in a vacuum. The trajectories of AI governance are critically mediated by how "follower" states align, resist, or adapt to these models. In Europe, for example, the EU's AI Act attempts to project a rights-based template, while Singapore experiments with hybrid governance, and Brazil and India navigate between infrastructural attraction and regulatory caution.

Additionally, the role of security considerations further complicates this picture. Follower states do not only weigh efficiency or ethics, they assess risks of dependency, surveillance, and cyber vulnerability. As a result, technological governance emerges not as a static hierarchy but as a fluid and contested field, where even the "rules of the game" are constantly renegotiated under the shadow of security concerns.

## 4. Inside the Leading States: Paradoxical Infrastructuring

Leadership and state-making also need to be examined within the leading states themselves. Hu (2025) traces how China's governance of emerging technologies evolved from blockchain hype to AI strategy. The article presents this trajectory not as a simple progression from enthusiasm to repression, but as a case

of paradoxical infrastructuring. In this process, decentralised technologies are alternately valorised, domesticated, and redeployed within contradictory regimes of power.

The analysis employs Foucault's governmentality and Szonyi's "art of being governed" to highlight the role of intermediary actors, such as crypto developers, influencer-entrepreneurs, and policy-facing venture capitalists, who tactically navigate regulatory opacity. These actors perform decentralisation while materially benefiting from its state-sanctioned translation. The lingering influence of blockchain discourse remains a symbolic resource, reemerging in the AI era as a foundation for speculative sovereignty and infrastructural nationalism.

This genealogy exposes a deeper dynamic: even within "leadership" states, the relationship between governing and governed is unstable and negotiated. Security concerns do not simply descend from the centre; they are co-produced by intermediaries who translate technological imaginaries into governance practice. This is precisely why China's AI trajectory cannot be read only as top-down control; it is also a story of bottom-up adaptation, entrepreneurial statism, and securitised speculation.

## 5. The Security Turn in Decentralised Infrastructures

The security dynamics traced above reach their most acute form in decentralised infrastructures. The Web 3.0 cases analyzed by Ziyuan Wang (2025) and Wang and Qiu (2025) demonstrate the culmination of this process, showing how cross-border data controls meant as defensive measures are perceived as offensive, triggering spirals of suspicion and retaliation—a textbook digital security dilemma—and illustrating how blockchain-based platforms, metaverse projects, and other Web3 technologies enhance the organisational resilience of non-state armed groups. These groups weaponise blockchain and encrypted platforms to finance, recruit, and coordinate beyond state reach. These developments clarify why many governments are securitising decentralised infrastructures and how this securitisation further entrenches the identified dynamics:

- In relational leadership, it raises the stakes for follower states, who must navigate standards, ecosystems, espionage fears, and sanctions.
- In governance, it accelerates paradoxical infrastructuring, where decentralisation is simultaneously a threat to be tamed and a resource to be mobilised.

Rather than treating securitisation as inevitable, this thematic issue raises the question: is there an alternative pathway for governing decentralised technologies that mitigates risks while maintaining openness? Can technology enable statecraft without collapsing into securitised rivalry?

## 6. Comparative Techno-Governance: Metaverse, AI, and Beyond

Before turning to the empirical cases, it is worth reframing why the metaverse still matters. Once heralded as the next frontier of human interaction, the metaverse has largely receded as a failed commercial and ideological project, but this very failure is revealing. What has collapsed is not the imaginary itself, but its totalising promise. As an imaginary, the metaverse encapsulated the fantasy of seamless immersion and borderless connectivity; as an ecosystem, it has been disassembled into commercially viable modules, spatial

computing, digital twins, interoperable avatars, and simulation engines that quietly feed into adjacent domains such as AI model training, robotics, and industrial automation.

Rather than disappearing, the metaverse persists as a modular infrastructure of governance imagination: a repackaged set of technical and rhetorical components through which states and corporations continue to articulate aspirations of control, presence, and sovereignty in the digital space. In this afterlife, the metaverse operates less as a unified platform than as an ideological relay between centralised AI architectures and decentralised Web3 infrastructures. Its immersive design logics prefigure AI's ambitions to render the world computable, while its rhetoric of decentralised ownership anticipates blockchain's moral economy of participation and trust. Both draw on the same speculative imaginary of empowerment through technological mediation—and both reproduce dependency through new layers of infrastructural enclosure.

Seen genealogically, then, the metaverse should not be dismissed as passé but understood as a transitional dispositif that crystallises the contradictions of contemporary techno-governance: the oscillation between openness and control, innovation and securitisation, participation and capture. Its decomposition into AI and Web3-enabled components is more a sign of absorption than obsolescence and an example of how failed imaginaries are metabolised into new configurations of power and capital.

With this theoretical and genealogical scaffolding in place, this editorial presents this issue's comparative empirical studies, which map how diverse political systems encode openness, sovereignty, and accountability into their technological regimes.

Ingersleben-Seip (2025) contrasts China's industrial metaverse, which strengthens party control and economic growth, with the EU's vision of an open and interoperable metaverse grounded in digital rights. The US, although lacking a unified vision, dominates the infrastructure through Big Tech, producing a consumer-focused metaverse at odds with European aspirations. These competing visions shape both technical architectures and normative imaginaries.

Zhang and Wang (2025) extend the analysis to 34 metaverse policy documents from 13 countries, identifying four archetypes: Techno-economic vanguards (e.g., U.S., China), industrial innovators (e.g., Japan, South Korea), transformative opportunists (e.g., UAE, Brazil), and regulatory vigilants (e.g., EU). This typology shows how strategic positioning, technological capacity, and industrial structure shape policy priorities, whether by fostering key technologies, encouraging applications, or regulating behaviour.

Mark and Morison (2025) add a crucial dimension to the discussion: the divergent ways algorithmic decision-making is problematised across jurisdictions. Drawing on Carol Bacchi's framework, the article shows how the US emphasises innovation gaps, the EU stresses trust deficits, and China foregrounds stability risks. These framings shape distinct regulatory trajectories. Yet the article also notes an emerging convergence post-2024: a softening of regulatory stances to favour innovation, revealing the gravitational pull of competitive pressure and securitised narratives.

Finally, Sun and Chen (2025) examine centralised and decentralised approaches to AI governance using fuzzy-set qualitative comparative analysis. The findings complicate any simple binary: high-income states with strong R&D tend to decentralise; those with weak capacity but high perceived ethical risk to centralise;

and hybrid approaches emerge as a possible equilibrium, reallocating governance power between central and local governments as well as public and private sectors.

So what do these comparative studies tell us? First, techno-governance is deeply shaped by national imaginaries, not only of innovation and competition, but of vulnerability, risk, and legitimacy. Second, even divergent paths often converge under geopolitical pressure, raising questions about the long-term viability of rights—or trust-based models. Third, infrastructural asymmetries, who builds, who maintains, who controls, continue to structure not only access to digital power, but the very language through which governance is imagined.

Taken together, these comparative studies reveal that the trajectories of AI, metaverse, and Web3 governance are not parallel but mutually constitutive. Each expresses a different resolution to the same underlying tension between innovation, sovereignty, and legitimacy. The metaverse's fragmentation into infrastructural components, AI's consolidation into centralised data regimes, and Web3's diffusion through decentralised experiments together map the shifting frontier of digital governmentality. What emerges is not a coherent global model but a field of adaptive convergences: rights-based frameworks bending toward competitiveness, centralised systems adopting selective decentralisation, and experimental networks absorbing regulatory rationalities once meant to contain them.

In this sense, techno-governance appears less as a race between models than as a process of mutual appropriation and discursive recycling, where imaginaries of openness and control continually reconfigure one another. These patterns underscore that power in the digital age no longer resides solely in innovation capacity or regulatory strength, but in the ability to translate failure into infrastructure, to convert fading imaginaries like the metaverse into new logics of AI-enabled governance and blockchain-mediated legitimacy.

## 7. Conclusion: Navigating the Paradoxes of Technological Governance

Across all the contributions, a common theme emerges: technological governance is no longer simply about regulating applications at the "end" of innovation. It is about shaping infrastructures, imaginaries, and alliances at every stage of the technological life cycle. Three intertwined processes stand out:

1. Cultivating innovation: funding, talent pipelines, and supportive ecosystems.
2. Infrastructuring sovereignty: embedding strategic and ideological goals into technical standards and architectures.
3. Governing use and risk: constructing legal and ethical regimes to manage downstream applications.

Security logics permeate each of these processes, making them mutually reinforcing but also mutually destabilising. Securitisation can provide a rationale for investment and coordination, and the repurposing of failed imaginaries into strategic assets; but it also entrenches rivalries, narrows policy imagination, and undermines global interoperability. The contributions in this issue reveal three core insights:

First, technological governance is inseparable from state-making, particularly under the sovereign imperatives unleashed by AI-driven data infrastructures and the geopolitical afterlives of projects such as the metaverse.

Second, leadership is always relational, contingent on follower responses, reputational legitimacy, and evolving forms of dependence and resistance. Third, securitisation intensifies all of the above, not merely as a policy trend but as a deep structuring force that reshapes incentives, institutions, and imaginaries.

In this light, the convergence of AI, metaverse, and Web3 is less a story of technological evolution than of security-driven adaptation, where the remains of one paradigm continually feed the next, and where the language of protection becomes the idiom through which digital futures are imagined and governed.

This thematic issue invites readers to confront these paradoxes head-on. By moving from theory to empirics, from state-making to relational leadership, from internal genealogies to comparative policy typologies, we show that technological governance in a multipolar digital order is neither linear nor uniform. It is a recursive process shaped by competition and cooperation, centralisation and decentralisation, innovation and securitisation. Understanding this process is essential for scholars and policymakers who hope to steer emerging technologies toward outcomes that are not only competitive or secure but also just, open, and sustainable.

This special issue offers no singular model for digital governance. Instead, it offers a cartography of competing logics—sovereign, liberal, entrepreneurial, and insurgent—across multiple sites and scales. Taken together, the cases show that the governance of AI, metaverse, and Web3 does not unfold along parallel trajectories but through recursive entanglements of imagination and infrastructure. The metaverse's disassembly into modular protocols, AI's consolidation into centralised data regimes, and Web3's diffusion through decentralised experiments reveal not discrete paradigms but successive reconfigurations of the same desire: to render the digital world governable through code. Intracing these converges, this issue invites a rethinking of what it means to govern, to secure, and to lead in a world where technology is statecraft, infrastructures are never neutral, and the future is built protocol by protocol. Digital governance thus appears not as a race toward a stable model, but as an evolving struggle over how imaginaries of openness and control are encoded, repurposed, and securitised across the architectures that now constitute global order.

## Funding

This research received financial support from the National Social Science Fund of China (Grant Number: 24BCJ002).

## Conflict of Interests

The authors declare no conflict of interests.

## LLMs Disclosure

ChatGPT5.1 was used for proofreading and shorten some sentences.

## References

Fang, Y., & Zhang, S. (2025). Reconceptualizing technological leadership: A relational and dynamic framework. *Politics and Governance*, *13*, Article 10243. https://doi.org/10.17645/pag.10243

Hu, Z. (2025). Paradoxical infrastructuring: Genealogies of governance and "art of being governed" in China's blockchain–AI hypes. *Politics and Governance*, *13*, Article 10247. https://doi.org/10.17645/pag.10247

Mark, D., & Morison, J. (2025). Governing AI decision-making: Balancing innovation and accountability. *Politics and Governance*, *13*, Article 10245. https://doi.org/10.17645/pag.10245

Sun, C., & Chen, X. (2025). Destined for Balance? Centralized and decentralized approaches to AI governance. *Politics and Governance*, *13*, Article 10197. https://doi.org/10.17645/pag.10197

von Ingersleben-Seip, N. (2025). A tale of two metaverses: How America, China, and Europe are shaping the "new internet". *Politics and Governance*, *13*, Article 10246. https://doi.org/10.17645/pag.10246

Wang, Y., & Qiu, Y. (2025). The social movement evolution of non-state armed groups in the web 3.0 era. *Politics and Governance*, *13*, Article 10218. https://doi.org/10.17645/pag.10218

Wang, Z. (2025). Data Flows Meet Great Power Politics: The emerging digital security dilemma between China and the US. *Politics and Governance*, *13*, Article 10234. https://doi.org/10.17645/pag.10234

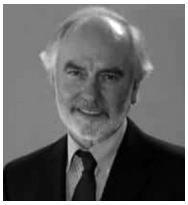
Wang, Z. (2025). Generative AI-Making and State-Making: Sovereign AI race and the future of digital geopolitics. *Politics and Governance*, *13*, Article 10222. https://doi.org/10.17645/pag.10222

Zhang, C., & Wang, L. (2025). Virtual worlds, real politics: A cross-national comparative study of metaverse policy approaches. *Politics and Governance*, *13*, Article 10239. https://doi.org/10.17645/pag.10239

## About the Authors

**Zichen Hu** is a PhD researcher at the Media and Communications Department, London School of Economics and Political Science, and a researcher associate for Oxford Global Society and Digital Futures for Children. Her research focuses on political communication, media technology governance, and global network of disinformation networks in today's geopolitical tensions.

**Chang Zhang** is an associate professor at the School of Government and Public Affairs, Communication University of China, and the director of the Center for International Organization Studies. Her research focuses on international political communication, media and global governance, and Chinese and Russian foreign policy.



**Denis Galligan** is an associate fellow of the Centre for Socio-Legal Studies. He is an emeritus fellow of Wolfson College Oxford. He was for many years the Jean Monnet professor of european public law at the Universita' degli Studi di Siena and a visiting professor at Princeton University.

Politics and Governance
2025 • Volume 13 • Article 10222
https://doi.org/10.17645/pag.10222

cogitatio

ARTICLE

Open Access Journal

# Generative AI-Making and State-Making: Sovereign AI Race and the Future of Digital Geopolitics

Zhenyu Wang

Journalism Institute, Shanghai Academy of Social Sciences, China

**Correspondence:** Zhenyu Wang (lucienw@sass.org.cn)

**Submitted:** 27 February 2025 **Accepted:** 9 September 2025 **Published:** 27 November 2025

**Issue:** This article is part of the issue "Technology and Governance in the Age of Web 3.0" edited by Chang Zhang (Communication University of China), Zichen Hu (London School of Economics and Political Science), and Denis Galligan (University of Oxford), fully open access at https://doi.org/10.17645/pag.i443

## Abstract

This article examines how intensifying global competition for sovereign AI, fueled by the rise of generative AI, is reshaping state capacity and digital geopolitics. Drawing on classical theories of state formation, this research introduces the Generative AI-Making and State-Making framework and applies it to four cases—the US, France, Brazil, and Singapore. The analysis shows that strategic pressures from the sovereign AI race compel nation-states to enter a new phase of state-building. Key findings reveal that the intensity of these state-building efforts is directly driven by elites' perceptions of transboundary competition: the sharper the perceived rivalry, the greater the strategic investment in strengthening coercive, extractive, delivery, and informational capacities. Although states converge in their efforts to augment these capacities, their objectives and methods diverge depending on international position, geopolitical context, and domestic endowments. As a result, the sovereign AI race is not merely a technological contest but also a powerful force reshaping domestic state structures and international power dynamics. It contributes to a more complex geopolitical landscape marked by US–China bipolarity alongside the rise of regional technological powers. By tracing how governments leverage AI to reinforce capacity, this study provides a theoretically grounded perspective on the evolving nature of geopolitical competition in the AI era.

## Keywords

digital geopolitics; generative AI; sovereign AI race; state-building; state capacity

## 1. Introduction

Twenty-first-century geopolitics is being reshaped above all by two forces: rapid technological change—most visibly the recent advances in AI—and the sharpening rivalry among major powers such as the US, China,

and Russia (Schmidt, 2022). As nations increasingly unveil AI strategies to assert ambitions for technological leadership, this competition has been framed as "the next space race"—a zero-sum contest where the victor stands to gain substantial economic, political, and military advantages, whereas the laggards risk being left behind in critical technological domains (Ulnicane, 2022). While this narrative carries a degree of exaggeration, the reality of intensified international competition over AI technologies, particularly large language models (LLMs), has become undeniable amid escalating geopolitical tensions.

The emergence of generative AI systems such as ChatGPT's LLMs has raised global awareness of AI's profound implications for national security, economic prosperity, and societal values. As a novel general-purpose technology (GPT), generative AI demonstrates the capacity to comprehend, learn, and simulate human cognitive processes. Unlike earlier GPTs such as electricity and the internet, which primarily delivered developmental or security benefits through economies of scale and indirect effects, generative AI directly enhances the efficiency of a wide array of economic and security-related tasks by augmenting fundamental human cognitive and creative abilities (Bresnahan & Trajtenberg, 1992; Eapen et al., 2023). This direct empowerment has led to an unprecedented rate of diffusion. For example, ChatGPT amassed 100 million active users within just two months of its launch, whereas TikTok, a leading consumer internet application, took nine months to reach the same milestone (Hu, 2023). Furthermore, the global generative AI market is projected to grow at a compound annual growth rate of 45% over the next decade ("Generative AI to become," 2023), compared with the 9.1% compound annual growth rate of the global consumer internet market during its "golden decade" from 2010 to 2020 (IBISWorld, 2024).

The rapid proliferation of generative AI has not only forged a swift consensus among political and economic leaders on its disruptive strategic value but also triggered a systematic deployment of state capacity aimed at securing technological leadership—or at least, technological autonomy. Consequently, the competition over generative AI has escalated into arguably one of the most intense technological race in history, thereby significantly amplifying its geopolitical dimensions. Recognition of generative AI's strategic value has spurred unprecedented investments in "sovereign AI"—defined as a nation's capacity to develop AI systems using domestic infrastructure, data resources, workforce expertise, and commercial ecosystems (A. Lee, 2024). As this competition has become increasingly central to national strategies and international politics, scholarly debates on its implications have also intensified, particularly with respect to national strategies, governance frameworks, and public–private partnerships. However, two critical gaps remain in the discussion (Radu, 2021; Roberts et al., 2024; Von Ingersleben-Seip, 2023). First, there is still a lack of cross-national comparative analyses examining sovereign AI competition through theoretical lenses. Second, the literature does not adequately address the causal mechanisms through which this technological rivalry shapes the emerging digital geopolitical landscape.

To address these gaps, this study asks a central question: How are nation-states, the primary actors in global geopolitics, recalibrating their capacities and international postures in response to the intensifying competition over sovereign AI, particularly in the era of LLMs? This inquiry is critical because the race for sovereign AI is not merely a technological contest but a profound force reshaping the nature of state power, strategic autonomy, and the global order. Drawing on a comparative analysis of distinct national cases, this research argues that strategic pressures emanating from sovereign AI competition are compelling states to embark on a new phase of state-building, focused on augmenting specific institutional capacities—coercive, extractive, delivery, and informational. While these reconfiguration efforts exhibit convergent patterns

globally, the objectives and intensity diverge depending on national ambitions, geopolitical positioning, and unique endowments. This study contributes to the theoretical and empirical understanding of state-making under conditions of technological competition by applying classical state formation theory to the contemporary challenge of sovereign AI. It develops a theoretically grounded framework that clarifies the causal mechanisms through which AI rivalry reshapes domestic state structures and international power dynamics. Empirically, this study substantiates its claims through a comparative analysis of four countries, offering insights into the commonalities and divergences in how contemporary sovereign AI competition drives state-building. In conclusion, this article contributes to the thematic issue Technology and Governance in the Age of Web 3.0 by linking state-building theory to both centralized AI systems and decentralized Web 3.0 technologies, showing how geopolitical pressures shape governance models across different technological paradigms.

## 2. From Competition to Capacity: Sovereign AI and State-Making in the Intelligent Age

The competition over sovereign AI is not merely a technological race; it is also a geopolitical struggle with far-reaching consequences for international relations. This competition is multifaceted, encompassing the control of critical technologies, data resources, and market access. The concept of sovereign AI captures the essence of this complex interplay between national strategies and international interactions, making it an indispensable lens for analyzing the digital geopolitical landscape. Charles Tilly's theory of "war making and state making" (Tilly, 1985, 1992) offers a useful starting point for examining these dynamics. Tilly argued that, from the early modern period through the 19th century, the imperative of success in warfare drove states to centralize power, extract resources, and build administrative capabilities, ultimately leading to the formation of nation-states and the modern world system. However, Tilly's theory has long been criticized for its Eurocentrism and bellicist tendencies. Postcolonial scholars argue that it is ill-suited to non-European contexts (Centeno, 2002; Herbst, 2000; Jung, 2006), and other researchers in state-building studies contend that it overstates the role of warfare while neglecting other crucial factors in state formation (Sharma, 2017; Spruyt, 1994). Acknowledging these limitations, this study moves beyond Tilly's specific claim that "war made the state and the state made war" (Tilly, 1985). Instead, it builds on a broader generational assumption shared by Tilly and subsequent state formation theorists: that enduring external pressures—military, economic, or technological—generate domestic imperatives for capacity building, which in turn reshape the architecture of state power and the geopolitical order (Hui, 2017). We argue that the current race for sovereign AI represents a new manifestation of this causal mechanism, compelling states to expand strategic, administrative, and technological capacities to secure autonomy and influence within the evolving global system.

### *2.1. Core Mechanism of Sovereign AI Competition and State Capacity Building*

This study posits a core mechanism of how sovereign AI rivalry translates external technological competition into domestic state-building dynamics. The argument begins with a consensus among national elites on the urgency of safeguarding technological sovereignty and geopolitical competitiveness. The rapid development of AI and the ensuing transboundary competition—marked by both pressure and opportunity—intensifies this consensus, compelling governments to pursue strategic investments in administrative, industrial, and cognitive capacities. The mechanism rests on two foundational pillars of state-building theory: elites' perception of external pressures and the functional demands placed on states to adapt to transforming technological and geopolitical environments.

First, elites' perception of competition is the starting point for state-building. Since Tilly, theories of state formation have underscored the central role of competitive pressures—ranging from the existential threat of war to performance-based competition in governance—in driving the development of state capacity (Cerny, 2010; Freudlsperger & Schimmelfennig, 2023; Grzymala-Busse, 2020; Thies, 2004). When elites perceive external competition as a critical challenge or opportunity for regime security, economic advantage, and power interests, these pressures and incentives prompt a reassessment of their existing capabilities and strategic orientation (Lavery, 2024; Vu, 2010), thereby fostering a collective will to enhance state capacity. The sharper and more stable the perception of rivalry, the stronger the consensus and momentum for state-building (Genschel, 2022; Reinhard, 1996, pp. 3–18).

Second, functional demands serve as a guide for state-building. The impetus arises not only from the need to centralize power in response to security threats but also from pressures to innovate institutionally and expand capacity for economic development (Hamm et al., 2012; Mann, 1984; Marquette & Beswick, 2011). To compete and succeed internationally, states often establish specialized bureaucracies to design industrial policies, while investing heavily in infrastructure, education, and R&D (Evans, 1995; Mazzucato, 2011). Weiss and Thurbon (2021) conceptualize such strategic state actions—driven by explicit international rivalry and aimed at advancing a nation's high-tech frontier—as "economic statecraft." They distinguish between two primary drivers for this statecraft: a "geo-economic" logic, which pursues technological autonomy for commercial competitiveness, and a "geo-political" logic, which seeks technological superiority for military advantage. In both cases, the elites' perception of external threats is translated into a concrete state-building agenda that strengthens technological capacity and secures the nation's position in the international system. In other words, the functional demand to gain a competitive advantage determines the specific content of state-building.

AI exemplifies these dynamics. As a GPT, it has engendered a global, transboundary competition, further accelerated by the rapid diffusion of representative technologies like LLMs. National elites increasingly view AI as determining their country's future prospects and status (Chui et al., 2023; U.S. Department of Defense, 2023). This perception is epitomized by the rise of the "sovereign AI" concept, through which elites elevate technological advantage to a core national interest, believing that states must achieve autonomy in AI R&D and industrial application (Satariano & Mozur, 2024; "Welcome to the era," 2024). Once consensus forms, the construction of sovereign AI capacity often enters a "state of exception" (Agamben, 2005), transcending ordinary institutional routines. In this context, political agenda-setting, policy formulation, and resource allocation become mechanisms through which state power is mobilized to meet the functional demands of AI development (International Institute for Strategic Studies, 2023). In this process, the stronger the perception of AI rivalry, the greater the willingness of elites to channel state investment toward capacity building, producing more pronounced forms of AI-related state-building. Infrastructure upgrades driven by sovereign AI competition can also enhance state "governmentality," making decision-making and implementation more efficient and precise (Foucault, 1991). This, in turn, reinforces elites' perceptions of technological competition, generating a feedback loop. At the same time, as state capacities are reshaped in response to the functional demands of sovereign AI competition, their "strategic selectivity" makes them inherently predisposed toward actions that favor technological competition (Jessop, 1990). In this sense, the dynamics of sovereign AI competition create a self-reinforcing cycle, making state-building processes increasingly visible in practice.

### 2.2. Auxiliary Mechanisms: Objective Differentiation and Strategic Convergence

State-building driven by sovereign AI competition is a process marked by both divergence and convergence, primarily driven by two auxiliary mechanisms. The first is objective differentiation, rooted in states' varying positions within the international system (Katzenstein, 1985, p. 20; Waltz, 1979, p. 72). Hegemonic powers facing clear challengers (Brands & Gaddis, 2021; Gilpin, 1981, p. 186), as well as small states that are more susceptible to shifts in the international system (Ayoob, 1995; Keohane, 1969), are more likely than others to interpret the current international environment as "tense." Consequently, they tend to place greater emphasis on the disruptive impact of GPTs like AI. Under heightened pressure, such states respond more rapidly to sovereign AI competition, pursue more ambitious objectives, and commit to higher costs of state-building, yet differences in geopolitical objectives lead them to follow differentiated pathways of response.

Divergent strategies are also shaped by differences in digital capacity. The success of sovereign AI supremacy depends heavily on what Mann (1984) defined as "infrastructural power"—the state's capacity to penetrate society and thereby determine whether its decisions can be effectively implemented. However, the control of digital infrastructure by dominant technology corporations often compels states to form strategic partnerships with these firms to execute their policies, which produces a form of "modern mercantilism," where state power is used to cultivate national champions in key sectors such as AI (Jensen, 2024). Due to the uneven global distribution of these champions, approaches to national capacity-building vary significantly. AI superpowers leverage state power to expand the global reach of domestic tech giants while constraining rivals. By contrast, nations with nascent AI capabilities negotiate with foreign AI leaders for cooperation and market access, with the principal aim of using foreign capital and technology to develop their own AI industries and infrastructure.

The second auxiliary mechanism is strategic convergence, driven by the shared capacity requirements of AI competition. AI competition—particularly the development of generative AI—is characterized by enormous cost, high intensity, and complex impacts (Horowitz, 2018; Maslej et al., 2024; Schrepel & Pentland, 2024; Singla et al., 2025). These features compel states to enhance four key capacities (Tang, 2022, pp. 180–207):

- Extractive capacity: The ability to mobilize and harness sufficient capital, data, and other material resources from society to support the development of an autonomous AI production system, given the immense investment required (Besley & Persson, 2009);
- Coercive capacity: The authority of the state to deploy non-market mechanisms to mobilize industries, society, and various governmental agencies, reinforcing its political authority in implementing directive and exclusionary AI policies (Mazzucato, 2018; Weiss, 1997);
- Delivery capacity: The ability to coordinate diverse stakeholders and provide essential public goods such as research networks and AI education initiatives(Mikhaylov et al., 2018);
- Informational capacity: The ability to collect, process, and analyze data on technologies, social impacts, and global competition in order to make high-quality policy decisions (M. M. Lee & Zhang, 2017).

These four capacities determine a nation's ability to maintain competitiveness in developing sovereign AI. The preceding analysis underpins the theoretical framework of Generative AI-Making and State-Making, as illustrated in Figure 1. Within this framework, dotted lines illustrate the mechanism of objective differentiation, while solid lines depict strategic convergence. Together, they demonstrate the new wave of state capacity building driven by the perception of transboundary competition amidst the rise of AI technologies like LLMs.

The next section applies this framework through a comparative analysis of four countries that are situated differently within the international system—the US, France, Brazil, and Singapore—to empirically examine the core mechanisms proposed in this article and present a global panorama of sovereign AI.

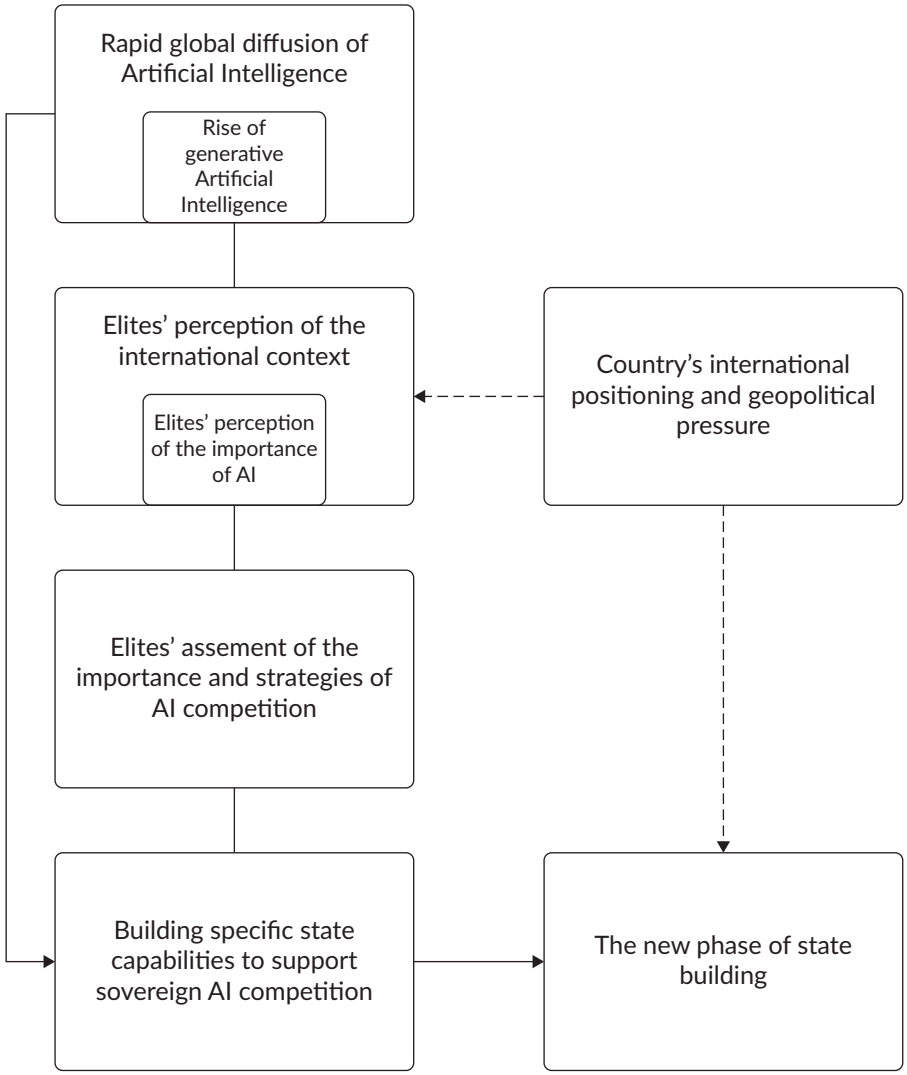



**Figure 1.** The mechanism of generative AI-making and state-making.

### *2.3. Methodology and Data Sources*

This study employs a systematic comparative case study methodology to test the proposed Generative AI-Making and State-Making framework. The comparative method is well-suited for examining complex causal processes in emerging phenomena like sovereign AI competition, where large-*N* analysis is not feasible (Collier, 1993).

Case selection follows Mill's method of agreement to identify common causal mechanisms across cases exhibiting similar outcomes despite varying contexts (Ghalehdar, 2022; Mill, 1978). This design allows us to test whether elites' perception of AI competition consistently drives state capacity building across diverse national settings. This selection further reflects the principles of typicality, diversity, and influence in case

selection (Seawright & Gerring, 2008). The aim is to include cases that are not only theoretically and empirically significant but also broadly representative in terms of geopolitical power and regional distribution. The four cases—the US, France, Brazil, and Singapore—all demonstrate enhanced state capacity in response to sovereign AI competition, despite their major differences in geopolitical positions, economic strength, and technological endowment. The US, as a global superpower facing intense challenges and a global leader in AI technology, is expected to most clearly reveal the proposed mechanisms. Singapore, a least-likely case, illustrates new possibilities for small states in an AI-driven world and represents the East Asian region. France and Brazil serve as contrasting cases, revealing the potential influences of geopolitical competitive pressure and technological endowments on the shaping of state capacity. By selecting cases that vary significantly in terms of international positioning (hegemonic power vs. great power vs. regional power vs. middle power), economic development level (advanced vs. emerging economies), and technological capabilities (AI leaders vs. AI followers), we can better isolate the causal effect of sovereign AI competition perception on state-building efforts.

For each case, analysis focuses on two dimensions: (a) elites' perceptions of AI competition and their evolution over time; (b) policy initiatives and institutional reforms designed to enhance AI capabilities. This structured approach enables systematic comparison while preserving the contextual richness that is essential for understanding complex political processes.

To construct the dataset, a systematic collection strategy was employed. To capture each nation's perception of AI competition, we primarily gathered statements and materials issued by the highest executive and legislative bodies and leaders of the sample countries since 2017 (see Appendix A in Supplementary File). These include speeches and documents from official occasions (e.g., diplomatic affairs or domestic formal meetings) and official websites of national institutions. To assess state capacity building, we employ a triangulation approach (Tzagkarakis & Kritas, 2023) that relies on three multi-dimensional evaluation criteria. These are: (a) policy documents and authoritative statements that reflect elites' perceptions of competition; (b) legally binding national AI strategies aimed at developing new state capabilities; and (c) concrete establishment and implementation status of new institutions and programs tasked with implementing this capacity building. This methodological approach strengthens the reliability and validity of our findings and provides a robust foundation for evaluating and comparing state capacity transformations across the four cases in the context of sovereign AI competition.

## 3. Case Study: Between Global Hegemony and Regional Integration

### *3.1. The Reshaped Superpower: The US's AI Strategy*

The US, as the only enduring global superpower, has officially designated China as a "strategic competitor" since 2017 (The White House, 2017). Under both the Biden and Trump administrations, this perception has intensified, with China portrayed as the most potent and dangerous adversary. This perception has fueled US motivations in AI competition and prompted extensive strategic actions with significant geopolitical implications. This section reviews the evolution of US AI policy (2017–2025), its competitive strategies, and the overarching objective of maintaining global AI hegemony.

Between 2017 and 2025, AI shifted in US policymaking from a technological opportunity to a strategic imperative. The 2017 FUTURE of Artificial Intelligence Act (2017) recognized AI as vital for economic prosperity. By 2019, Executive Order 13859 underscored the necessity of US leadership in AI for national security (The White House, 2019). The National Artificial Intelligence Initiative Act of 2020 (2020) reinforced commitments to sustained leadership in AI. The 2021 *National Security Commission on Artificial Intelligence* report stressed AI's transformative potential, advocating urgent measures (National Security Commission on Artificial Intelligence, 2021). Following the emergence of GPT-based LLMs, US policy activity intensified sharply. In 2023 alone, nine administrative orders, plans, and acts were issued at the ministerial level or higher. In 2024, policy shifts emphasized US leadership amid rising tensions (The White House, 2024). In 2024, against the backdrop of rising tensions, the U.S.–China Economic and Security Review Commission urged Manhattan Project-scale AI investments (U.S.–China Economic and Security Review Commission, 2024). In 2025, executive orders under both the Biden and Trump administrations, alongside Vice President J. D. Vance's Paris AI Summit speech, reaffirmed the urgency of maintaining US AI dominance through both domestic policies and foreign toolkits (The White House, 2025a, 2025b; Vance, 2025).

Overall, US policymakers increasingly link sovereign AI competition to national security and to economic, military, and technological primacy (Horowitz et al., 2018). Since the emergence of generative AI, US policy documents have increasingly emphasized the imperative of global leadership, often through narratives of intensifying strategic rivalry (The White House, 2025a, 2025b). As a result, the US is the actor most likely to adopt high-cost measures to reinforce its technological capabilities.

Coercive capacity has expanded through direct market interventions, particularly in restricting critical AI supply chains to disadvantage competitors, most notably China. Executive Order 13859 institutionalized technological control via export bans on high-end computing chips (Bureau of Industry and Security, 2025; The White House, 2019). Between 2022 and 2024, systematic export controls on advanced chips and AI models marked a decisive departure from market principles, reflecting state-directed interventions on both supply and demand to restrict competitor access (Swanson, 2024).

Extractive capacity involves significant federal investments and public–private partnerships. While direct societal resource extraction remains limited, initiatives like the National Artificial Intelligence Research Resource pilot and the National Science Foundation (NSF) Regional Innovation Engines exemplify centralized funding mechanisms. New initiatives like the $500 billion Stargate Initiative—a collaboration among OpenAI, SoftBank, Oracle, and MGX—represent state-led yet corporately executed resource extraction strategies. Such partnerships mobilize substantial capital to achieve national AI objectives (Friesen, 2025).

Delivery capacity is evident in administrative support for AI infrastructure, workforce development, and research platforms. Executive Order 14141 streamlined federal land acquisition for AI facilities. Initiatives like Educate AI and the National AI Research Institutes emphasize workforce training and interdisciplinary R&D (NSF, 2023a, 2023c; The White House, 2025a). The NSF's National Artificial Intelligence Research Resource Pilot program integrates computational resources and private-sector collaboration, supplemented by seven new National AI Research Institutes to advance infrastructure and innovation (NSF, 2023a, 2023b).

Informational capacity has also advanced, reflected in a dense advisory system. Key bodies include the Office of Science and Technology Policy, the National Science and Technology Council, the National AI Initiative

Office, the National Security Commission on Artificial Intelligence, and the President's Council of Advisors on Science and Technology, informing comprehensive policymaking across government and legislative sectors.

In sum, driven by geopolitical ambition to sustain hegemonic status and the perceived threat posed by China, the US has pursued explicit and exclusionary leadership in AI. To confront the complexity of rapid technological advancement, the US has undertaken aggressive measures that have ultimately reshaped the state itself. Since the emergence of ChatGPT in 2022, the generative AI era has significantly amplified the United States' sovereign AI endowments: dominance in English-language AI markets, control over advanced semiconductor supply chains, and the world's largest AI investment ecosystem (Maslej et al., 2024). The US also leverages extraterritorial jurisdiction to secure global data resources—advantages that collectively underpin its hegemonic strategy. Recent policies reaffirm this vision, presenting the US as the preferred global partner in AI cooperation (The White House, 2025a, 2025b; Vance, 2025).

As a result of these initiatives, the US government has substantially expanded its coercive power through direct market interventions and regulatory mandates. Its recent adoption of politically committed policy incentives and mission-oriented financing has also opened new pathways for enhancing extractive capacity. In terms of delivery capability, the intensifying AI competition has catalyzed the expansion of state institutions, empowering new agencies and enhancing coordination with existing bodies. These institutional developments have systematically improved the US state's informational capacity. The empirical analysis supports the theoretical hypothesis: The US has demonstrated substantial efforts to enhance all four dimensions of state capacity in response to sovereign AI competition. These efforts reflect its strategic pursuit of absolute advantage, and appear more extensive than those observed in other cases. Table 1 provides an overview of the United States' approach to sovereign AI competition.

**Table 1.** An overview of the sovereign AI competition in the US.

| Technological Perception | | |
|---|---|---|
| 2017: AI seen as a promising technology with societal impacts. | | |
| 2019: AI recognized as crucial for national security. | | |
| 2021: AI viewed as a general-purpose technology with economic, military, and geopolitical implications. | | |
| 2024: AI framed as a global competition to maintain US leadership. | | |
| 2025: AI seen as a strategic imperative for global dominance in security and technology. | | |
| | Institutions | Key policies and contents |
| Coercive capacity | Department of Commerce/Bureau of Industry and Security, Department of Defense | Use of trade controls to restrict technological diffusion, directives to guide private-sector investment, regulatory framework for the responsible diffusion of advanced artificial intelligence technology. |
| Extractive capacity | NSF, President | Traditional model of research funding, new state-led corporate-driven operational model, NSF regional innovation engines, Stargate initiative. |

**Table 1.** (Cont.) An overview of the sovereign AI competition in the US.

| | Institutions | Key policies and contents |
|---|---|---|
| Delivery capacity | Department of Defense, Department of Energy, NSF, National AI Research Institutes | Promoting development of AI infrastructure, optimizing AI talent cultivation, establishing AI research platforms, EducateAI initiative, National Artificial Intelligence Research Resource pilot program. |
| Informational capacity | White House Office of Science and Technology Policy, National Science and Technology Council, National Artificial Intelligence Initiative Office, National Security Commission on Artificial Intelligence, President's Council of Advisors on Science and Technology | Establishing advisory bodies, enhancing governmental information capabilities, creating regulatory frameworks, National Artificial Intelligence Research and Development Strategic Plan, National Artificial Intelligence Initiative Act of 2020. |
| Capability goal | | |
| US AI capacity-building aims to maintain global leadership by securing technological, military, and economic supremacy. | | |

### *3.2. A Catching-Up Great Power: France's AI Strategy*

As a UN Security Council permanent member and a core EU state, France's geopolitical vision embodies dual identities: participating as a global power and leading regionally by promoting European autonomy. This duality profoundly shapes France's AI strategy. Currently, France is the most competitive AI actor outside the US and China, exemplified by Mistral AI's $6 billion valuation and LightOn's prominence as Europe's first publicly listed generative AI startup ("LightOn to become," 2024).

French policymakers have demonstrated an ambivalent stance toward AI competition—expressing concerns about falling behind superpowers while simultaneously projecting regional leadership. This tension has produced periodic "catch-up" policy behaviors. France's 2018 Villani Report identified AI as essential, warning of the nation becoming "a data colony" due to US and Chinese dominance. Thus, preserving independence and European coordination became central objectives (Villani, 2018). The 2021 national AI strategy reaffirmed earlier policy focuses but underwent a significant transformation in 2024 with the Artificial Intelligence Commission's (AIC) publication, which explicitly highlighted generative AI's emergence in 2022 as a pivotal inflection point. It emphasized the intense pressure from US and Chinese advances on French sovereignty and competitiveness (Commission de l'Intelligence Artificielle, 2024). President Macron's 2025 declaration of a "third way" in AI explicitly positioned France against the US and China (Chavez, 2025). The president has recently taken a highly assertive and hands-on role in promoting France's AI industry, unveiling a €109 billion investment plan that he pointedly framed as "France's Stargate" to rival US initiatives ("Intelligence artificielle: Emmanuel," 2025). This initiative extends beyond funding to include direct presidential intervention and economic diplomacy. A notable example is his personal involvement in forging a partnership between the French startup Mistral AI and US chipmaker Nvidia. According to *PYMNTS* reporting, Nvidia's CEO Jensen Huang explained that Macron personally intervened after Mistral AI sought his assistance in initiating direct contact with Nvidia's leadership to accelerate a cloud-computing partnership: "Who are they? Let me call them" ("French President rallies," 2025). And he called them. Macron himself later praised this collaboration as a "game changer" crucial for "strengthening France's technological

independence," illustrating his aggressive, top-down effort to cultivate national champions like Mistral AI ("French President rallies," 2025).

France has leveraged its early positioning and resource advantages to shift from supporting European coordination to explicitly claiming leadership in Europe. By 2025, the "Make France an AI Powerhouse" strategy has positioned France as Europe's generative AI hub (Présidence de la République Française, 2025). However, its stimulus-driven policy reflects a lack of a clear model competitor, creating a reactive policy trajectory. In sum, French political elites increasingly frame AI competition as integral to maintaining national geopolitical influence and regional leadership. This perspective has prompted a significant shift in industrial policy, moving beyond market-oriented approaches toward a form of "geo-dirigisme" (Seidl & Schmitz, 2024), in which the state actively directs economic activity and resources into technologies it deems geoeconomically or geopolitically vital. However, unlike the US, France has not developed a clear narrative identifying specific competitors. Instead, it positions itself in opposition to an ambiguous notion of "technological hegemony." Within the theoretical framework adopted here, France is not expected to pursue aggressive coercive interventions or large-scale extractive investment strategies. Rather, it is expected to adopt a balanced approach that integrates technological capacity-building with social governance considerations.

Regarding coercive capacity, France promotes technological sovereignty alongside regulatory frameworks, primarily within the EU context. While earlier strategies (République Française, 2021; Villani, 2018) focused on governance, recent policies have shifted slightly toward developing autonomous capabilities through domestic incentives. Nevertheless, compared to the aggressive market interventions by the US, France remains largely regulatory in orientation rather than overtly competitive.

France's extractive capacity relies on government investments, R&D funds, and public–private partnerships. The 2021 national AI strategy involved €2.22 billion, including substantial public funding and private co-financing (République Française, 2021). The proposed "France & AI" fund in 2024 mobilized €10 billion to accelerate AI ecosystem development (Commission de l'Intelligence Artificielle, 2024). However, these investment scales remain significantly smaller than US initiatives (e.g., the $500 billion Stargate Initiative).

In terms of delivery capacity, France has prioritized the development of an integrated ecosystem for AI education and research. Notably, interdisciplinary autonomous research institutes—the Instituts Interdisciplinaires d'Intelligence Artificielle, or 3IA—and computational infrastructure such as the Jean Zay supercomputer have significantly enhanced administrative capabilities (Centre National de la Recherche Scientifique, 2025; Villani, 2018). In addition, administrative efficiency has been improved through the streamlining of AI-related data processing procedures (Commission de l'Intelligence Artificielle, 2024). However, since the 3IA network is time-limited and France has not established permanent institutions aligned specifically with AI, its delivery capacity remains more limited compared to the US.

In the domain of informational capacity, France has made notable advances through new evaluation systems and societal feedback mechanisms. The establishment of the National Institute for AI Evaluation and Security (INESIA) in 2025 provides a credible institutional framework for model evaluation, strengthening governmental responsiveness ("The French government," 2025). Furthermore, initiatives such as "AI Cafés" facilitate public engagement and enhance mutual understanding between citizens and the state in the context of AI governance

(Présidence de la République Française, 2025). While smaller in scale and less institutionalized than US efforts, France nonetheless occupies a competitive position in AI information governance.

In conclusion, the establishment of new institutions such as INESIA and the upgrading of the Commission Nationale de l'Informatique et des Libertés (CNIL; Commission de l'Intelligence Artificielle, 2024) underscore the reinforcement of the French state apparatus through participation in AI competition. Across the four dimensions, France has significantly enhanced capabilities, though in ways that are partly regulatory rather than purely developmental, which reflects distinctively European characteristics. As discussed, France's geopolitical objectives in the AI era are composite: It aims to maintain global great-power influence beyond the primary US–China rivalry while continuing to assume a leading role within Europe. Yet given the EU's deep integration and complementary economies, France faces no genuine European rival and lacks the conditions to challenge a hegemon.

Although France remains an active participant in global AI competition, it has not heavily securitized the field or framed AI development primarily in national security terms. As a result, the impact of its sovereign AI strategy on the restructuring of national capabilities is significantly more limited than that of the US. Specifically, France exercises greater restraint in the use of administrative authority, adopts a more decentralized and smaller-scale approach to resource extraction, and lags behind the US in terms of the institutionalization and systematization of administrative delivery. Unlike the US, France lacks a coherent set of formal institutions dedicated to managing AI-related affairs, which in turn constrains its informational capacity. Apart from INESIA, most improvements in informational capacity are centered on public communication and opinion feedback initiatives, while their direct impact on governmental decision-making remains unclear. Table 2 summarizes France's approach to sovereign AI competition, showing how this European power transforms the pressures brought about by technological competition into the practice of state-building.

**Table 2.** An overview of the sovereign AI competition in France.

| Technological Perception | | |
|---|---|---|
| 2018: AI strategic awakening, concern over US–China dominance. | | |
| 2021: AI positioned as a national priority through institutional governance and European coordination. | | |
| 2024: Pressure from the generative AI wave redefining competition as a sovereignty crisis. | | |
| 2025: France asserts "third way" leadership within the European AI strategy. | | |
| | Institutions | Key policies and contents |
| Coercive capacity | Secrétariat général pour l'investissement (SGPI), Ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation (MESRI), Ministère de l'Économie, des Finances et de la Relance, Coordinateur national pour l'intelligence artificielle | Specification of priority development sectors, strengthening of AI ethics and data flow regulations, preferential policies for domestic AI R&D activities. |
| Extractive capacity | Matignon and other government departments, Bpifrance, Commission nationale de l'informatique et des libertés (CNIL) | Hybrid model combining direct government investment, R&D funds, public–private partnerships, and international data sharing, France 2030, "France & AI" Fund. |

**Table 2.** (Cont.) An overview of the sovereign AI competition in France.

| | Institutions | Key policies and contents |
|---|---|---|
| Delivery capacity | MESRI, Centre national de la recherche scientifique (CNRS), SGPI, CNIL | Creation of interdisciplinary AI hubs (3IA), expansion of public computing infrastructure, coordination of academic–industrial partnerships for AI innovation. |
| Informational capacity | Initiative nationale pour l'éthique et la sécurité de l'intelligence artificielle (INESIA), CNIL, Conseil national du numérique (CNNum) | Strengthening government decision-making capabilities by establishing AI risk prediction and model evaluation mechanisms, developing public information feedback systems, and hosting nationwide AI outreach programs such as "AI Cafés." |
| Capability goal | | |
| French AI capacity-building aims to maintain global great-power influence beyond the primary US–China rivalry while continuing to assume a leading role within Europe. | | |

### *3.3. A Lagging Regional Power: Brazil's AI Strategy*

Brazil, Latin America's largest economy and a leading representative of the Global South through BRICS and the G20, has lagged behind in responding to sovereign AI competition. While Colombia and Argentina introduced national AI strategies in 2019, Brazil's first comprehensive strategy emerged only in 2021. Law No. 21 primarily established regulatory guidelines without robust enforcement mechanisms or a clear technological development framework, presenting AI largely as a tool for public service improvement and economic growth rather than for sovereignty or international competition (Câmara dos Deputados, 2021).

The 2021 Brazilian Strategy for Artificial Intelligence (*Estratégia Brasileira de Inteligência Artificial*, EBIA) signaled a shift, recognizing AI's economic significance and estimating an additional 1.2% annual contribution to global GDP by 2030 (Ministério da Ciência, Tecnologia e Inovações [MCTI], 2021). Yet the strategy emphasized societal and service-related impacts more than strategic competition or sovereignty. Critics contend that the EBIA represents a passive imitation of global trends. It lacked instrumental policy mechanisms, failed to overcome collective action challenges, and showed weak integration with existing policy frameworks—rendering it an ambitious but largely ineffectual document (Filgueiras & Junquilho, 2023).

Following the rapid global spread of generative AI (Singla et al., 2025), Brazil launched IA Para o Bem de Todos (AI for the Good of All) at the Fifth National Conference on Science, Technology, and Innovation in July 2024 as a strategic update to the EBIA. Incorporated into the Programa Brasileiro de Inteligência Artificial (PBIA), the document frames AI as a disruptive force and the third wave of the ICT revolution. Crucially, it marks the first official linkage between AI and national sovereignty, portraying the global proliferation of AI strategies as "a race for dominance with geopolitical implications" (Conselho Nacional de Ciência e Tecnologia [CCT], 2024).

Compared with advanced economies like the US and France, Brazil recognized AI's strategic significance relatively late. This delay partly reflects its fragmented policymaking process: The PBIA emerged from an extended consultation involving 38 proposals, six workshops, and 30 bilateral meetings with stakeholders (CCT, 2024). Brazil's benign geopolitical setting and moderate technological capabilities further limit incentives for assertive engagement in AI competition. While Portuguese is globally widespread, its strategic

utility is diminished by the geographic separation between Brazil and other Lusophone nations, primarily in Europe and Africa (Comunidade dos Países de Língua Portuguesa, n.d.).

Structural weaknesses—including low R&D spending, weak cybersecurity, and acute digital inequality—further constrain AI development (UNESCO, n.d.). With no significant regional or global rivals, Brazil lacks strong external pressures to securitize AI. In the absence of external threats and facing relatively low international pressure, sovereign AI competition has not become a pressing political priority (de Almeida et al., 2021; Malamud, 2011). Nonetheless, the PBIA reflects growing awareness, and Brazil has begun laying the institutional groundwork to address the challenges of sovereign AI through four state capacities: coercive, extractive, delivery, and informational.

In terms of coercive capacity, Brazil relies primarily on existing regulatory frameworks, including instruments such as the *Lei Geral de Proteção de Dados Pessoais*. The 2021 EBIA and the 2024 PBIA introduced ethical guidelines, public-sector directives, and multi-level governance structures to oversee the national implementation of AI policy (CCT, 2024; MCTI, 2021). However, Brazil's coercive capacity remains limited, focusing on the oversight of AI applications rather than non-market interventions to boost technical capacities.

With respect to extractive capacity, the PBIA outlined a more coherent funding mechanism totaling R$23.03 billion (approximately USD 4 billion), drawing from both public and private sources, and replacing previously fragmented approaches (CCT, 2024). Despite this improvement, the scale of investment remains modest compared to AI leaders, constraining Brazil's global competitiveness.

Administrative delivery capacity has shown tangible improvement. Educational reforms, targeted AI training programs, and partnerships with international firms like OpenAI have strengthened institutional implementation capacity (CCT, 2024; MCTI, 2021). Programs such as IA² MCTI and various startup incubators have further supported the development of Brazil's AI R&D ecosystem. Nonetheless, these improvements are largely concentrated in specific areas such as education and entrepreneurship, and rely on pre-existing innovation service structures rather than representing a broader expansion of the state apparatus.

Informational capacity is Brazil's most developed domain. The PBIA created the Brazilian AI Observatory and the National Center for Algorithmic Transparency and Trustworthy AI, which have enhanced the government's evidence-based decision-making through comprehensive data monitoring and risk assessment systems (CCT, 2024).

Brazil's AI policies issued in 2021 and 2024 demonstrate a gradual enhancement of national capabilities, with the most significant progress occurring in the domain of informational capacity. This emphasis on information governance aligns with Brazil's highly fragmented political structure and reflects the relatively low resource requirements of informational capacity compared to coercive, extractive, and administrative functions. Brazil continues to articulate aspirations for regional technological leadership, as evidenced by its emphasis on technological sovereignty and Lusophone AI initiatives (CCT, 2024; MCTI, 2021). However, due to limited external pressure and suboptimal strategic conditions, Brazil has made substantially less progress in strengthening coercive and extractive capacities. Consequently, its participation in sovereign AI

competition remains delayed and comparatively less influential on the global stage. Table 3 summarizes Brazil's approach to sovereign AI competition, highlighting how it mobilizes its coercive, extraction, delivery, and information capabilities to strengthen sovereignty and regional leadership, although this process is less pronounced than in the United States and France.

**Table 3.** An overview of the sovereign AI competition in Brazil.

| Technological Perception | | |
|---|---|---|
| 2020: AI identified as an emerging technology for enhancing international competitiveness. | | |
| 2021: AI recognized as a core driver of national economic growth. | | |
| 2024: AI framed as a disruptive technology with sovereign and geopolitical consequences through technological competition. | | |
| | **Institutions** | **Key policies and contents** |
| **Coercive capacity** | Presidência da República, Ministério da Ciência, Tecnologia e Inovação (MCTI), Ministério da Economia, Ministério da Justiça e Segurança Pública, Autoridade Nacional de Proteção de Dados | An AI regulatory framework built upon the Lei Geral de Proteção de Dados (LGPD, General Data Protection Law), a cross-institutional and directive-based approach to policy formulation and coordination. |
| **Extractive capacity** | Fundo Nacional de Desenvolvimento Científico e Tecnológico (FNDCT), Financiadora de Estudos e Projetos , Banco Nacional de Desenvolvimento Econômico e Social , Lei Orçamentária Anual, MCTI, and other institutions | Provision of non-repayable funding and credit, collaboration with the private sector to secure investment support, and promotion of open data policies within the framework of the LGPD. |
| **Delivery capacity** | MCTI, Presidência da República, Ministério da Educação e Cultura, Agência Brasileira de Desenvolvimento Industrial, FNDCT | Comprehensive education reforms, expansion of research networks, and development of innovation ecosystems, increased emphasis on technology-related disciplines, joint training initiatives with companies such as OpenAI, implementation of the IA² MCTI program, support for entrepreneurship through Start-Up Brasil and Conecta Start-Up Brasil, and targeted investments in technological infrastructure. |
| **Informational capacity** | Ministério da Ciência, MCTI, Supremo Tribunal Federal, Comitê Gestor da Internet no Brasil, Ministério das Relações Exteriores | Development of a comprehensive information collection and analysis system, establishment of the Observatório Brasileiro de Inteligência Artificial, foundation of the Centro Nacional de Transparência Algorítmica e IA Confiável, and creation of Brazilian AI Governance Support Network and the Brazilian International Debate Participation Support Network. |
| **Capability goal** | | |
| Brazil's AI capacity-building aims to establish regional leadership, advance technological sovereignty, and develop a Portuguese-language LLM, thereby enhancing its international influence and discursive power. | | |

### *3.4. An Unexpected Middle Power: Singapore's AI Strategy*

Singapore has actively engaged in sovereign AI competition, publishing national AI strategies in 2019 and 2023, and launching a SGD 70 million national multimodal LLM project in late 2023. Although traditional geopolitical theories predict neutrality or hedging for small states like Singapore (Chang, 2022; Teo & Koga, 2022), breakthroughs in AI have reshaped its strategic calculus. The rise of generative AI—particularly the release of ChatGPT—has profoundly transformed Singapore's perception of AI's disruptive potential and its implications for regional geopolitics. As stated in the preface to its 2023 National AI Strategy 2.0, "Since the release of ChatGPT by OpenAI on 30 November 2022, Artificial Intelligence (AI) has gone mainstream" (Ministry of Communications and Information [MDDI], 2023). While Singapore lacks traditional advantages such as population size, territorial expanse, or economic scale, its longstanding national digitalization strategy and multilingual environment provide distinct comparative strengths in AI. This positioning has enabled Singapore to carve out a unique geopolitical niche and pursue regional leadership in global technological competition.

Singapore's evolving AI strategies initially framed AI as a disruptive force for society and industry (GovTech Singapore, 2017). The 2019 National AI Strategy marked a conceptual shift, identifying AI as a pivotal force in reshaping economic structures and geopolitical configurations, and emphasizing technological capability as vital to national prosperity and survival (MDDI, 2019). By 2023, the updated strategy explicitly set AI leadership as a national objective, positioning Singapore as a global frontrunner in AI innovation (MDDI, 2023).

Policymakers now view AI competition as central to advancing regional influence and national economic growth, framing it explicitly as a matter of national survival and strategic opportunity. The pressure on Singapore's political elite—stemming from the nation's position as "a tiny little island with no natural resources" in an era of intensifying global AI competition—has prompted state-led mobilization (Prime Minister's Office of Singapore, 2023). Although coercive measures are less pronounced, Singapore's approach still aligns with the competitive response model of coercion–extraction–delivery–information, with the nation's machinery continuously strengthening in the competition.

Coercive capacity is exercised mainly through government directives that guide and regulate the market to channel resources such as capital, talent, and data into the AI sector. In the 2019 National AI Strategy, the Singaporean government emphasized the need to build digital infrastructure and promote the widespread adoption of AI technologies across various sectors, particularly by applying AI to improve the quality and efficiency of public services and administrative processes (MDDI, 2019). In the 2023 National AI Strategy, Singapore plans to further strengthen the government's role in driving the deployment of AI technologies, especially in key economic sectors and public services. It also promoted collaboration between industry and the research community, aligning innovation with market demands and facilitating interdepartmental integration (MDDI, 2023).

Extractive capacity has been expanded through national AI projects. The 2019 National AI Strategy project's portfolio launched five flagship projects spanning intelligent freight planning and efficient municipal services, among five critical domains. The Singaporean government aims to drive investment in AI research through these projects, generating demand to strengthen the country's talent pool and capabilities while guiding the development of digital infrastructure. By fostering a partnership between academia,

industry, and government, Singapore has established stable funding and data foundations to support its AI competitiveness (MDDI, 2019).

Delivery capacity is pursued through the building of an ecosystem that includes dedicated platforms for research, talent cultivation, data management, and international collaboration. The 2023 strategy introduced an AI-focused innovation site and "data concierge" services, promoting public–private data flows for AI development, further strengthening the operational framework for administrative efficiency (MDDI, 2023).

Singapore has significantly advanced informational capacity through strategic infrastructure and governance frameworks. The establishment of the National AI Office under the Smart Nation and Digital Government Office ensures coordinated national AI agendas (MDDI, 2019). The 2023 AI Verify initiative by the Infocomm Media Development Authority enhanced transparency and regulatory compliance in AI research and applications, reinforcing governmental responsiveness to AI-related risks (Infocomm Media Development Authority, 2023).

Singapore's AI strategy also emphasizes leveraging linguistic and cultural regionalization as key geopolitical assets in the sovereign AI era. Official narratives stress the importance of creating localized AI models sensitive to Southeast Asia's diverse cultural contexts ("Singapore pioneers flagship AI initiative," 2024). The strategic objectives outlined in 2023—selective excellence and empowerment—highlight a deliberate approach to developing regional AI capabilities complementary to dominant global models, thereby securing regional technological influence without direct confrontation with leading global powers ("Singapore builds AI model," 2024). Upon launching its first LLM project, the Singaporean government highlighted that its primary objective was to develop sovereign capabilities by creating multimodal and localized LLMs that reflect the context and values of Southeast Asia's diverse cultures and languages ("Singapore pioneers flagship AI initiative," 2024). In this way, Singapore has shifted from an independent, balancing approach to becoming a regional technological core in the era of sovereign AI. Table 4 outlines Singapore's approach to sovereign AI competition, illustrating how the development of its four key capacities has strengthened the city-state's capabilities and positioned it as both a regional AI leader and an innovation hub in Southeast Asia.

**Table 4.** An overview of the sovereign AI competition in Singapore.

| Technological Perception | | |
|---|---|---|
| 2017: Viewing AI as a solution to social challenges without emphasizing global competition. | | |
| 2019: The National AI Strategy framed AI competition as essential for national survival and prosperity, highlighting its geopolitical implications. | | |
| 2023: The updated strategy emphasized AI leadership, positioning Singapore as a global AI hub. | | |
| | Institutions | Key policies and contents |
| Coercive capacity | Ministry of Communications and Information, and other government departments | Implementation of the 2019 and 2023 National AI Strategies by the MDDI, integration of AI policy into broader national digital governance and security frameworks. |
| Extractive capacity | Government of Singapore | Launch of National AI Projects and the Triple Helix Partnership, facilitating collaboration between the state, private sector, and academia to mobilize resources and drive national AI initiatives. |

**Table 4.** (Cont.) An overview of the sovereign AI competition in Singapore.

| | Institutions | Key policies and contents |
|---|---|---|
| Delivery capacity | Singapore Department of Statistics, and other government agencies | Building a national AI ecosystem, introducing a dedicated AI data platform, and developing data concierge services to enhance inter-agency data coordination. |
| Informational capacity | Smart Nation and Digital Government Office, National AI Office, Government Technology Agency, Infocomm Media Development Authority | Establishment of the National AI Office and Government Data Architecture, development of centralized digital infrastructure for public-sector employees, and creation of AI Verify and the AI Verify Foundation to enhance trust and accountability in AI governance. |
| Capability goal | | |
| Singapore aims to foster deeper collaboration within Southeast Asia by developing AI technologies tailored to the region's languages, cultures, and values. By focusing on localized AI models, Singapore seeks to bridge gaps between regional countries and build a unified technological ecosystem that reflects Southeast Asia's diversity, consolidating its leadership in regional digital development. | | |

## 4. Conclusion

By integrating contemporary AI development with classical state formation theory, this study offers a novel perspective on the geopolitical implications of generative AI. We introduce the Generative AI-Making and State-Making framework to explain how sovereign AI competition reshapes state capacity and digital geopolitics. Our comparative analysis of the US, France, Brazil, and Singapore illustrates that the emergence of LLMs has accelerated international competition as nations acknowledge AI's transformative potential. The findings suggest that, under the strategic pressures and opportunities of generative AI, elite consensus drives the enhancement of state capacities across four dimensions: coercive, extractive, delivery, and informational. However, the objectives and intensity of this capacity-building vary according to a nation's position in the international system, its geopolitical pressure, and its unique endowments. Table 5 provides an overview of the distinct capacity-building paths and strategic objectives of the four cases.

Sovereign AI competition, as a GPT contest spanning geographical and policy boundaries, aligns with state-building theory: intensified external, transboundary competitive pressures catalyze state apparatus development and reinforcement. This framework requires further empirical observation of the evolving global order and refinement of digital-era state capacity concepts and measurement tools. Nonetheless, this study offers two contributions to post-fourth industrial revolution international relations. First, it situates domestic politics within the context of generative AI competition. Current literature (Brown et al., 2023) often overlooks the systemic effects of this prolonged competition on state formation, focusing instead on policy instruments or governance model variations. The universal impact of such competition on nations could exert evolutionary force on the international system, potentially culminating in structural transformation (Tang, 2010). Second, this study offers a geopolitical analysis focused on objective differentiation. Prevailing debates often spotlight great powers like the US and China while overlooking middle powers (Schindler et al., 2024; Schmid et al., 2025). However, as exemplified by Singapore, sovereign AI competition extends beyond "a game of titans." Intensifying AI rivalry also drives technologically capable

**Table 5.** Comparison of the sovereign AI competition approaches in the four cases.

| Sample countries | US | France | Brazil | Singapore |
|---|---|---|---|---|
| Coercive capacity | Using coercive measures to directly intervene in markets and enterprises | Directive-driven prioritization and regulatory governance | Regulation and technological application based on existing institutional frameworks | Cross-departmental policy coordination and market regulation |
| | Very strong | Strong | Moderate | Strong |
| Extractive capacity | Government-backed, policy-committed financing totaling up to $500 billion | Traditional public–private partnership model with a scale exceeding EUR 10 billion | A blended financing mechanism totaling approximately USD 4 billion | Systematic financing based on national AI projects, with a target of approximately USD 10 billion |
| | Very strong | Strong | Moderate | Strong |
| Delivery capacity | Institutional support for AI infrastructure, talent development, and research platforms, with direct expansion of the state apparatus | Establishment of temporary research institutions and optimization of administrative efficiency | Provision of specialized service programs in areas such as education and entrepreneurship | Building an AI ecosystem through dedicated multifunctional institutions and project platforms |
| | Very strong | Moderate | Moderate | Strong |
| Informational capacity | A federal AI advisory system based on the expansion of the state apparatus | Creation of dedicated research advisory bodies and mechanisms for publicity and feedback collection | Establishment of information processing and risk assessment institutions such as the Observatório Brasileiro de Inteligência Artificial | Establishment of new formal institutions such as the National AI Office |
| | Strong | Strong | Strong | Strong |
| Capability goal | Defeating rivals to maintain technological hegemony | Maintaining global technological leadership, technological independence, and regional influence | Preserving regional leadership and developing a Portuguese-language LLM | Becoming a regional technological hub and developing a Southeast Asia–focused LLM |

nations to consolidate linguistic communities via national LLMs (e.g., Brazil in Portuguese, UAE in Arabic; Kerr & Murgia, 2023; MCTI, 2021). This dynamic signals a more complex landscape, with nations competing intensely for regional AI leadership. The growing UAE–Saudi Arabia rivalry—between the two Gulf allies traditionally bound by shared security and economic interests—exemplifies this. Despite their strategic alliance, AI competition fuels an aggressive nation-building race. Saudi Arabia's Vision 2030, for example, identifies AI as a core enabler for achieving up to 70 percent of its national digital transformation objectives, while the UAE established the world's first Minister of State for Artificial Intelligence in 2017 ("Saudi Arabia and UAE," 2025).

Beyond sovereign AI, this study addresses a key theme in the thematic issue. The proposed Generative AI-Making and State-Making framework offers a versatile analytical tool for understanding state responses to technological disruption in the digital age. Its applicability transcends generative AI, extending to the broader spectrum of Web 3.0 technologies. This study's central mechanism—elites' perceptions of transboundary tech competition driving systematic state-building—operates across different technology paradigms. Comparing generative AI and blockchain governance highlights a paradox. While sovereign AI and Web 3.0 embody seemingly opposing logics—state-driven centralization versus socially-driven decentralization—this article argues against a technological determinism concerning geographical impacts. Applying this framework to Web 3.0 governance reveals a fundamental paradox in digital geopolitics. Technologies like blockchain, cryptocurrency, and decentralized autonomous organizations are designed to be decentralized and reduce dependence on state institutions; however, their development, adoption, and regulation remain deeply intertwined with state capacity. Consequently, centralized AI and decentralized Web 3.0 logics, though seemingly opposed, may paradoxically converge in shaping a global digital order characterized by regional multipolarity and an overarching US–China bipolarity.

Sovereign AI enhances state capability through the mandated integration of societal resources. By contrast, the social decentralization enabled by blockchain, while appearing to weaken national sovereignty, paradoxically reinforces it by empowering smaller units and preventing any single actor from achieving global hegemony. Despite these differences, both paradigms demand a comprehensive digital infrastructure, a critical mass of skilled talent, and immense reserves of data, capital, and market access. Fulfilling these prerequisites is contingent upon national capacity—especially extractive, informational, and delivery capabilities. Given that the US and China together account for over 40% of global GDP and 48% of global manufacturing output (Council on Foreign Relations, 2024), they hold a distinct advantage in meeting these demands. Crucially, their escalating strategic competition provides the most potent impetus for both state-building and technological advancement. This dynamic is illustrated by the significant role of figures like David Sacks, who was appointed to the chair of the President's Council of Advisors on Science and Technology and informally referred to as the White House "czar" for AI and cryptocurrency (Schleifer, 2024). Consequently, while the US and China are emerging as poles of digital geopolitics, the multipolar nature of new technologies precludes the rigid bloc formation of the Cold War.

In summary, this study's primary theoretical contribution is an analytical framework for Web 3.0 governance that links the material demands of new technologies to state strategies. It challenges deterministic or anti-state interpretations, showing that governing decentralized systems still requires understanding how geopolitical pressures shape state responses. This explains why Web 3.0 technologies, despite decentralization, display geographic clustering and national advantage similar to centralized technologies (Holicka & Vinodrai, 2022; Zhang & Lu, 2025). For centralized AI, states focus on building domestic industrial capacity and controlling key resources (e.g., advanced semiconductors, large datasets). For decentralized Web 3.0 technologies, statecraft shifts to regulatory frameworks and infrastructure oversight. Ultimately, renewed geopolitical competition drives both: Elites frame tech competition as a zero-sum game requiring greater state intervention (Mueller & Farhat, 2022). Web 3.0 (bottom-up innovation via community/tech trust) and sovereign AI (top-down security via state/legal authority) are distinct but interconnected paradigms. Their adoption reflects each country's state–market–society nexus under geopolitical pressure, not abstract utopian or dystopian visions.

We conclude with a critical reflection on our central concept of "sovereign AI." While articulated in Westphalian terms, this concept, functioning as a "technopolitical imaginary" rather than a legal category, acknowledges digital tech's challenge to traditional sovereignty (Pohle & Thiel, 2020). Despite its limited normative clarity, the concept underscores nation-states' determination to defend domestic authority and external independence amid technological revolution (Oppenheim, 1905). This suggests that international technological and geopolitical competition will continue to revolve around the nation-state. Yet, technological advances are simultaneously reshaping the very substance of sovereignty and interstate relations. As emphasized throughout this article, LLMs increasingly align geopolitical competition with linguistic and ecosystem divides rather than purely territorial concerns. Thus, analyzing policy instruments and technological prowess alone is insufficient for forecasting digital geopolitics. Scholars must "bring the state back in" to the generative AI era. The same holds for Web 3.0: Even in decentralized technological systems, states remain central actors shaping rules, infrastructures, and power distributions. This study therefore contributes not only to debates on sovereign AI but also to the governance challenges of Web 3.0.

## Acknowledgments

The author would like to express sincere gratitude to the editors of this thematic issue for their guidance and support; to the anonymous reviewers for constructive feedback; and to Zhibo Zhang, Qiaoying Tang, and Xiruo Tang for research assistance.

## Funding

This study was supported by the Chinese Academy of Social Sciences' laboratory incubation project (2024SYFH012), and the 2023 Shanghai Morning Light Program.

## Conflict of Interests

The author declares no conflict of interests.

## LLMs Disclosure

This article used the DATGS LLM, developed by Alogorain, for policy text analysis and language polishing.

## Supplementary Material

Supplementary material for this article is available online in the format provided by the author (unedited).

## References

Agamben, G. (2005). *State of exception*. University of Chicago Press.

Ayoob, M. (1995). *The third world security predicament: State making, regional conflict, and the international system*. Lynne Rienner Publishers.

Besley, T., & Persson, T. (2009). The origins of state capacity: Property rights, taxation, and politics. *American Economic Review*, *99*(4), 1218–1244.

Brands, H., & Gaddis, J. L. (2021). The new cold war. *Foreign Affairs*, *100*(6), 10–21.

Bresnahan, T., & Trajtenberg, M. (1992). *General purpose technologies: Engines of economic growth?* (NBER Working Paper No. 4148). National Bureau of Economic Research.

Brown, M. A., Neuberger, J., D'Acunto, F., Raji, A., Sun, C., & Wheeler, T. (2023). *The geopolitics of AI and the rise of digital sovereignty*. Brookings Institution. https://www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty

Bureau of Industry and Security. (2025, January 13). *Biden-Harris administration announces regulatory framework for the responsible diffusion of advanced artificial intelligence technology* [Press release]. U.S. Department of Commerce. https://www.bis.gov/press-release/biden-harris-administration-announces-regulatory-framework-responsible-diffusion-advanced-artificial

Câmara dos Deputados. (2021). *Projeto de Lei nº 21/2020: Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil* (Bill No. 21/2020). http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1853928&filename=PL-21-2020

Centeno, M. A. (2002). *Blood and debt: War and the nation-state in Latin America*. Pennsylvania State University Press.

Centre National de la Recherche Scientifique. (2025, May 14). *Jean Zay supercomputer: France has increased its AI-dedicated resources fourfold* [Press release]. https://www.cnrs.fr/en/press/jean-zay-supercomputer-france-has-increased-its-ai-dedicated-resources-fourfold

Cerny, P. G. (2010). The competition state today: From *raison d'État* to *raison du Monde*. *Policy Studies*, *31*(1), 5–21. https://doi.org/10.1080/01442870903052801

Chang, J. Y. (2022). Not between the devil and the deep blue sea: Singapore's hedging. *International Studies Quarterly*, *66*(3), Article sqac034. https://doi.org/10.1093/isq/sqac034

Chavez, P. (2025, February 13). France pursues an AI "third way." *Center for European Policy Analysis*. https://cepa.org/article/france-pursues-an-ai-third-way

Chui, M., Hazan, E., Roberts, R., Singla, A., Smaje, K., Sukharevsky, A., Yee, L., & Zemmel, R. (2023, June). *The economic potential of generative AI: The next productivity frontier*. McKinsey & Company. https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/the%20economic%20potential%20of%20generative%20ai/the-economic-potential-of-generative-ai-the-next-productivity-frontier.pdf

Collier, D. (1993). The comparative method. In A. W. Finifter (Ed.), *Political science: The state of the discipline II*. American Political Science Association.

Commission de l'Intelligence Artificielle. (2024). *AI : Notre ambition pour la France*. https://www.info.gouv.fr/upload/media/content/0001/09/02cbcb40c3541390be391feb3d963a4126b12598.pdf

Comunidade dos Países de Língua Portuguesa. (n.d.). *CPLP: Comunidade dos Países de Língua Portuguesa*. https://www.cplp.org/id-2752.aspx

Conselho Nacional de Ciência e Tecnologia. (2024). *IA para o bem de todos: Documento do Plano Brasileiro de Inteligência Artificial (PBIA)*. https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/cct/legislacao/arquivos/IA_para_o_Bem_de_Todos.pdf

Council on Foreign Relations. (2024). *The contentious U.S.–China trade relationship*. https://www.cfr.org/backgrounder/contentious-us-china-trade-relationship#:~:text=Think%20Global%20Health&text=Combined%2C%20their%20economies%20comprised%2043,the%20United%20States%2C%20after%20Japan.&text=This%20economic%20reality%20%E2%80%9Cunderscores%20the,trade%20relationship%20in%20recent%20decades

de Almeida, M. H. T., Fernandes, I. F., & de Sá Guimarães, F. (2021). Structuring public opinion on foreign policy issues: The case of Brazil. *Latin American Research Review*, *56*(3), 557–574. https://doi.org/10.25222/larr.876

Eapen, T., Finkenstadt, D. J., Folk, J., & Venkataswamy, L. (2023). How generative AI can augment human creativity. *Harvard Business Review*, *101*(4), 56–64.

Evans, P. B. (1995). *Embedded autonomy: States and industrial transformation*. Princeton University Press.

Filgueiras, F., & Junquilho, T. A. (2023). The Brazilian (non)perspective on national strategy for artificial intelligence. *Discover Artificial Intelligence*, *3*, Article 7. https://doi.org/10.1007/s44163-023-00052-w

Foucault, M. (1991). Governmentality. In G. Burchell, C. Gordon, & P. Miller (Eds.), *The Foucault effect: Studies in governmentality* (pp. 87–104). University of Chicago Press.

French President rallies behind Mistral-Nvidia cloud partnership. (2025, June 11). PYMNTS. https://www.pymnts.com/artificial-intelligence-2/2025/french-president-rallies-behind-mistral-nvidia-cloud-partnership

Freudlsperger, C., & Schimmelfennig, F. (2023). Rebordering Europe in the Ukraine War: Community building without capacity building. *West European Politics*, *46*(5), 843–871.

Friesen, G. (2025, January 23). Trump's AI push: Understanding the $500 billion Stargate Initiative. *Forbes*. https://www.forbes.com/sites/garthfriesen/2025/01/23/trumps-ai-push-understanding-the-500-billion-stargate-initiative

*FUTURE of Artificial Intelligence Act of 2017*, H.R. 4625, 115th Cong. (2017). https://www.congress.gov/bill/115th-congress/house-bill/4625

Generative AI to become a $1.3 trillion market by 2032, research finds. (2023, June 1). *Bloomberg*. https://www.bloomberg.com/company/press/generative-ai-to-become-a-1-3-trillion-market-by-2032-research-finds

Genschel, P. (2022). Bellicist integration? The war in Ukraine, the European Union and core state powers. *Journal of European Public Policy*, *29*(12), 1885–1900.

Ghalehdar, P. (2022). Mill's method of agreement and method of difference as methods of analysis in international relations. In *Oxford research encyclopedia of international studies*. Oxford University Press. https://oxfordre.com/internationalstudies/display/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-701

Gilpin, R. (1981). *War and change in world politics*. Cambridge University Press.

GovTech Singapore. (2017, November 23). *AI Singapore: How a small island plans to bridge AI research and reality*. https://www.tech.gov.sg/technews/ai-singapore-how-a-small-island-plans-to-bridge-ai-research-and-reality

Grzymala-Busse, A. (2020). Beyond war and contracts: The medieval and religious roots of the European state. *Annual Review of Political Science*, *23*(1), 19–36.

Hamm, P., King, L. P., & Stuckler, D. (2012). Mass privatization, state capacity, and economic growth in post-communist countries. *American Sociological Review*, *77*(2), 295–324.

Herbst, J. (2000). *States and power in Africa: Comparative lessons in authority and control*. Princeton University Press.

Holicka, M., & Vinodrai, T. (2022). The global geography of investment in emerging technologies: The case of blockchain firms. *Regional Studies, Regional Science*, *9*(1), 177–179.

Horowitz, M. C. (2018). Artificial intelligence, international competition, and the balance of power. *Texas National Security Review*, *1*(3), 36–57.

Horowitz, M. C., Scharre, P., Allen, G. C., Frederick, K., Cho, A., & Saravalle, E. (2018). *Artificial intelligence and international security*. Center for a New American Security. https://www.cnas.org/publications/reports/artificial-intelligence-and-international-security

Hu, K. (2023, February 2). ChatGPT sets record for fastest-growing user base—Analyst note. *Reuters*. https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01

Hui, V. T. (2017). How Tilly's state formation paradigm is revolutionizing the study of Chinese state-making. In L. B. Kaspersen & J. Strandsbjerg (Eds.), *Does war make states? Investigations of Charles Tilly's historical sociology* (pp. 268–295). Cambridge University Press.

IBISWorld. (2024). *Global internet service providers—Market size (2005–2030)*. https://www.ibisworld.com/global/market-size/global-internet-service-providers/1716

Infocomm Media Development Authority. (2023, June 7). *Singapore launches AI Verify Foundation to shape the future of international AI standards through collaboration* [Press release]. https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/singapore-launches-ai-verify-foundation

Intelligence artificielle: Emmanuel Macron annonce des investissements en France de «109 milliards d'euros dans les prochaines années». (2025, February 9). *Le Monde*. https://www.lemonde.fr/pixels/article/2025/02/09/intelligence-artificielle-emmanuel-macron-annonce-des-investissements-en-france-de-109-milliards-d-euros-dans-les-prochaines-annees_6539115_4408996.html

International Institute for Strategic Studies. (2023). *Large language models: Fast proliferation and budding international competition*. https://www.iiss.org/publications/strategic-comments/2023/large-language-models-fast-proliferation-and-budding-international-competition

Jensen, G. (2024, December 19). We are all mercantilists now. *Bridgewater Associates*. https://www.bridgewater.com/what-trumps-global-order-could-look-like

Jessop, B. (1990). *State theory: Putting capitalist states in their place*. Pennsylvania State University Press.

Jung, D. (2006). War-making and state-making in the Middle East. In D. Jung (Ed.), *Democratization and development: New political strategies for the Middle East* (pp. 3–32). Palgrave MacMillan.

Katzenstein, P. J. (1985). *Small states in world markets: Industrial policy in Europe*. Cornell University Press.

Keohane, R. O. (1969). Lilliputians' dilemmas: Small states in international politics. *International Organization*, *23*(2), 291–310.

Kerr, S., & Murgia, M. (2023, August 30). UAE launches Arabic large language model in Gulf push into generative AI. *Financial Times*. https://www.ft.com/content/ab36d481-9e7c-4d18-855d-7d313db0db0d

Lavery, S. (2024). Rebuilding the fortress? Europe in a changing world economy. *Review of International Political Economy*, *31*(1), 330–353.

Lee, A. (2024, February 28). What is sovereign AI? *NVIDIA Blog*. https://blogs.nvidia.com/blog/what-is-sovereign-ai

Lee, M. M., & Zhang, N. (2017). Legibility and the informational foundations of state capacity. *The Journal of Politics*, *79*(1), 118–132.

LightOn to become Europe's first listed GenAI startup with Paris IPO. (2024, November 8). *Reuters*. https://www.reuters.com/markets/europe/lighton-become-europes-first-listed-genai-startup-with-paris-ipo-2024-11-08

Malamud, A. (2011). A leader without followers? The growing divergence between the regional and global performance of Brazilian foreign policy. *Latin American Politics and Society*, *53*(3), 1–24. https://doi.org/10.1111/j.1548-2456.2011.00123.x

Mann, M. (1984). The autonomous power of the state: Its origins, mechanisms and results. *European Journal of Sociology/Archives européennes de sociologie*, *25*(2), 185–213.

Marquette, H., & Beswick, D. (2011). State building, security and development: State building as a new development paradigm? *Third World Quarterly*, *32*(10), 1703–1714.

Maslej, N., Fattorini, L., Perrault, R., Parli, V., Reuel, A., Brynjolfsson, E., Etchemendy, J., Ligett, K., Lyons, T., Manyika, J., Niebles, J. C., Shoham, Y., Wald, R., & Clark, J. (2024). *The AI Index 2024 annual report*. AI Index Steering Committee, Institute for Human-Centered Artificial Intelligence, Stanford University. https://hai.stanford.edu/assets/files/hai_ai-index-report-2024-smaller2.pdf

Mazzucato, M. (2011). The entrepreneurial state. *Soundings*, *49*(49), 131–142.

Mazzucato, M. (2018). Mission-oriented innovation policies: Challenges and opportunities. *Industrial and Corporate Change*, *27*(5), 803–815.

Mikhaylov, S. J., Esteve, M., & Campion, A. (2018). Artificial intelligence for the public sector: Opportunities and challenges of cross-sector collaboration. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2128), Article 20170357.

Mill, J. S. (1978). *A system of logic, ratiocinative and inductive*. University of Toronto Press.

Ministério da Ciência, Tecnologia e Inovações. (2021). *Estratégia Brasileira de Inteligência Artificial (EBIA)*. https://lapin.org.br/wp-content/uploads/2021/04/Estrategia-Brasileira-de-Inteligencia-Artificial.pdf

Ministry of Communications and Information. (2019). *National Artificial Intelligence Strategy: Advancing our smart nation journey*. Government of Singapore.

Ministry of Communications and Information. (2023). *National Artificial Intelligence Strategy 2.0: AI for the public good for Singapore and the world*. Government of Singapore.

Mueller, M. L., & Farhat, K. (2022). Regulation of platform market access by the United States and China: Neo-mercantilism in digital services. *Policy & Internet*, *14*(2), 348–367.

National Artificial Intelligence Initiative Act of 2020, H.R. 6216, 116th Cong. (2020). https://www.congress.gov/bill/116th-congress/house-bill/6216

National Security Commission on Artificial Intelligence. (2021). *Final report*. https://reports.nscai.gov/final-report/table-of-contents

National Science Foundation. (2023a). *NSF announces 7 new National Artificial Intelligence Research Institutes*. https://www.nsf.gov/news/nsf-announces-7-new-national-artificial

National Science Foundation. (2023b). *NSF partners to kick off NAIRR pilot program*. https://www.nsf.gov/news/nsf-partners-kick-nairr-pilot-program

National Science Foundation. (2023c). *NSF launches EducateAI initiative*. https://www.nsf.gov/news/nsf-launches-educateai-initiative

Oppenheim, L. (1905). *International law: A treatise* (Vol. 1). Longmans, Green, and Co.

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, *9*(4), 2–19. https://doi.org/10.14763/2020.4.1532

Présidence de la République Française. (2025). *Make France an AI powerhouse*. https://www.elysee.fr/admin/upload/default/0001/17/d9c1462e7337d353f918aac7d654b896b77c5349.pdf

Prime Minister's Office of Singapore. (2023, December 4). *Speech by Deputy Prime Minister and Minister for Finance Lawrence Wong at the Singapore conference on AI for the global good* [Speech transcript]. https://www.pmo.gov.sg/Newsroom/DPM-Lawrence-Wong-at-the-Singapore-Conference-on-AI-for-the-Global-Good

Radu, R. (2021). Steering the governance of artificial intelligence: National strategies in perspective. *Policy and Society*, *40*(2), 178–193.

Reinhard, W. (Ed.). (1996). *Power elites and state building*. Oxford University Press.

République Française. (2021, November 8). *Stratégie nationale pour l'intelligence artificielle – 2e phase : dossier de presse*. Ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation ; Ministère de l'Économie, des Finances et de la Relance. https://www.enseignementsup-recherche.gouv.fr/sites/default/files/2021-11/dossier-de-presse---strat-gie-nationale-pour-l-intelligence-artificielle-2e-phase-14920.pdf

Roberts, H., Hine, E., Taddeo, M., & Floridi, L. (2024). Global AI governance: Barriers and pathways forward. *International Affairs*, *100*(3), 1275–1286.

Satariano, A., & Mozur, P. (2024, August 14). The global race to control A.I.. *The New York Times*. https://www.nytimes.com/2024/08/14/briefing/ai-china-us-technology.html

Saudi Arabia and UAE vie for Middle East AI supremacy. (2025, June 9). *PYMNTS*. https://www.pymnts.com/artificial-intelligence-2/2025/saudi-arabia-and-uae-vie-for-middle-east-ai-supremacy

Schindler, S., Alami, I., DiCarlo, J., Jepson, N., Rolf, S., Bayırbağ, M. K., Cyuzuzo, L., DeBoom, M., Farahani, A. F., Liu, I. T., McNicol, H., Miao, J. T., Nock, P., Teri, G., Vila Seoane, M. F., Ward, K., Zajontz, T., & Zhao, Y. (2024). The second cold war: US–China competition for centrality in infrastructure, digital, production, and finance networks. *Geopolitics*, *29*(4), 1083–1120.

Schleifer, T. (2024, December 5). Trump names top Silicon Valley conservative to oversee crypto and A.I. *The New York Times*. https://www.nytimes.com/2024/12/05/us/politics/david-sacks-crypto-ai-trump.html

Schmid, S., Lambach, D., Diehl, C., & Reuter, C. (2025). Arms race or innovation race? Geopolitical AI development. *Geopolitics*, *30*(4), 1907–1936.

Schmidt, E. (2022). AI, great power competition & national security. *Daedalus*, *151*(2), 288–298. https://doi.org/10.1162/daed_a_01916

Schrepel, T., & Pentland, A. (2024). Competition between AI foundation models: Dynamics and policy recommendations. *Industrial and Corporate Change*. Advance online publication. https://doi.org/10.1093/icc/dtae042

Seawright, J., & Gerring, J. (2008). Case selection techniques in case study research: A menu of qualitative and quantitative options. *Political Research Quarterly*, *61*(2), 294–308.

Seidl, T., & Schmitz, L. (2024). Moving on to not fall behind? Technological sovereignty and the 'geo-dirigiste' turn in EU industrial policy. *Journal of European Public Policy*, *31*(8), 2147–2174.

Sharma, V. (2017). Beyond the Tilly thesis: "Family values" and state formation in Latin Christendom. In L. B. Kaspersen & J. Strandsbjerg (Eds.), *Does war make states? Investigations of Charles Tilly's historical sociology*. Cambridge University Press.

Singapore builds AI model to 'represent' Southeast Asians. (2024, February 8). *Bangkok Post*. https://www.bangkokpost.com/life/tech/2738624/biased-gpt-singapore-builds-ai-model-to-represent-southeast-asians

Singapore pioneers flagship AI initiative to develop South-East Asia's first large language model ecosystem. (2023, December 19). *Allen & Gledhill*. https://www.allenandgledhill.com/sg/publication/articles/26930/pioneers-flagship-ai-initiative-to-develop-south-east-asia-s-first-large-language-model-ecosystem

Singla, A., Sukharevsky, A., Yee, L., Chui, M., & Hall, B. (2025). *The state of AI: How organizations are rewiring to capture value*. McKinsey & Company.

Spruyt, H. (1994). *The sovereign state and its competitors: An analysis of systems change*. Princeton University Press.

Swanson, A. (2024, December 2). Biden targets China's chip industry with wider trade bans. *The New York Times*. https://www.nytimes.com/2024/12/02/business/economy/biden-china-chips-exports.html

Tang, S. (2010). Social evolution of international politics: From Mearsheimer to Jervis. *European Journal of International Relations*, *16*(1), 31–55.

Tang, S. (2022). The new development triangle: State capacity, institutional foundation, and socioeconomic policy. In H.-J. Chang (Eds.), *The institutional foundation of economic development* (pp. 180–207). Princeton University Press.

Teo, A. G., & Koga, K. (2022). Conceptualizing equidistant diplomacy in international relations: The case of Singapore. *International Relations of the Asia-Pacific*, *22*(3), 375–409. https://doi.org/10.1093/irap/lcab011

The French government creates a national institute to assess and secure AIs. (2025, January 31). *Campus*

*France*. https://www.campusfrance.org/en/actu/creation-d-un-institut-national-pour-l-evaluation-et-la-securite-de-l-ia

The White House. (2017). *National security strategy of the United States of America*. https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

The White House. (2019, February 14). *Executive Order 13859: Maintaining American leadership in artificial intelligence* (Federal Register 84 FR 3967). https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence

The White House. (2024, April 29). *Biden–Harris administration announces key AI actions 180 days following President Biden's landmark executive order* [Press release]. https://www.whitehouse.gov/briefing-room/statements-releases/2024/04/29/biden-harris-administration-announces-key-ai-actions-180-days-following-president-bidens-landmark-executive-order

The White House. (2025a). *Executive Order 14141: Advancing United States leadership in artificial intelligence infrastructure* (Federal Register 90 FR 5469). https://www.federalregister.gov/documents/2025/01/17/2025-01395/advancing-united-states-leadership-in-artificial-intelligence-infrastructure

The White House. (2025b). *Executive Order 14179: Removing barriers to American leadership in artificial intelligence*. https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence

Thies, C. G. (2004). State building, interstate and intrastate rivalry: A study of post-colonial developing country extractive efforts, 1975–2000. *International Studies Quarterly*, *48*(1), 53–72.

Tilly, C. (1985). War making and state making as organized crime. In P. B. Evans, D. Rueschemeyer, & T. Skocpol (Eds.), *Bringing the state back in* (pp. 169–191). Cambridge University Press.

Tilly, C. (1992). *Coercion, capital, and European states: AD 990–1992*. Blackwell.

Tzagkarakis, S. I., & Kritas, D. (2023). Mixed research methods in political science and governance: Approaches and applications. *Quality & Quantity*, *57*(Suppl. 1), 39–53.

U.S. Department of Defense. (2023, August 10). *DOD announces establishment of generative AI task force* [Press release]. https://www.defense.gov/News/Releases/Release/Article/3489803/dod-announces-establishment-of-generative-ai-task-force

U.S.–China Economic and Security Review Commission. (2024). *2024 annual report to Congress*.

Ulnicane, I. (2022). Against the new space race: Global AI competition and cooperation for people. *AI & Society*, *38*(2), 681–683. https://doi.org/10.1007/s00146-022-01423-0

UNESCO. (n.d.). *Brazil*. https://www.unesco.org/ethics-ai/en/brazil

Vance, J. D. (2025). *Read J.D. Vance's full speech at the AI Summit in Paris* [Speech transcript]. The Spectator. https://thespectator.com/topic/read-j-d-vance-full-speech-ai-summit-paris

Villani, C. (2018). *Donner un sens à l'intelligence artificielle: Pour une stratégie nationale et européenne*. La Documentation Française. https://www.vie-publique.fr/files/rapport/pdf/184000159.pdf

Von Ingersleben-Seip, N. (2023). Competition and cooperation in artificial intelligence standard setting: Explaining emergent patterns. *Review of Policy Research*, *40*(5), 781–810.

Vu, T. (2010). Studying the state through state formation. *World Politics*, *62*(1), 148–175.

Waltz, K. N. (1979). *Theory of international politics*. Addison-Wesley.

Weiss, L. (1997). Globalization and the myth of the powerless state. *New Left Review*, *225*, 3–27.

Weiss, L., & Thurbon, E. (2021). Developmental state or economic statecraft? Where, why and how the difference matters. *New Political Economy*, *26*(3), 472–489.

Welcome to the era of AI nationalism. (2024, January 1). *The Economist*. https://www.economist.com/business/2024/01/01/welcome-to-the-era-of-ai-nationalism

Zhang, H., & Lu, Y. (2025). Web 3.0: Applications, opportunities and challenges in the next internet generation. *Systems Research and Behavioral Science*, *42*(4), 996–1015.

## About the Author

Zhenyu Wang studies digital geopolitics and AI for social science, as an assistant professor at the Journalism Institute, Shanghai Academy of Social Sciences. He is also a researcher at the Digital Civilization and Intelligent Decision-Making Laboratory, University of Chinese Academy of Social Sciences, and is the CEO of Alogorain, an AI start-up focusing on research and decision support.

Politics and Governance
2025 • Volume 13 • Article 10243
https://doi.org/10.17645/pag.10243

cogitatio

ARTICLE

Open Access Journal

# Reconceptualizing Technological Leadership: A Relational and Dynamic Framework

Yuanyuan Fang [1] and Shenghao Zhang [2]

[1] School of International Politics and Communication, Beijing Language and Culture University, China
[2] Institute for International Relations, Tsinghua University, China

**Correspondence:** Shenghao Zhang (shenghaozhang@tsinghua.edu.cn)

**Submitted:** 28 February 2025 **Accepted:** 4 September 2025 **Published:** 29 October 2025

**Issue:** This article is part of the issue "Technology and Governance in the Age of Web 3.0" edited by Chang Zhang (Communication University of China), Zichen Hu (London School of Economics and Political Science), and Denis Galligan (University of Oxford), fully open access at https://doi.org/10.17645/pag.i443

## Abstract

This article challenges conventional economic-based understandings of technological leadership, which often conflate technological leadership with innovation capability or leading status in the technology sector. Instead, it develops a relational and dynamic framework for understanding technological leadership from an IR perspective. It introduces a novel typology differentiating leadership from leading, and followership from imitation and purchase. Technological leadership is defined as the relational and dynamic process through which a state establishes and sustains influence by setting and enforcing rules, standards, and frameworks that guide innovation and collaboration within a technological ecosystem. The formation of technological leadership is a complex and dynamic process, involving interaction between leaders, followers, and the technological environment, shaped by leadership behaviors, followers' choices, and technological context. This article applies the proposed framework to examine the US–China rivalry for global leadership in artificial intelligence. Through a systematic analysis of AI-related policy documents from both nations spanning the period from 2016 to 2025, the study elucidates how these two major powers have formulated their respective AI leadership strategies and influenced the evolution of global AI governance. The analysis reveals that US leadership in AI is characterized by a dual-focused approach that integrates technological advancement with value-oriented governance, manifesting through three key dimensions: ethical governance frameworks, international collaborative initiatives, and strategic competitive measures. China's leadership behavior, adhering to the principle of mutual benefit, manifests primarily through infrastructure development and standard-setting, adopting a development-centric approach. However, the formation of technological leadership is not solely determined by US and Chinese strategies but is equally influenced by the strategic choices of follower states. Consequently, the ultimate trajectory of the US–China rivalry in AI leadership will predominantly depend on both nations' capacity to attract and maintain follower support.

**Keywords**
AI governance; leadership theory; norm-building; technological leadership; US–China rivalry

## 1. Introduction

Technology is an important component in IR (D. W. Drezner, 2019). Scholars argue that technological revolutions can empower economic and military strength, thereby facilitating power transition (Freeman, 1995; Gilpin, 1981; Kennedy, 1987; Porter, 1990). Fast-evolving technology, particularly AI, has fundamentally reshaped the global geopolitical landscape, reflecting the intensifying competition among states for dominance in emerging technological domains. As a result, the concept of technological leadership has emerged a central focus in IR scholarship. However, it is typically assumed that countries with strong innovation capabilities or skills hold technological leadership, and therefore, the focus is mostly on identifying and comparing the factors that drive a nation's innovation capacity (e.g., D. W. Drezner, 2019; Ding, 2024b; Porter, 1990). This perspective, however, remains incomplete. It still does not explain why a country with strong technological advancements, such as China, with its 5G and Deepseek technologies, faces bans from many other countries. In this context, does the country holding the technology possess leadership, or is it the banning country (the US) that holds the leading power? Also, what constitutes true technological leadership in the context of global power dynamics?

Existing research on international political leadership has predominantly focused on macro-level analyses, emphasizing broad power structures, hegemonic transitions, and the role of major states or institutions in shaping the global order (Ikenberry, 2001; Keohane, 1984; Nye, 1990; Schweller & Pu, 2011; Yan, 2011). While these studies provide valuable insights into the distribution of power and the dynamics of international relations, they often overlook the intricate and context-specific mechanisms that define leadership within specialized domains. As Nye (2011, p. 231) states, in a global information age, power is becoming more diffuse, and leadership is becoming more contextual. No country can dominate across all issues, and the ability to exercise power depends heavily on the context of the situation. The logic of leadership varies significantly across different domains. Against this backdrop, this study focuses on technological leadership, a domain that has become increasingly central to global power dynamics in the digital age.

This research seeks to address this question by challenging the conventional economic-centric view of technological leadership, which equates leadership with innovation capability or market dominance. Instead, we propose a relational and dynamic framework for understanding technological leadership, emphasizing the interplay between leaders, followers, and the technological environment. Drawing on leadership theory (Burns, 1978; Nye, 2008), we argue that technological leadership is not merely about being ahead in innovation but about the ability to set and enforce rules, standards, and frameworks that guide global technological ecosystems. This framework shifts the focus from static measures of technological capability to the dynamic processes of influence and norm-setting in international relations.

This article contributes to the existing literature in three ways. First, it offers a novel conceptualization of technological leadership as a relational and dynamic process, distinct from mere technological capability. Second, it highlights the issue-specific nature of leadership, allowing for a nuanced comparison of US and Chinese strategies in AI governance. Third, it underscores the importance of follower choices in determining

the success of leadership strategies, as nations align with the model that best serves their national interests. Via examination of the US–China rivalry for global leadership in AI, this article sheds light on the broader implications of technological leadership for global governance and power dynamics in the 21st century. By integrating conceptual clarity, theoretical innovation, and empirical analysis, this study aims to advance scholarly understanding of technological leadership and its implications for global power dynamics.

Technological leadership, while a critical subject of inquiry, is conceptually ambiguous and demands rigorous examination. Therefore, this article begins by addressing these foundational conceptual issues, drawing on the existing literature to interrogate and refine the definition of technological leadership: What constitutes technological leadership, and how can it be systematically distinguished from related concepts such as technological dominance or innovation capacity? Building on this conceptual groundwork, this article introduces an alternative relational and dynamic conceptual framework, distinguishing between leadership and mere technological capability. We then apply this framework to the US–China rivalry for global leadership in AI, analyzing how each country mobilizes leadership through governance strategies, regulatory frameworks, and geopolitical alignments. Finally, this article concludes by summarizing key findings, discussing implications for global technological competition, and outlining avenues for future research.

## 2. Economic Centric Approach of Technological Leadership

Early discussions of technological leadership emerged in the context of public policy and management studies, often equating it with a country's or firm's ability to lead technological innovation and investigate whether it will contribute to a country's economy. Scholars such as Freeman (1987, 1995) emphasize the role of national innovation systems in fostering technological leadership, highlighting the interplay between government policies, corporate R&D, and educational institutions. In this view, technological leadership was primarily understood as the ability to produce and commercialize cutting-edge technologies, giving states or firms a competitive edge in global markets. Technological leadership, then, is often measured or evaluated through four factors: R&D intensity, R&D inputs and outputs, number of scientific publications, and patents (Huang & Sharif, 2016). R&D related data, market share in leading sectors, and other economic growth indices have been widely used as evidence of the rise and fall of British, American, and Japanese technological leadership (Kindleberger, 1961; Kranzberg & Pursell, 1967; Maddison, 1982; Mokyr, 1990).

From the international political economy perspective, Gilpin (1981) argues that a country's dominance in key leading technological sectors drives significant economic and political advantages, sustaining an empire or hegemony. However, the loss of technological dominance, i.e., the transfer of advanced techniques from more developed societies to less developed ones, especially in modern society, is a key driver of the redistribution of power in an international system (Gilpin, 1981, p. 180). Compared with Gilpin's emphasis on maintaining dominance over key technology, long-cycle theorists (e.g., Modelski, 1987; Modelski & Thompson, 1988; Thompson, 1990) suggest a cyclical nature of global power transitions driven by technological innovations. The rise and fall of power may depend on the same technology, driven by its breakthrough, diffusion, and eventual decline. Thus, the future of global leadership will depend on which countries and sectors lead the next wave of technological innovation.

Much of the subsequent literature follows suit by identifying and comparing factors contributing to technological innovation within great powers. Some focus on the domestic institutions. Olson (1982) finds

that political stability forms special interest groups that pursue narrow, rent-seeking goals, therefore hindering innovation. D. Drezner (2001) argues that decentralized state structures are better at fostering innovation and maintaining hegemony because centralized systems are more likely to make errors, which cannot be reversed at the local level. Focusing on Japan's success, Kitschelt (1991) argues that rather than imposing a successful formula, the industrial governance structures need to match the properties of new technologies to achieve innovation success. Rosenberg (1992) argues that innovation is unpredictable, and no single entity can foresee which technologies will succeed. He therefore suggests that a system with multiple, independent experiments is more likely to uncover successful innovations.

Scholars' interest in technology innovation is not only in leading sectors, but also in the diffusion of technology. Challenging the conventional wisdom of monopolizing innovation in new, fast-growing industries (leading sectors), Ding (2024b) argues that general-purpose technologies (GPTs) are foundational innovations that enhance economic productivity after a lengthy process of spreading across various sectors. He argues (Ding, 2024a, p. 190) that "innovation laggards can be diffusion leaders" and compared with the US, China has limited capability to transform new technologies into standardized products across various sectors. In contrast, its diffusion efforts may be more focused on market-seeking strategies (Huang & Sharif, 2016). Huang and Sharif (2016) argue that, compared with the US, China has an edge in technological leadership from its big domestic and overseas markets and low-cost forms of innovation (Losacker & Liefner, 2020).

Though the concept of technological leadership has been widely discussed, there are limitations within the technological leadership literature. First, technological leadership is similar to hegemonic leadership literature, which emphasizes the capabilities of a country rather than its relational influence. Relying on its unprecedented structural material capacity, a hegemon can exert influence on other countries (Russett, 1985; Strange, 1987). Similarly, by relying on its technological capabilities (including a monopoly on leading sectors, diffusion transformation capability, market resources, and R&D or patent outputs), a country can set the norm to influence other countries. However, it does not explain why Huawei technologies, with its cost-effective performance, has been banned by the US, a ban that has since been followed by many other countries.

Second, the existing technological leadership may conflate the supplier-customer and creator-imitator relationship with a political mobilization relationship. Much of the literature or policy papers frame the US–China tech-rivalry in competing for technological leadership, because China accesses many overseas markets, implying China possesses strong technological leadership (e.g., Wu, 2024). Or when countries or companies imitate the advanced competitors' products, the advanced competitors hold strong leadership. We argue that the commercial relationship does not equate with the power of mobilization, i.e., technological leadership. Whether a country holds technological leadership depends on whether a norm is set and whether followers accept the norm.

Third, the existing literature, especially literature on great powers' global leadership, tends to treat technology as a subordinate element of the economy. Given that technology empowers economic and military strength, we would expect that technological leadership will go hand-in-hand with leadership in other domains, contributing to the overall global leadership. However, the US's ban on China's technology may suggest that technological leadership may harm its liberal economic leadership and its global leadership overall (Ryan & Burman, 2024).

## 3. A Relational and Dynamic Framework of Technological Leadership

We follow a relational and dynamic leadership concept from the prevailing leadership literature, which has predominantly focused on the dynamic interplay between leaders and followers within contexts (Avolio et al., 2009; Hollander, 1992; Northouse, 2021). Leadership is not a fixed national attribute defined solely by a country's capacity to innovate, nor is it—following Burns' critique—merely the exercise of authority to compel compliance (Burns, 1978, p. 19) or the manipulation of followers to serve the leader's interests (Burns, 1978, p. 449). It is closer to Nye's (2008, p. xi) concept, "a social relationship with three key components": leaders (individuals or entities with positional or personal influence), followers (those who choose to align with or respond to leadership), and the domain of interaction (the specific issue, task, or context in which leadership is exercised). We see leadership, at its core, as a relational and interactive process that involves influencing others to achieve shared goals in a specific context.

While the broader leadership literature offers a clear and well-developed understanding of leadership as a relational and dynamic process, the technological leadership literature often deviates from this foundation, conflating leadership with being ahead and imitation/procurement with followership. To address these conceptual misunderstandings, we begin this section by analysing how leadership and followership are commonly misrepresented in the technological domain. We then summarize these issues into a nuanced framework, presented in Figure 1, which distinguishes between different behavioral patterns associated with leadership and followership. Building on this clarification, we introduce our conceptualization of technological leadership and explore the key factors that shape its interdependent components.

From the leader's perspective, the difference between leading and leadership is often overlooked, with technological advances mistakenly seen as leadership. Leadership is about fostering mutual purpose and aligning the values and motivations of both leaders and followers, rather than merely exercising a leading advantage. In contrast, being ahead, whether in technology, market position, or innovation, is often a result of competitive advantage or resource superiority, which does not inherently involve the relational and motivational dimensions that define true leadership. An Olympic champion, by virtue of their exceptional athletic abilities and skills, may achieve a leading position in their sport, but this does not inherently make them a leader among their competitors. For example, Usain Bolt, widely regarded as the fastest sprinter in history, dominated the 100-meter and 200-meter events for over a decade, setting world records and winning multiple Olympic gold medals. However, fellow competitors will not regard him as their leader. In another case, Sebastian Coe is a two-time Olympic gold medalist in the 1500 meters (1980 and 1984). He became President of World Athletics and chaired the London 2012 Olympic Games Organizing Committee. In these roles, he has driven reforms to strengthen the sport's integrity, promote gender equality, and shape its future (Salguero, 2024). Coe's journey illustrates that leadership involves leveraging influence to inspire change and leave a lasting impact—not just individual success.

Microsoft, once known for dominating personal computing through products like Windows and Office, was often criticized in the 1990s and early 2000s for its monopolistic practices and limited collaboration with the industry (Cusumano, 2004). This changed under CEO Satya Nadella from 2014, who shifted Microsoft's focus from competition to broader industry leadership. Key initiatives include: (a) embracing open-source platforms like GitHub and supporting collaborative innovation (Microsoft, 2018); (b) expanding Azure to lead in cloud computing, which competes directly with Amazon Web Services and sets standards for cloud

security, interoperability, and sustainability; and (c) promoting ethical AI and accessibility through initiatives like AI for Good, which tackles global challenges by expanding access to digital skills, supporting education, and collaborating with researchers to develop impactful solutions, highlighting Microsoft's commitment to societal benefit (High, 2025). This transformation shows that while innovation drives technical success, it is not a necessary and sufficient condition for forming technological leadership; shaping standards and fostering collaboration matter too.

In the 19th century, Germany emerged as a dominant country in the global chemical industry, driven by strong academic-industrial collaboration, breakthroughs in organic chemistry, and innovations in synthetic dyes and pharmaceuticals (D. Drezner, 2001; Moe, 2007). However, Germany's chemical production model—which relied heavily on highly trained chemists and artisanal batch processes—did not diffuse widely to other nations. Instead, it was the US that institutionalized the discipline of chemical engineering, thus becoming the global leader in the chemical sector (Ding, 2024a, 2024b).

From the follower's perspective, treating imitation or purchase as a behavior of following is also problematic. Rogers (2003) regards innovation diffusion as a process through which an innovation spreads within a social system. Products spread and are adopted by more individuals and organizations. They gradually achieve market share. Market share is therefore used as a metric to demonstrate a country's economic and technological leadership, because it may reflect consumers' acceptance and shifted market dynamics. However, the act of purchasing a product does not imply that the consumer is aligned with or willing to follow the seller's vision or direction. Similarly, imitation is also not followership. According to a Levitt (1966), innovative imitation is a strategic choice for companies. When new and successful technology emerges in the market, other companies may imitate it to keep up with the competition. However, it also does not mean that imitators follow the vision of those they imitate. For example, during the mid-20th century, Japan actively engaged in imitating American technology, particularly in key industries such as automotive manufacturing and electronics. Japanese companies like Toyota meticulously studied American production techniques, including Ford's assembly line system, and even imported American machinery to replicate their processes (Womack et al., 1990). However, Japan's objective was not to follow the US as a leader; rather, Japan surpassed it. By embracing kaizen (continuous improvement) and focusing on innovation, Japanese companies transformed imitative technologies into superior products. Moreover, Japan redefined global standards in the automotive manufacturing and electronics industries.

Figure 1 summarizes the above arguments and offers a nuanced framework for distinguishing behaviors associated with technological leadership at the state level. Much of the literature illustrates behaviors in the right panel, which are essentially non-relational, competition-oriented, and detached from power-based dynamics. A country with a strong technological capability is leading *per se* in terms of its products, but not necessarily relationally engaged with other countries, as is the case for Germany and the US. Conversely, a country with weak technological capabilities may imitate or acquire technologies from a more advanced country, but the engagement is non-power-based, because weak countries do not necessarily follow the leading countries' vision or standard. Furthermore, it is a competition-oriented relationship, mostly driven by the market. Imitators may replicate technologies or business models to capture market share; procurers may adopt these innovations to strengthen their own capabilities. Despite the innovation inspired by competition, it creates an environment where alliances are fluid, unstable, and temporary, and rivalries are prevalent.

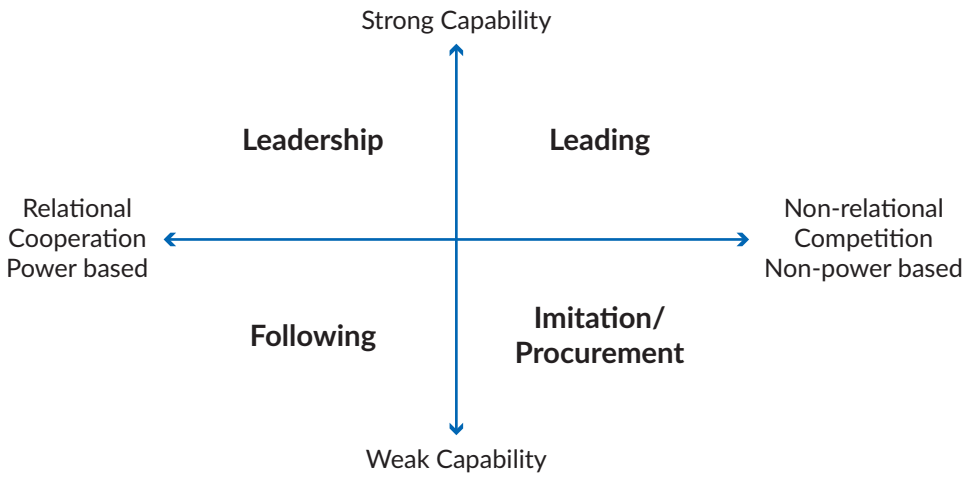



**Figure 1.** Behavioral typologies in the technology sector.

Technology leadership is fundamentally a collaborative and power-based relationship between leaders and followers, as seen in Figure 1's left panel. Leaders provide public goods such as technological standards, an innovation framework, and market stability, which benefit both themselves and their followers. In return, followers align with leaders, contributing to the ecosystem's growth while relying on the leader's direction and resources. In the technology sector, leaders must also offer value creation to sustain their influence. This includes access to cutting-edge technologies and collaborative platforms that enable followers to innovate and compete effectively, rather than preventing competition from the followers. As noted in the previous case, Microsoft provides open-source tools, cloud infrastructure, and developer ecosystems that empower smaller firms and startups, strengthening its role as a technological leader. In short, the right panel portrays a leading entity's static technological capability, and adopts a fluid and unstable competition driven by the market, while the left panel shows an interdependent structure and a relational and dynamic process. A state leader builds and sustains influence by setting norms and shaping standards to encourage collaboration and innovation. It aligns followers with shared goals, provides public goods like technological infrastructure and market stability, and fosters cooperation while maintaining a power-based yet mutually beneficial relationship with stakeholders.

Given that country's technological leadership is a complex and dynamic process shaped by interactions among leaders, followers, and the technological environment, we dissect it into core components: the leader's fundamental qualities and behaviors, the choices of followers, and the influence of the broader technological context. These elements interact and shape one another, collectively driving the formation and evolution of technological leadership. We analyze each in detail in the subsequent paragraphs.

Regarding states' leadership behavior, we argue that it is determined by technological capability and internal drive to lead. Innovation is the core driver of technological advancement. A state's innovation ability enables the creation of new technologies and enhances the evolution of current technologies, granting the state the potential to shape the broader technological ecosystem. States often face a dilemma: whether to protect their technological advantages by keeping innovations proprietary or to open their technologies to promote global standards, even at the risk of economic loss. While protecting innovations may secure short-term competitive advantages, openness can establish long-term leadership and influence. Ultimately, a state's internal drive for leadership is to maximize its national interests, encompassing not only short-term economic benefits but also

long-term considerations such as strategy, security, geopolitics, and global influence. A country will assume leadership when it believes this will safeguard its national interests.

State leaders establish their technological leadership not only through technological superiority but also by leading behaviors such as setting rules, providing public goods, and shaping a compelling vision for the future. Their influence depends on creating value and profit for followers, thereby fostering a collaborative and sustainable ecosystem. By setting technical standards and industry norms, they embed their technologies and values into the international order, securing long-term strategic influence. They also supply public goods, including technological infrastructure, innovation platforms, and an open market, to attract followers' collaboration. Additionally, these leaders inspire collective action by promoting visions aligned with global challenges and opportunities, attracting followers with similar goals and values.

As leadership is a relational process, it cannot only be formed by leaders. The choice of following countries is also important in technological leadership. We argue that it is influenced by technological and economic interests, and political and security considerations.

First, following countries need to balance their technological needs with economic interests when deciding on cooperation. Technological requirements often dictate the scope of engagement with leading countries. Developing countries seek partnerships with technologically advanced countries to bridge the technological gap. China, with its rapid advancements and cost-effective solutions, has become an attractive partner for many developing nations. The *Digital Silk Road* initiative exemplifies this dynamic. Southeast Asian countries choose to follow China in this framework to modernize their digital infrastructure, including high-speed broadband networks and data centers (Mochinaga, 2021). Economic interests, such as market access and investment opportunities, are also crucial. The EU, while economically advanced, recognizes the strategic value of partnering with the US in technology. Such collaborations offer access to American capital and markets, enabling European tech firms to expand operations, boost revenues, and improve competitiveness globally.

Second, political interests and security concerns shape followers' decisions. Strong political alliances often drive collaborative efforts, as shared strategic interests create a foundation of trust and mutual benefit. For example, Japan, as a key ally of the US, actively engages in joint technological initiatives, especially in emerging fields like quantum computing. This cooperation is propelled not only by technological and economic considerations but by shared political interests. Nations may distance themselves from leading powers if there are conflicting political or security interests. For example, countries opposing a leader's political or economic policies might avoid collaboration to prevent being perceived as aligned with that leader's political ideology. Such tensions can hinder technological and economic cooperation, as broader political objectives outweigh short-term technological gains. Furthermore, technologies like information systems and telecommunications carry both economic and security risks. Follower countries must ensure that their partnerships do not jeopardize national security. In the 5G domain, for example, countries evaluate potential security risks linked to foreign-made equipment and choose partners based on security assurances and reputations for safeguarding sensitive data. The US's campaign against Huawei's 5G technology is a typical example to illustrate political interests and security concerns considered by follower countries. Due to concerns about national security and the potential for Chinese government surveillance, many Western countries, including the UK, Australia, and Canada, have restricted or outright banned Huawei's participation

in 5G infrastructure projects. Political and ideological differences between the US and China and national security concerns have thus created a rift in technological collaboration, which will eventually affect European countries' choice, despite Huawei's advancement in 5G innovation and the economic growth it potentially generates for them (Friis & Lysne, 2021; Zhang, 2024).

In short, the technological cooperation choices of follower countries stem from a multi-dimensional evaluation of technological and economic, political, and security factors. Driven by these considerations, while some commit to a single bloc, others might adopt hedging strategies to balance competing interests and mitigate risks. These nations diversify their technological partnerships across multiple leading powers, leveraging each partner's unique strengths while avoiding over-dependence on any single entity. By engaging in simultaneous collaborations with different countries, follower states can protect themselves against potential technological monopolies, political coercion, or security threats. This hedging approach not only serves to safeguard national interests but also enhances diplomatic flexibility, allowing countries to navigate the complex geopolitical landscape of global technology cooperation more effectively. Understanding such strategies is crucial for both followers and leading nations to establish sustainable and successful partnerships, especially in the technology context.

The technological domain differs significantly from traditional interstate leadership due to the rapid evolution and decentralization of innovation, which redefines leadership as more dynamic and adaptive. First, unlike conventional power domains, breakthroughs in AI, quantum computing, and other frontier fields face compressed lifecycles, where temporary advantages (e.g., in blockchain or Web 3.0) can be swiftly overturned. Sustaining leadership thus requires not only continuous innovation but also structural stabilization through regulation, alliance-building, and norm and standard setting. For example, the US has led in AI through advancements in machine learning, natural language processing NLP, and large-scale models. OpenAI's release of ChatGPT in late 2022 showcased this edge. To protect its interests, the US imposed export controls on advanced semiconductors and increased scrutiny of Chinese investment via the Committee on Foreign Investment in the United States (Chan, 2021). Yet China's progress, as seen with DeepSeek, reveals the limits of containment. Its incremental advancements demonstrate adaptive resilience. This underscores a paradox: technological leadership is neither static nor monopolistic.

Second, in the era of Web 3.0, the globalization of technology has enabled more countries and non-state actors to participate in technological innovation, making the leadership environment more decentralized. The rise of open-source technologies, global cooperation networks, and multinational R&D projects has lowered the barriers to technological innovation. The widespread adoption of open-source AI frameworks like TensorFlow and PyTorch has allowed developers and small businesses worldwide to engage in AI research and applications. In such a decentralized leadership environment, leading countries must attract followers through open collaboration and resource sharing, while follower countries have more choices and can select leaders based on their specific needs. This interaction makes leadership relationships more flexible and dynamic. Aligning with Nye's (2011) perception of global leadership stated, no country can dominate all issues in technology in the Web 3.0 era; therefore, the rivalry for technological leadership should be approached as an issue-based inquiry.

## 4. US and China's Rivalry for Global Leadership in AI

The US–China rivalry in AI has emerged as one of the most consequential geopolitical and technological contests of the 21st century. As AI becomes central to economic growth, national security, and global governance, the stakes of this competition continue to rise. Both countries have explicitly expressed their goal of developing or sustaining global leadership, providing an opportunity to examine our leadership framework.

This section analyzes how the US and China pursue global AI leadership, based on their AI-related policy documents between 2016 and 2025. Our analysis begins with each country's domestic strategic priorities and implementation mechanisms, which serve as the foundation for its global leadership. We then examine how these domestic foundations shape their international engagement, particularly in efforts to influence global AI governance and followers. Lastly, we illustrate followers' responses towards two countries.

The US and China are actively promoting different visions of AI leadership, each seeking to align the global ecosystem with their strategic interests and values. To understand this rivalry, it is important to recall the conceptual framework, which emphasizes that AI leadership goes beyond mere technological breakthroughs in algorithms, computing power, or data collection. It also involves defining the rules of the game—setting the norms, standards, and ethical frameworks that govern AI's deployment, development, and regulation. We present their different versions of AI leadership in a comparative approach. In summary, the US leads in AI by fostering a collaborative, values-based ecosystem grounded in innovation, open-source platforms, public-private partnerships, and multilateral cooperation, while China pursues a state-led, infrastructure-anchored, and development-embedded model of AI leadership. The US mostly attracts its democratic allies, such as the EU countries, while China's leadership is followed by many developing countries in need of infrastructure and development.

The US has cultivated its AI leadership through establishing a technological ecosystem that exemplifies the collaborative model of technology governance. Rather than pursuing unilateral dominance, the US has established itself as a system leader by providing key public goods that simultaneously strengthen its position while enabling broader ecosystem participation. The US seeks to balance its national interests with the values and expectations of other countries. This approach manifests in three interlocking dimensions that create a self-reinforcing leadership structure: enhancing strong innovation capability, multilateral cooperation, and relational governance through leveraging multilateral institutions to shape global AI norms and standards.

First, the US leads in AI through public-private partnerships and deregulatory policies that sustain its competitive edge, forming the domestic foundation for exercising global leadership. Rather than directing, the US fosters an innovation ecosystem where federal coordination supports private sector dynamism, with global tech giants driving progress under a light-touch regulatory model (Bradford, 2023) and combining it with market-driven agility. A key institutional mechanism is the National Science and Technology Council's Subcommittee on Machine Learning and AI, established in 2016 to align federal research efforts and streamline cooperation across sectors. This laid the groundwork for the National Artificial Intelligence Research and Development Strategic Plan, which advances three priorities crucial for global leadership: long-term research investment to maintain technological advantage, ethical frameworks to ensure social license for innovation, and multi-stakeholder governance to mobilize resources from industry, academia, and

government (US National Science and Technology Council, 2016). These domestic arrangements serve not only to bolster US competitiveness but also to lay the foundation for its global AI leadership, particularly in setting international norms and standards.

Second, the US is providing an international public good by using open-source platforms and ethical frameworks in its leadership strategy. The US government collaborates with the private sector and supports open-source AI platforms, such as TensorFlow (developed by Google) and PyTorch (developed by Meta), allowing anyone (including other countries) to participate. The practice (such as in the Blueprint for an AI Bill of Rights) helps establish de facto technical industry standards, including fairness, transparency, accountability, and privacy (White House Office of Science and Technology Policy, 2022), enabling worldwide access to building and deploying AI models efficiently (High, 2025; Microsoft, 2018). Building on these efforts, the US has played a leading role in shaping international AI governance, exemplified by its key contribution to the 2019 Principles on Artificial Intelligence of the OECD, which emphasize human-centric AI, transparency, and accountability. By actively engaging with its allies, the principles of the US have been adopted by over 50 countries (OECD, 2020). Furthermore, the US is actively setting up ethical framework initiatives such as GPAI and the US–EU Trade and Technology Council to lead in the global AI governance.

Third, in a relational way, the US is strategic and selective in mobilizing its potential followership and seeks to shape the global evolution of AI in a manner that aligns with its economic and national security interests. The US adopts a dual-track policy that can be summarized as open to its followers but decoupled from its competitors. Trump notes at the beginning of the *American Artificial Intelligence Initiative* that "continued American leadership in AI is of paramount importance to maintaining the economic and national security of the United States and to shaping the global evolution of AI in a manner consistent with our Nation's values, policies, and priorities" (Office of Science and Technology Policy, 2020, p. 1). The EU is an important partner. At the G7 and G20 summits, the US promoted shared AI governance frameworks to coordinate with its democratic allies, and the EU engaged with these efforts. Through bilateral science and technology agreements, such as those with the UK and France, the US fostered collaborative R&D efforts and helped set common standards for AI development (Khasru et al., 2025). However, it needs to be noted that the EU is also advocating its own version of AI governance, spearheading regulatory frameworks that prioritize ethical principles, fundamental rights, and accountability. The EU issued the EU General Data Protection Regulation, aiming to offer EU citizens a harmonized approach towards privacy, emphasizing people's rights to data protection. The Artificial Intelligence Act entered into force in August 2024, aiming to promote human-centric, trustworthy, and sustainable AI, while protecting individuals' freedoms and rights. However, while the EU's framework is innovative and rigorous, its influence remains largely confined to its own jurisdiction, as few non-EU nations truly follow the EU's model. The EU lacks the capability to diffuse its standards and norms to make its normative model a tool to build relational partnerships with other nations; therefore, we may regard the EU as leading in terms of AI ethical regulation, but without followers, we cannot perceive it as a leader. By highlighting shared interests in AI governance, the US fostered alignment with the EU.

In response to its competitors, the US also prioritized partnerships to counter authoritarian AI models, leveraging multilateral forums to advance its regulatory principles. The US includes strategic competition as a core component of its international leadership, integrating national security imperatives into its global strategy. *The National Security Commission on Artificial Intelligence Final Report* (2021) highlights the need to

counter adversarial nations, particularly China, by advancing AI capabilities in defense and cybersecurity. On February 21, 2025, the Trump administration signed a memorandum instructing CFIUS to restrict Chinese investment in certain strategic areas. In short, the US leadership in AI is characterized by a technology-and values-driven approach that integrates ethical and technological governance, international collaboration, and strategic competition. These combined efforts not only reinforce the US's global leadership but also aim to build a more equitable and secure AI ecosystem aligned with democratic values and national interests.

In contrast, China's global AI leadership is advanced through national development plans, efforts to combine AI standardization within national economic transformation and social governance, and large-scale digital infrastructure investment. First, China's AI global leadership is rooted in a domestic long-term strategic vision, exemplified by the Next Generation Artificial Intelligence Development Plan (The State Council of the People's Republic of China, 2017). The plan sets clear milestones and shows a state-led leadership style. It outlines three stages: achieve global parity and integrate AI into key sectors such as healthcare and education by 2020; make major breakthroughs in AI theory and applications, driving economic transformation and establishing China as a global AI innovation hub by 2025; and become the world's primary AI innovation center, leading in theory, technology, and applications, with AI as a core driver of economic and social development by 2030. The plan's strategic priorities are on foundational technology breakthroughs, open AI platforms, infrastructure and ecosystem development, and international collaboration, actively promoting global cooperation and participation in setting international AI standards to strengthen China's role in global AI governance (The State Council of the People's Republic of China, 2017).

Second, building on this, China integrates AI technology within broader socio-economic development and infrastructure objectives, aiming to establish ethical and legal norms that support the sustainable development of the AI ecosystem. This can be clearly observed in China's AI policy shift, which previously emphasized technology catch-up and talent cultivation. The White Paper on Artificial Intelligence Standardization (2018–2023; China Electronics Standardization Institute, 2018) shows this transition—from an early focus on building a technological foundation through R&D and talent development to a more integrated approach that combines AI development with national priorities. As AI applications grow, the emphasis has shifted toward standard-setting in data, algorithms, and system interoperability to strengthen domestic market health and boost international influence. The latest version framework embeds AI into broader goals of economic transformation, improved social governance, and public welfare—particularly in areas like smart cities, healthcare, and environmental protection—underscoring China's emphasis on sustainable and socially embedded AI development.

Third, China's AI strategy, which integrates development and infrastructure, is central to its global leadership approach and has attracted and mobilized followership, particularly among developing countries seeking digital and AI infrastructure, while embedding Chinese-led AI standards into these systems. China's Digital Silk Road reflects this strategy by using infrastructure investment to forge durable technological and geopolitical alliances. By offering a comprehensive package that combines affordable financing, technology transfer, and strategic political alliances, China has institutionalized collaboration and has attracted numerous developing countries to follow its lead in digital development. The Digital Silk Road, launched in 2015, has over 130 projects under Belt and Road Initiative's label (Russel & Berger, 2021). The initiative advances China's leadership through three main goals: achieving interconnection and interoperability of

digital infrastructure among participating countries, creating a new form of digital economy driven by data elements, and establishing clear-cut digital governance rules (He & Zhou, 2024). China acts as a provider of infrastructure, institutions, and ideas—constructing data centers and smart cities in Kenya, fiber-optic networks in Pakistan, and 5G testing in Thailand. Technologies from Chinese firms like Huawei and ZTE are widely adopted in countries such as Malaysia, Ecuador, and Kenya, improving digital capacity in local areas. China also promotes its technical standards through bilateral agreements, signing over 90 with 52 countries by 2019 (Russel & Berger, 2021), and integrates these standards into foreign projects to support trade and industrial cooperation (The State Council of the People's Republic of China, 2015).

In summary, the competition between the US and China in AI governance extends beyond technological advancement to the establishment of international norms and technical standards. Both nations, based on their domestic foundation, have actively promoted their respective frameworks, seeking to shape the global AI ecosystem in ways that reflect their strategic interests and values. Especially, the US's framework promotes open ecosystems and ethical norms, while China focuses on building infrastructure and exporting its technology and standards, particularly to developing countries. This competition is particularly intense in areas such as data governance, algorithmic transparency, and AI ethics, where the stakes are high due to AI's transformative impact on economies, security, and societal structures.

However, the above comparison still largely focuses on countries' leading strategies without necessarily emphasizing followership and a relational process. The ultimate establishment of leadership in AI also hinges on followers' perceptions of which model provides greater benefits to the preservation of their national interests. The unique nature of the AI environment, characterized by rapid technological change, data dependency, and geopolitical competition, amplifies the importance of follower choices. The fragmented nature of the global AI ecosystem, characterized by differing regulatory environments and technological capabilities, means that follower nations will choose based on their specific needs and priorities, driven by either political and security considerations or technological and economic interests.

The EU aligns with US AI leadership primarily due to shared security interests. While the EU positions itself as a regulator of AI ethics and promotes "strategic autonomy," its actual AI development remains deeply intertwined with a US-led framework. Its member states often align with US AI strategies on political and security fronts, especially within NATO and transatlantic defense partnerships. For instance, EU members (e.g., France and Germany) participate in US-led military AI projects, such as NATO's AI strategy and drone surveillance systems. Despite advocating for "digital sovereignty," the EU has *de facto* aligned with US export controls on AI-related technologies to China.

Serbia's embrace of Chinese AI technologies, especially in smart city infrastructure and surveillance, is motivated by economic and technological needs. Serbia needs affordable and advanced AI solutions; China is willing to provide financing and technology transfer. For instance, Chinese companies like Huawei have deployed facial recognition and surveillance technologies in Serbia, aligning with the country's goals of modernizing its infrastructure (Russel & Berger, 2021). The adoption of Chinese AI technologies has accelerated Serbia's digital transformation. Projects like the Belgrade Smart City initiative, powered by Chinese technology, have improved urban management and public safety. Chinese financing terms, technology transfer packages, and implementation speed address Serbia's immediate developmental needs more effectively than Western alternatives. This case highlights the infrastructure-for-influence dynamic in the AI sector.

Singapore provides a compelling example of a nation that has adopted a pragmatic hedging approach, aligning with both the US and China in different areas of AI technology and governance. Singapore has adopted the US-led ethical AI framework in areas such as data governance and algorithmic transparency. For instance, Singapore's Model AI Governance Framework, released in 2019 and updated in 2020 and 2024, aligns closely with the OECD AI Principles and the US Blueprint for an AI Bill of Rights. These frameworks emphasize fairness, accountability, and transparency in AI systems, reflecting Singapore's commitment to building trust in AI technologies (Personal Data Protection Commission & Infocomm Media Development Authority, 2020). In 2023, Singapore launched the Singapore National AI Strategy 2.0 (NAIS 2.0), in which infrastructure and environment are one of the key systems of Singapore as a smart nation (Government of the Republic of Singapore, 2023). To that aim, Singapore has adopted Chinese AI technologies in areas such as smart city infrastructure and surveillance systems. For example, Singapore has collaborated with Chinese tech giants like Huawei and SenseTime to implement AI-powered surveillance and facial recognition systems as part of its Smart Nation Initiative. These technologies are used to enhance public safety and urban management, aligning with Singapore's goals of becoming a global leader in smart city development (He & Zhou, 2024). This dual-alignment approach reflects Singapore's pragmatic strategy of maximizing benefits from both models while maintaining its own technological sovereignty and economic interests. Singapore's case illustrates that follower nations do not have to choose exclusively between the US and China. Instead, they can adopt a pragmatic, context-specific approach that aligns with different aspects of each model based on their strategic priorities. Singapore is leveraging its followership as a strategic resource—the ability to access and synthesize multiple systems to develop its own AI governance and leadership in the region. In short, the ultimate determination of the US–China rivalry of AI leadership will depend on the ability of the US and China to attract and retain followers by offering tangible benefits. The US appeals to nations prioritizing ethical governance, democratic values, and individual rights, as seen in the EU's alignment with US-led frameworks. In contrast, China's emphasis on affordable technology, infrastructure development, and economic growth resonates with developing nations like Pakistan and Serbia. Meanwhile, pragmatic followers like Singapore demonstrate that nations can strategically align with both models, leveraging the strengths of each to address their unique needs.

## 5. Conclusion

This article has developed a relational and dynamic framework for understanding technological leadership, emphasizing the interplay between leaders, followers, and the technological environment. Unlike traditional approaches that conflate leadership with innovation capability or market dominance, our framework highlights the importance of norm-setting, rule-making, and the ability to inspire collective action within global technological ecosystems. Through this lens, we have analyzed the US–China rivalry in AI, revealing how both nations are vying to shape the global AI governance landscape in ways that reflect their strategic interests and values. The ultimate outcome of the US and China rivalry for AI leadership will depend on the ability of the US and China to attract and retain followers. The US appeals to nations prioritizing ethical governance, democratic values, and individual rights, as seen in the EU's alignment with US-led frameworks. In contrast, China's emphasis on affordable technology, infrastructure development, and economic growth resonates with developing nations like Pakistan and Serbia. Meanwhile, pragmatic followers like Singapore demonstrate that nations can strategically align with both models, leveraging the strengths of each to address their unique needs.

AI significantly amplifies the challenges for leaders. In the AI field, it is extremely difficult to maintain long-term and comprehensive leadership. The dispersive nature of leadership in AI is determined by the characteristics of this fundamental leadership context. AI is a rapidly evolving and complex technology. The speed of innovation means that any advantage a leader may have can quickly be eroded. The widespread adoption of open-source technologies and the increasing number of players in the AI field have decentralized the power structure. This decentralization makes it challenging for leaders to exert absolute control and maintain their position over an extended period. Looking ahead, both the US and China are likely to continue leveraging their technological advantages to establish more norms and standards in AI governance. However, AI governance remains a nascent space, and building international consensus will be critical to addressing the risks and uncertainties of AI development.

## Acknowledgments

We are grateful for feedback from Prof. Yan Xuetong. The manuscript was also improved with the help of suggestions provided by two anonymous reviewers and the issue's editors.

## Funding

The research is funded by "A Study on the International Leadership in New Era," National Social Science Fund of China (Grant No. 21&ZD167). Yuanyuan Fang acknowledges financial support from Beijing Language and Culture University (Grant No. 401232202). Shenghao Zhang acknowledges financial support from the Shuimu Tsinghua Scholar Program.

## Conflict of Interests

The author declares no conflict of interest.

## Correction Statement

This article was originally published with errors that have now been corrected. Please see Correction: https://doi.org/10.17645/pag.11880

## References

Avolio, B. J., Walumbwa, F. O., & Weber, T. J. (2009). Leadership: Current theories, research, and future directions. *Annual Review of Psychology*, *60*, 421–449.

Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press.

Burns, J. M. (1978). *Leadership*. Harper & Row.

Chan, A. (2021, September 28). *CFIUS, Team Telecom and China*. Lawfare. https://www.lawfaremedia.org/article/cfius-team-telecom-and-china.

China Electronics Standardization Institute. (2018). *Artificial intelligence standardization white paper*. https://cset.georgetown.edu/publication/artificial-intelligence-standardization-white-paper

Cusumano, M. A. (2004). *The business of software: What every manager, programmer, and entrepreneur must know to thrive and survive in good times and bad*. Free Press.

Ding, J. (2024a). The diffusion deficit in scientific and technological power: Re-assessing China's rise. *Review of International Political Economy*, *31*(1), 173–198.

Ding, J. (2024b). The rise and fall of technological leadership: General-purpose technology diffusion and economic power transitions. *International Studies Quarterly*, *68*(2), Article sqae013. https://doi.org/10.1093/isq/sqae013

Drezner, D. (2001). State structure, technological leadership and the maintenance of hegemony. *Review of International Studies*, *27*(1), 3–25.

Drezner, D. W. (2019). Technological change and international relations. *International Relations*, *33*(2), 286–303.

Freeman, C. (1987). *Technology policy and economic performance: Lessons from Japan*. Pinter Publishers.

Freeman, C. (1995). The 'national system of innovation' in historical perspective. *Cambridge Journal of Economics*, *19*(1), 5–24.

Friis, K., & Lysne, O. (2021). Huawei, 5G and security: Technological limitations and political responses. *Development and Change*, *52*(5), 1174–1195. https://doi.org/10.1111/dech.12680

Gilpin, R. (1981). *War and change in world politics*. Cambridge University Press.

Government of the Republic of Singapore. (2023). *Singapore national AI strategy 2.0* (NAIS 2.0). https://file.go.gov.sg/nais2023.pdf

He, Z. P., & Zhou, M. (2024). China's role, challenges, and responses in building the digital silk road. *Northeast Asia Forum*, *33*(6), 110–124, 126. https://doi.org/10.13654/j.cnki.naf.2024.06.008

High, M. (2025, February 6). AI for good: Why Microsoft is using AI for positive change. *AI Magazine*. https://aimagazine.com/articles/ai-for-good-why-microsoft-is-using-ai-for-positive-change

Hollander, E. P. (1992). Leadership, followership, self, and others. *The Leadership Quarterly*, *3*(1), 43–54. https://doi.org/10.1016/1048-9843(92)90005-Z

Huang, C., & Sharif, N. (2016). Global technology leadership: The case of China. *Science and Public Policy*, *43*(1), 62–73. https://doi.org/10.1093/scipol/scv019

Ikenberry, G. J. (2001). *After victory: Institutions, strategic restraint, and the rebuilding of order after major wars*. Princeton University Press.

Kennedy, P. (1987). *The rise and fall of the great powers: Economic change and military conflict from 1500 to 2000*. Random House.

Keohane, R. O. (1984). *After hegemony: Cooperation and discord in the world political economy*. Princeton University Press.

Khasru, S. M., Gillwald, A., Sesan, G., & Zondi, S. (2025). *International AI governance framework: The importance of G7-G20 synergy* (Policy Brief No. 2025). Think 7 Canada. https://www.cigionline.org/static/documents/TF1_Khasru_et_al_rev.pdf

Kindleberger, C. P. (1961). Obsolescence and technical change. *Bulletin of the Oxford University Institute of Economics & Statistics*, *23*(3), 281–297. https://doi.org/10.1111/j.1468-0084.1961.mp23003003.x

Kitschelt, H. (1991). Industrial governance structures, innovation strategies, and the case of Japan: Sectoral or cross-national comparative analysis? *International Organization*, *45*(4), 453–493. https://doi.org/10.1017/s002081830003318x

Kranzberg, M., & Pursell, C. W. (1967). *Technology in Western civilization*. Oxford University Press.

Levitt, T. (1966). Innovative imitation. *Harvard Business Review*, 44(5), 63–70. https://hbr.org/1966/09/innovative-imitation

Losacker, S., & Liefner, I. (2020). Implications of China's innovation policy shift: Does "indigenous" mean closed? *Growth and Change*, *51*(3), 1124–1141. https://doi.org/10.1111/grow.12400

Maddison, A. (1982). *Phases of capitalist development*. Oxford University Press.

Microsoft. (2018, June 4). Microsoft to acquire GitHub for $7.5 billion. *Microsoft News*. https://news.microsoft.com/source/2018/06/04/microsoft-to-acquire-github-for-7-5-billion

Mochinaga, D. (2021, June 10). *The digital silk road and China's technology influence in Southeast Asia*. Council on Foreign Relations. https://www.cfr.org/sites/default/files/pdf/mochinaga_the-digital-silk-road-and-chinastechnology-influence-in-southeast-asia_june-2021.pdf

Modelski, G. (Ed.). (1987). *Exploring long cycles*. Lynne Rienner Publishers.

Modelski, G., & Thompson, W. R. (1988). *Seapower in global politics, 1494–1993*. University of Washington Press.

Moe, E. (2007). *Governance, growth and global leadership: The role of the state in technological progress, 1750–2000*. Ashgate.

Mokyr, J. (1990). *The lever of riches: Technological creativity and economic progress*. Oxford University Press.

National Security Commission on Artificial Intelligence. (2021). *Final report* (*National Security Commission on artificial intelligence*). US Government. https://www.govinfo.gov/app/details/GOVPUB-Y3-PURL-gpo153246

Northouse, P. G. (2021). *Leadership: Theory and practice* (9th ed.). Sage.

Nye, J. S., Jr. (1990). *Bound to lead: The changing nature of American power*. Basic Books.

Nye, J. S., Jr. (2008). *The powers to lead*. Oxford University Press.

Nye, J. S., Jr. (2011). *The future of power*. PublicAffairs.

OECD. (2020). *Global partnership on artificial intelligence*. https://www.oecd.org/en/about/programmes/global-partnership-on-artificial-intelligence.html

Office of Science and Technology Policy. (2020, February). *American Artificial Intelligence Initiative: Year one annual report*. The White House. https://www.nitrd.gov/nitrdgroups/images/c/c1/American-AI-Initiative-One-Year-Annual-Report.pdf

Olson, M. (1982). *The rise and decline of nations: Economic growth, stagflation, and social rigidities*. Yale University Press.

Personal Data Protection Commission & Infocomm Media Development Authority. (2020). *Model artificial intelligence governance framework* (2nd ed.). https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf

Porter, M. E. (1990). *The competitive advantage of nations*. Free Press.

Rogers, E. M. (2003). *Diffusion of Innovations* (5th ed.). Free Press.

Rosenberg, N. (1992). Economic experiments. *Industrial and Corporate Change*, *1*(1), 181–203. https://doi.org/10.1093/icc/1.1.181

Russel, D. R., & Berger, B. H. (2021). Chinese influence, the digital silk road, and the diffusion of Chinese technical standards. In L. Tobin & D. Strub (Eds.), *Stacking the deck: China's influence in international technology standards setting* (pp. 27–30). Asia Society. https://www.jstor.org/stable/resrep48538.10

Russett, B. (1985). The mysterious case of vanishing hegemony; or, is Mark Twain really dead? *International Organization*, *39*(2), 207–231.

Ryan, M., & Burman, S. (2024). The United States–China 'tech war': Decoupling and the case of Huawei. *Global Policy*, *15*(2), 355–367.

Salguero, D. R. (2024, October 13). Sebastian Coe, a sporting leader with a strong political profile. *Inside the Games*. https://www.insidethegames.biz/articles/1149222/sebastian-coe-sporting-leader-political

Schweller, R. L., & Pu, X. (2011). After unipolarity: China's visions of international order in an era of US decline. *International Security*, *36*(1), 41–72.

Strange, S. (1987). The persistent myth of lost hegemony. *International Organization*, *41*(4), 551–574.

The State Council of the People's Republic of China. (2015). *Notice of the General Office of the State Council on issuing and implementing the "Deepening Standardization Work Reform Plan" action plan (2015–2016)*. State Council of the People's Republic of China. http://www.gov.cn/zhengce/content/2015-09/10/content_10154.htm

The State Council of the People's Republic of China. (2017). *A Next Generation Artificial Intelligence Development Plan*. https://d1y8sb8igg2f8e.cloudfront.net/documents/translation-fulltext-8.1.17.pdf

Thompson, W. R. (1990). Long waves, technological innovation, and relative decline. *International Organization*, *44*(2), 201–233.

US National Science and Technology Council. (2016). *The national artificial intelligence research and development strategic plan*. https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/national_ai_rd_strategic_plan.pdf

White House Office of Science and Technology Policy. (2022, October). *Blueprint for an AI bill of rights*. https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf

Womack, J. P., Jones, D. T., & Roos, D. (1990). *The machine that changed the world: The story of lean production*. Harper Perennial.

Wu, C. X. (2024). A bargaining theory of US–China economic rivalry: Differentiating the trade and technology wars. *The Chinese Journal of International Politics*, *17*(4), 323–345.

Yan, X. (2011). *Ancient Chinese thought, modern Chinese power*. Princeton University Press.

Zhang, Z. (2024). Technology and geopolitics: The social construction of Huawei's 5G controversy in Europe. *Global Media and Communication*, *20*(2), 217–235. https://doi.org/10.1177/17427665241251448

## About the Authors

Yuanyuan Fang is an assistant professor at the School of International Politics and Communication, Beijing Language and Culture University. Her research focuses on international relations theory, international political leadership, China–US relations, Indo–Pacific economy, and security. She has published in the *Chinese Journal of International Politics* and the *Third World Quarterly*.

Shenghao Zhang is a postdoctoral fellow at the Institute for International Relations, Tsinghua University. He received his PhD from the University of Essex. His research focuses on peacekeeping, conflict dynamics, and international relations. He has published in the *International Peacekeeping* and *the Journal of Conflict Resolution*.

**Politics and Governance**
2025 • Volume 13 • Article 10247
https://doi.org/10.17645/pag.10247

cogitatio

ARTICLE

Open Access Journal

# Paradoxical Infrastructuring: Genealogies of Governance and "Art of Being Governed" in China's Blockchain–AI Hypes

**Zichen Hu**

Department of Media and Communications, London School of Economics and Political Science, UK

**Correspondence:** Zichen Hu (z.hu24@lse.ac.uk)

**Submitted:** 28 February 2025 **Accepted:** 16 July 2025 **Published:** 27 November 2025

**Issue:** This article is part of the issue "Technology and Governance in the Age of Web 3.0" edited by Chang Zhang (Communication University of China), Zichen Hu (London School of Economics and Political Science), and Denis Galligan (University of Oxford), fully open access at https://doi.org/10.17645/pag.i443

## Abstract

This research investigates the rise, transformation, and contested persistence of blockchain and AI within China's digital governance ecosystem, tracing how AI inherits and transforms blockchain's discursive legacy: the libertarian imaginaries of decentralization and cryptographic trust are rearticulated into new narratives of centralized data infrastructures, computational power, and algorithmic authority. Seen through this inheritance, blockchain's trajectory appears not as a linear transition from hype to repression, but as a process of *paradoxical infrastructuring*, where blockchain's affordances for decentralizing possibilities are alternately valorized, domesticated, and strategically redeployed within contradictory regimes of power. Bringing together Foucault's theory of governmentality, developed to interrogate Cold War modernity, and Michael Szonyi's framework of "the art of being governed," which captures the tactical adaptations of subjects under premodern Chinese statecraft, this analysis reveals how infrastructural governance in China is shaped by the agonistic interplay between historically sedimented repertoires of rule and their contemporary rearticulation through participatory contestations and adaptive strategies enacted by a plurality of stakeholders. Since the reform and opening-up era, these logics have not coexisted peacefully but clashed in painful and dramatic ways, producing new modes of infrastructural subjectivation. The study foregrounds intermediary actors, including crypto developers, influencer-entrepreneurs, and policy-facing venture capitals, who perform decentralization while materially benefiting from its state-sanctioned translation. These figures occupy the ambiguous space between resistance and complicity, tactically navigating regulatory opacity and ideological elasticity. The discourse once attached to blockchain has not disappeared; it re-emerges in the AI era as tools for imagining trustworthiness and legitimacy, enabling blockchain actors to revalorize themselves after the burst of the earlier hype. Ultimately, what appears as a shift from blockchain to AI is better understood as a recursive recalibration of infrastructural power: blockchain's imaginaries and architectures do not vanish but are folded into the emerging socio-technical apparatus of AI, that is, the interlinked infrastructures, institutions, and discourses through which

governance and contestation are exercised. In this process, ideological contradiction functions not as a failure in governance but as a generative feature of China's evolving techno-infrastructural governance.

**Keywords**
artificial intelligence; blockchain; China; decentralization; genealogy; geopolitics; governance; infrastructuring

## 1. Introduction

This research traces the rise, transformation, and contested persistence of blockchain and AI in China as a paradigmatic instance of *paradoxical infrastructuring*: a process in which technologies with affordances for (de)centralizing possibilities are selectively championed, disciplined, and rearticulated within a broader regime of techno-political governance. More than a linear story of innovation disrupted by the regime's control, blockchain and AI's trajectory in China reveals a dynamic terrain in which infrastructural imaginaries are mobilized, co-opted, and strategically performed not only by the state but by a diverse field of intermediaries, entrepreneurs, and transnational actors navigating China's digital ecosystem.

Since the reform and opening-up era, China's techno-political evolution has been marked by an uneven encounter between contradictory logics of governance. On one hand, state institutions adopt technocratic tools to classify, optimize, and control populations. On the other hand, a wide range of actors from provincial bureaucrats to crypto entrepreneurs continue to operate with tactical adaptation, negotiation, and improvisation. Read genealogically, these practices appear not as anomalies of the present but as continuities of a longer history of governing and being governed, including patterns of compliance, circumvention, and brokerage that persist within new infrastructural formations. This article brings together Foucault's concept of governmentality and Michael Szonyi's (2007) framework of "the art of being governed." While the former was developed in the Cold War context to analyze the rationalities and techniques through which modern forms of governing power operate, the latter foregrounds the everyday, opportunistic adaptations of subjects navigating the constraint produced by the former.

In this reading, Szonyi's account serves as a secondary entry point into the Foucauldian genealogical ethos that sustains the analytical process of this article. One that enriches the concept of governmentality by foregrounding the everyday tactics, improvisations, and embodied negotiations through which governance acquires its lived texture. Szonyi's analysis of coastal communities under Ming and Qing maritime prohibitions shows that regulation did not simply discipline subjects into compliance; it also provoked smuggling, identity-shifting, and opportunistic brokerage that were themselves integral to how the state functioned. In this sense, governance is encountered with the adaptive maneuvers of those being governed, whose practices inflect, redirect, and sometimes unexpectedly stabilize the very structures of power imposed upon them.

This conjunctive framework enables a more historically embedded reading of the process called infrastructuring: not as a top-down technical imposition, but as a dynamic choreography of regulation, speculation of power relations, and thus the outcomes of certain regulations, and symbolic (re-)alignment in policy and public discourse. In this light, technology governance in China is understood not merely through

institutional logics, but through the everyday performances of those who tactically navigate, and occasionally exploit, the ideological contradictions of technological hypes.

Blockchain, like peer-to-peer (P2P) lending before it, emerged from a conjuncture of utopian discourse, financial deregulation, and selective policy endorsement. Yet its promise of decentralization soon collided with concerns over monetary sovereignty, capital flight, and geopolitical insecurity. Yet even after its formal disavowal in 2017 in China, blockchain's discursive residue persisted: resurfacing in state-sanctioned infrastructures like the Blockchain-based Service Network, in decentralized media experiments, and in crypto-financial platforms like Binance that straddle the blurred boundary between dissidence and opportunism.

The aim of this article is not to chart the rise and fall of blockchain as a chronological episode in China's techno-political history. Instead, it is to reveal how the governance of technology, and the practices of being governed through technology, unfold through contestation, appropriation, and rearticulation. This research situates China's blockchain boom and bust within a wider genealogy of infrastructural governance, one shaped not only by policy shifts or global market cycles, but by speculative statecraft driven by postcolonial anxieties, and the ambivalent performances of alignment of non-state actors. It argues that decentralization, far from being simply suppressed, is continually rebranded and redeployed to attract capital, absorb risk, and perform ideological flexibility. The resulting mode of governance thrives not on resolution, but on *contradiction*: where opacity is instrumentalized, trust is staged, and socio-technical imaginaries are selectively appropriated to reassert state legitimacy in the language of disruption.

By foregrounding this historically layered and discursively volatile terrain, this research article challenges prevailing binaries between centralization and decentralization, compliance and resistance. It offers instead a theory of infrastructural subjectivation, where actors, from crypto miners and local officials to global tech firms, enact autonomy, perform legitimacy, and manoeuvre power through infrastructures whose meanings remain in flux. Ultimately, this case illuminates the hybrid logics underpinning China's digital statecraft, while foreshadowing the governance of AI to come, where emerging technologies are securitized and perform national aspiration through an economy of signifiers connotating "innovation."

## 2. Crypto Dreams and Algorithmic Order: The Discursive Battle for Digital Futures

To sustain the genealogical ethos, the article now turns to the infrastructural imaginaries of blockchain and AI. Here, genealogy functions as a meta-commentary: it does not search for the "origin" of these technologies but reveals how their epistemic authority is constituted through discursive sediments, including Cold War rationalities of governmentality, libertarian cryptographic imaginaries, and postcolonial anxieties of state in its digital sovereignty. By reading blockchain and AI in this way, the aim is not to isolate their technical architectures, but to situate them within overlapping historical layers of contestation, where infrastructures are continually re-signified as sites of authority, resistance, and opportunistic alignment.

### *2.1. Infrastructural Imaginaries of Blockchain and AI*

Blockchain and AI circulate within divergent *logics of infrastructuring* (Hartong & Piattoeva, 2021; Rozas et al., 2021): Blockchain foregrounds decentralization, cryptographic trust, and distributed consensus, while AI

privileges classification, prediction, and centralized data extraction. These logics are not simply functional choices; they differentially *embody normative orders*, claims about who has the authority to decide, and what forms of social organization are desirable or possible.

The epistemic legacy often attached to blockchain is the libertarian techno-utopianism of the 1990s "Crypto Wars," which imagined cryptography as a tool of resistance against institutional power. This legacy continues to animate social imaginaries of decentralisation through decentralized autonomous organizations (DAOs) to decentralized finance (DeFi) platforms, where cryptographic systems are posited as emancipatory alternatives to state or corporate control. These imaginaries construct subject positions such as the "sovereign individual," the "super-user," or the "crypto dissident," who claim agency through code, pseudonymity, financial autonomy, and disintermediation (Cossu, 2022).

AI, by contrast, derives its epistemic authority from a very different techno-political lineage, which is rooted in probabilistic modelling, systematization, and the logic of optimization. Unlike blockchain, whose credibility is discursively tied to transparency and cryptographic trust, AI derives legitimacy from its ability to model uncertainty, process vast datasets, and produce outputs that promise efficiency, prediction, and actionable insight. This authority is grounded not in openness, but in the transformation of human behaviours, social relations, and moral categories into data points, features, and statistical probabilities. These infrastructures produce systems that determine what is seen as true, reliable, or legitimate (Foucault, 2008). AI does not simply represent the world; it actively constructs social intelligibility through classification, optimization, and prediction (Crawford, 2021). Through practices such as sentiment analysis, facial recognition, risk scoring, and content moderation, AI embeds itself in truth-making functions once reserved for institutional actors like courts, universities, or medical authorities. In doing so, it reorganizes not only knowledge hierarchies but the very terrain of governance.

This epistemic power is deeply *ambivalent*. On one hand, AI systems are celebrated as tools of care, used in health diagnostics, elder support, or climate modelling. On the other hand, they are critiqued as instruments of surveillance, racialized policing, and labour discipline. In either case, AI infrastructures evoke ongoing political struggles over (a) *representation*, what and who is visible, classifiable, and governable, and (b) *intelligibility*, whose knowledge, identity, and agency are rendered legible or erased. These struggles are especially acute in contexts like China, where AI is positioned as a key discursive node in broader state projects of order, security, and ideological coherence.

### *2.2. Between Autonomy and Absorption: Everyday Politics of Infrastructuring in China's Digital Governance*

Despite the state's central role, the evolution of China's digital infrastructure is not a linear, top-down imposition but a contested field of ideological struggle and opportunistic alignment. Building on infrastructure studies (Bowker et al., 2009; Larkin, 2013; Star & Ruhleder, 1996), this research's analysis extends the concept of *infrastructuring* beyond the notion of technical co-production, to emphasize how infrastructural design becomes a site of strategic co-optation, where even actors who invoke decentralization, privacy, or techno-libertarian ideals frequently reorient these narratives to secure alignment with state legitimacy, or profit from it.

Michael Szonyi's framework of "the art of being governed," derived from his study *The Art of Being Governed*, is particularly pertinent to analyzing contemporary China's blockchain and AI governance. During the late Ming and early Qing periods, China's policy of maritime prohibition sought to sever external trade and migration in an effort to assert centralized control over the coastal frontier. Yet rather than achieving complete isolation, these regulatory constraints fostered a diverse array of evasive practices among coastal merchants, fishermen, and local elites. Engaging in smuggling, leveraging tributary trade exemptions, and manipulating official identities, these actors carved out economic niches within the interstices of imperial governance. Such strategies did not constitute overt resistance but reflected a quotidian politics of survival. This is what Michael Szonyi terms the "art of being governed," where ordinary people adapted, appropriated, and subtly manipulated state regimes for their own ends.

This "art of being governed" is not confined to premodern contexts. Rather, it reflects a mode of relational governance that remains salient in today's China, where formal regulations on technologies like blockchain are met with adaptive maneuvering by entrepreneurs, local officials, and intermediary institutions. These actors often work within and around policy frameworks—invoking official discourse while informally bending or selectively implementing regulations. In this sense, Szonyi's insights allow us to theorize how modern digital governance regimes can simultaneously assert central authority while leaving room for context-specific adaptations and tactical maneuvering at the local level.

In this context, this article extends Szonyi's intervention by offering a genealogical investigation of blockchain and AI governance not as ahistorical technical phenomena, but as sites in which Cold War epistemologies, postcolonial anxieties, and global power asymmetries are reassembled to form China's infrastructural imaginaries. This approach shows how discourses on innovation are haunted by the specters of modernity that China seeks to redefine against the "West", especially the US: techno-developmentalism as civilizational uplift, data sovereignty as postcolonial defense, decentralization as both threat and asset.

Crucially, this analysis identifies a new class of intermediaries, not dissidents or state agents per se, but opportunistic actors who perform decentralization while materially benefiting from its domestication. These are the brokers, "influencer-entrepreneurs," and venture capital (VC)-aligned developers who rebrand compliance as innovation, and whose success depends on the conversion of techno-libertarian aesthetics into state-compatible forms. This conversion process is negotiated, incentivized, and, at times, *voluntarily enacted* by those seeking advantageous positions within the economic and political system.

Actors in this system operate not only within the confines of present-day geopolitical competition, but also within historically sedimented governance logics, which are concerned with regulating flows (of capital, people, and now data), extracting value from strategic peripheries, and cultivating adaptive intermediaries (Szonyi, 2017). Rather than drawing direct equivalences to imperial or colonial systems, we highlight a continuity in techniques of mediation and navigation, where figures such as crypto developers and AI evangelists occupy liminal positions: translating global imaginaries (e.g., decentralization, autonomy) into locally legible forms, while simultaneously embedding themselves in state-sanctioned infrastructures. These actors do not simply replicate earlier roles such as the comprador or overseas broker as described in Szonyi's book, but their positionality reflects a similar structural ambivalence, operating at the interface of speculative value, national interest, and infrastructural dependence.

Therefore, instead of conceptualising infrastructuring as *only* a form of state-mediated ideological translation, where disruptive imaginaries (like the socio-political mobilization that leverages DAOs, cryptography and P2P transmission) are selectively absorbed into the state's techno-political project, this research explores a process in which entrepreneurial developers and investors operate within the discursive terrain of decentralization not to challenge state power, but to capitalize on its ideological elasticity. These actors strategically mobilize the symbolic capital of the imaginaries of decentralization and innovation to gain market position, attract investment, or secure regulatory favour, paradoxically reinforcing the very centralization they ostensibly resist.

Infrastructuring here is not a neutral or inclusive process nor just a technical layering of systems, but a continuation of geopolitical ordering processes in which subjectivities, territories, and futures are managed, interpolated, or excluded. By examining the political economy of Chinese blockchain and AI projects genealogically, we reveal how infrastructural power today reproduces older governmentality coordinates: vertical integration disguised as neutrality, calculability masked as innovation, and control legitimated through developmentalist promise.

Crucially, this logic is not unique to China. While the depth and ideological coherence of China's infrastructural integration is distinctive in its scope and ambition, it is far from ideologically coherent. Similar dynamics can be observed elsewhere, showing that the tension between centralized sovereign control and the decentralizing potential of technology cuts across different political regimes. In the US's "Crypto Wars" of the 1990s, state actors sought to curtail civilian access to strong encryption, perceiving decentralized systems as threats to institutional authority and attempting to absorb or recalibrate the disruptive potential of technologies to serve logics of governance, capital accumulation, and geopolitical ordering.

The research question guiding this article is thus: How are imaginaries of decentralization and sovereignty rearticulated through blockchain and AI infrastructures, and how do Chinese state and intermediary actors leverage this ambiguity and hype to co-produce new forms of governance?

## 3. Methodology: Mapping Discursive Regimes Through a Genealogical Lens

The preceding sections have shown how blockchain and AI emerge within distinct yet converging infrastructural imaginaries (resistance organized through decentralized forms and optimization based on centralization), each carrying normative claims about authority, legitimacy, and technological futurity. To unpack how these imaginaries are constructed, reconfigured, and selectively appropriated within China's digital governance landscape, this research adopts a Foucauldian genealogical approach. Rather than treating technological innovations as linear or governance models as top-down, genealogy traces their formation through discontinuities, crises, and ideological recalibrations. Following Foucault (1977, 1981, 1994) and more recent elaborations by Bauer and Schiele (2023), discourse here is not a mirror of power but a *strategic terrain* where meanings, institutions, and infrastructural configurations are continually contested and remade.

This analytical stance complements and extends the framework of infrastructuring introduced earlier: It views infrastructures not as neutral backdrops or merely technical assemblages, but as historically sedimented fields of struggles and negotiations, where the state, market actors, and transnational communities compete to define the boundaries of visibility, agency, and governability. What appears as a

dichotomy between blockchain's decentralization and AI's statist centralism dissolves under genealogical scrutiny. Both are expressions of a deeper recursive logic: technologies are absorbed, disciplined, and redeployed to align with evolving configurations of state power and geopolitical narrative.

Genealogy, in this article, is not presented as a discrete method but as an ethos that orients how the analysis unfolds. It functions as a historical consciousness attentive to discursive sedimentations and the reconfiguration of power/knowledge, rather than as a step-by-step procedure. This ethos becomes operationalisable through secondary interlocutors: most notably Michael Szonyi's *The Art of Being Governed*, which offers a concrete entry point into a Foucauldian genealogy by grounding abstract notions of governmentality in the lived negotiations, improvisations, and tactical adaptations of ordinary actors. In dialogue with what Bauer and Schiele (2023) call the mapping of discursive regimes, this approach treats China's digital governance not as the linear imposition of new infrastructures, but as a layered process where older bureaucratic repertoires and new technological imaginaries coexist, overlap, and rearticulate one another. It allows us to read the shift from blockchain enthusiasm to AI investment not as a rupture but as a *rearticulation*, a managed modulation of hype, risk, and innovation within the broader project of infrastructural nationalism. Through this lens, the "innovation" promoted in white papers or policy blueprints is less about technological breakthrough and more about *ideological maneuverability*: the ability to reframe global narratives of decentralization or optimization in state-compatible terms.

To operationalize this inquiry, I analyse a heterogeneous set of discursive and infrastructural artifacts (see the Supplementary File) through which competing imaginaries of technological governance are constructed, negotiated, and contested between the governing bodies and the governed actors, drawing on the conjunctive framework of both Foucault's governmentality and Szonyi's "art of being governed." These include state policy documents and legal frameworks, which formalise regulatory priorities and inscribe institutional visions of digital sovereignty. Party-state-affiliated media function not only as vehicles of ideological dissemination but also as sites of adaptive calibration, where official narratives are adjusted in response to emergent sociotechnical disruptions. In contrast, fintech journalism, industry white papers, and reports by VCs and tech companies articulate market-oriented imperatives and speculative projections. These texts often mirror, complicate, or opportunistically align with state-led innovation agendas, capable of both reinforcing and subtly reframing official priorities. Most revealing, however, are the discourses emanating from crypto-native communities and transnational actors such as Binance. These sources offer alternative epistemologies of value, autonomy, and technological futurity, some aligned with techno-libertarian logics, others shaped by exile, censorship, and diasporic positioning.

By tracing how these discursive fields intersect and diverge, I map the strategic frictions, alignments, and recursive appropriations among state, semi-state, domestic, and transnational actors. These dynamics do not simply reflect institutional pluralism but expose deeper structural tensions between decentralisation and infrastructural control, particularly as emerging technologies are assembled within China's layered and often contradictory techno-political regime. In doing so, this analysis foregrounds how power is not only exercised through regulation, but also performed, refracted, and materially enacted through the discursive infrastructures of innovation.

This methodological framework contributes to broader debates on emerging technologies by demonstrating how blockchain and AI governance cannot be understood through presentist or techno-determinist frames

alone. Instead, they must be situated within historical regimes of speculation, control, and developmentalist co-optation. The speculative fervor surrounding blockchain during the 2010s, its subsequent repression, and the rise of AI as the new state-sanctioned frontier reveal not a rupture, but a recursive logic in which technologies are selectively refunctioned as tools of infrastructural nationalism and geopolitical projection. By foregrounding these continuities and ruptures, genealogical analysis illuminates how contemporary debates over decentralisation, autonomy, and techno-sovereignty are the latest iteration of older contests over legitimacy and control.

## 4. Case Study: Paradoxical Infrastructuring Between Decentralization and Centralization Trajectories

This section traces the rise and fall of blockchain in China as a paradigmatic case of infrastructural governance, where emergent technologies are alternately hyped, co-opted, and disciplined by the state. What began as a techno-utopian vision of DeFi, which was initially valorized under the "Internet Plus" policy framework, was gradually subsumed into a speculative apparatus enabled by elite protection, geopolitical recalibration, and opaque regulatory ambiguity. From the P2P lending collapse to the initial coin offering (ICO) crackdown, the blockchain sector reveals a recurring infrastructural playbook: Decentralization is tolerated only when it can be folded into state priorities or rendered symbolically useful for digital sovereignty. As China's blockchain governance bifurcated, embracing consortium chains while criminalizing crypto, the contradictions of infrastructural statecraft became apparent. This trajectory prefigures the AI hype cycle that follows, wherein the centralization of technological power is not a corrective to blockchain's volatility, but its systemic successor: a securitized, state-sanctioned infrastructure of innovation that repurposes decentralization's remnants as symbolic capital.

It is noteworthy that the Chinese context provides a particularly rich site for genealogical analysis, as it foregrounds the persistent struggle between the decentralizing potential of blockchain technologies and the political powers that opt for centralization. This struggle is not unique to blockchain but reflects a longer genealogy of digital governance in China, from early internet regulation to the contemporary AI-driven governance model. The increasing sophistication of China's digital governance architecture must be situated within evolving political contexts, including episodes of institutional restructuring and shifting regulatory priorities during the mid-2010s (see Isachenkov & Tong-hyung, 2023) and their entanglement with broader mechanisms of governance. However, while this period provides a crucial historical and political context, attributing specific policy decisions or regulatory shifts solely to leadership changes or discrete political events remains methodologically not rigorous. The relative opacity of internal bureaucratic deliberations further complicates efforts to isolate causal mechanisms. Therefore, scholarly analyses must account for the complex and often multi-causal nature of regulatory transformations, which emerge through the interplay of institutional path dependencies, bureaucratic negotiations, and shifting geopolitical considerations.

Building on Kitchin's (2015) notion of the "sedimentary" nature of digital infrastructures, where older technological and institutional layers persist and shape contemporary governance, China's approach to blockchain and AI exemplifies how centralizing and decentralizing forces coexist within a unified framework: While blockchain's foundational ethos of decentralization and distributed authority appears at odds with the Chinese state's centralized governance model, and AI's data-driven systems ostensibly amplify centralizing

power, both technologies are embedded within preexisting infrastructural and institutional "strata" that mediate their implementation.

### *4.1. Paradoxical Infrastructuring Playbook of Blockchain*

#### 4.1.1. Prelude

The history of China's short-lived P2P lending boom, which was previously endorsed by top-level officials during the "Internet Plus" era, offers a cautionary prelude. Though P2P platforms were celebrated for disintermediating finance, they operated within a quasi-state ecosystem of implied guarantees, where close ties to local governments misled investors into assuming official backing (Chorzempa, 2018; Z. Tang et al., 2022; "Zhou Xiao Chuan Wei," 2015). However, by 2016, the Chinese Banking Regulatory Commission suggested that nearly 40% of P2P platforms were Ponzi schemes (Shao & Bo, 2021), leading to massive financial losses and public protests (Y. Yang & Liu, 2018). When the market collapsed, it was not just a financial failure but *an epistemic crisis*. Actors held conflicting understandings of what kind of system they were participating in: a decentralized market innovation or a state-backed financial product. Investors entered a market celebrated as decentralized, yet they implicitly trusted in state protection; when platforms failed, this contradiction exposed the fragility of both discursive claims of decentralization and the expectations that the state, as the apex of political and economic authority, would ultimately intervene to ensure stability and protect investors.

The blockchain sector, which inherited P2P's decentralization ethos, became the next frontier for regulatory experimentation and co-optation. Yet rather than breaking with earlier digital economies, it often reproduced their extractive dynamics. The rise of speculative token models, most visibly the various X2EARN schemes (e.g., Play-to-Earn, Move-to-Earn, etc.), illustrates this continuity. These models' value proposition depends less on sustainable utility and more on attracting users/investors who hope the token price will rise. Therefore, though participants generate value (data, content, activity), that value is siphoned off upward or becomes unsustainable for latecomers, making contributions unevenly rewarded and often ended up enriching a small group at the top. At the same time, blockchain's symbolic association with autonomy and ungoverned flows made it both an alluring and troubling phenomenon for the state: a potential site of innovation that promises new economic models, governance tools, and global leadership narratives, but also a challenge to established regulatory authority.

#### 4.1.2. Hype: A National Strategy That Breeds Corruption (2011–2017)

China's blockchain narrative began in the establishment of Bitcoin China in 2011, which at its peak handled 80% of domestic crypto trading (Wong & Wong, 2017), and Wanxiang Blockchain Labs' landmark 2015 Global Blockchain Summit marked the private sector's embrace of blockchain as both a financial and ideological disruptor. VCs followed: Wanxiang Holdings' $50 million distributed-capital fund (Cyzone, 2020) underscored the market's faith in blockchain's potential to redefine economic agency, echoing centuries of decentralized systems advocacy from Adam Smith to Satoshi Nakamoto (Schneider, 2019). Between 2014 and 2017, DeFi innovations, particularly ICOs, surged globally, raising $18 billion while simultaneously exposing China to capital flight (Kharpal, 2022) and fraud risks (Groden, 2017). Public discourse amplified this fervor: Retail investors and tech media championed Bitcoin as a tool of "financial liberation," with WeChat posts touting cryptocurrency returns way above traditional assets (Huang, 2022).

While early blockchain enthusiasm in China was driven by visions of financial innovation and digital modernization, it also opened up opportunities for regulatory arbitrage and rent-seeking behavior at the local level. A widely reported case emerged in Jiangxi province, where Qingxing Lin, founder of Genesis Technology, collaborated with Yi Xiao, then Party Secretary of Fuzhou, to attract foreign blockchain investment under the broader umbrella of the Belt and Road Initiative (BRI). In 2017, Lin secured a substantial partnership with Germany's GM Foundation, which is an Ethereum mining conglomerate, to deploy large-scale infrastructure, including over 100,000 Ethereum rigs and 60,000 Antminer S9 machines, valued at more than RMB 1 billion. Subsequent allegations suggested that Lin had redirected a portion of the mining output to private wallets over a period of several years. Although the foreign partner sought legal recourse, local judicial outcomes were perceived as lacking responsiveness, leading to diplomatic escalation. In 2021, following mounting public scrutiny and cross-border concern, the Central Commission for Discipline Inspection launched a targeted investigation into irregularities surrounding crypto-related projects in the region. Yi Xiao was removed from office, and the case became part of a broader anti-corruption campaign addressing misconduct in the digital finance and blockchain sectors (Shen, 2023).

This episode underscores the challenges of governing rapidly evolving technological frontiers, where innovation policy may, at times, be co-opted by opportunistic actors. Such instances reflect a form of corruption that the state's developmental goals are occasionally exploited for private gain amid regulatory ambiguity. In response to the catalyst for the 2021 "519" crackdown, Chinese regulators launched a coordinated effort to dismantle the speculative crypto economy, spanning exchanges, over-the-counter trading, and mining. In this light, the blockchain boom of 2011–2017 appears not as a linear story of innovation, but a volatile mix of utopian finance, platform capitalism, and opportunistic predation under the guise of developing digital economy.

These dynamics are not unique to China's political system but reflect a broader global pattern of techno-political opportunism. In the US, Trump publicly endorsed cryptocurrency, launched Trump-themed non-fungible tokens (NFTs) and a $TRUMP meme coin on Solana, and, along with his sons, co-founded the crypto firm World Liberty Financial, ventures that generated over $57 million in token sales and positioned him as a central figure in a crypto-focused America First economy (Steer, 2025). Likewise, Elon Musk's engagement with cryptocurrency consistently served his own interests. By tweeting support for Bitcoin and Dogecoin, he triggered dramatic price fluctuations that enriched early holders, himself included, while cultivating a cutting-edge, libertarian, and anti-establishment persona. Yet these gestures of empowerment from decentralizing technologies operated less as an ideological commitment than market manipulation. Musk's subsequent retreat, distancing himself from Dogecoin and exiting the Trump administration's DOGE initiative, might suggest not disillusionment but tactical disengagement after the peak of symbolic and financial extraction (Mourya, 2025).

In both cases, blockchain hype became a discursive smokescreen that masked deeper public–private entanglements. As in China's Fuzhou mining scandal, where local officials like Yi Xiao expropriated foreign blockchain assets under the guise of BRI-linked cooperation, US counterparts similarly repurposed innovation as spectacle, embedding political ideology and economic opportunism into the infrastructure of emerging technologies. Whether via princeling patronage or libertarian meme-currencies, both systems demonstrate how blockchain's emancipatory promise could be subordinated to political theatre and rentier accumulation.

### 4.1.3. Bifurcated Governance in Response to Crypto-Geopolitics: A Turning Point in 2017 and Elevation in 2019

The geopolitical rationale became particularly salient during the 2017 ICO crackdown. Against the backdrop of US tariffs, the Committee on Foreign Investment in the United States reforms targeting Chinese tech investments (Hanifin et al., 2017), and punitive sanctions against ZTE and Huawei (Gallagher, 2022), blockchain's borderless design was seen not as liberatory, but as a strategic liability. By banning domestic crypto exchanges and ICOs (L. Y. Chen & Lee, 2017), the state preemptively neutralized decentralized architectures that might undermine capital controls or expose China's tech ecosystem to US financial surveillance, insulating critical infrastructures from Western dependencies (Lin & Wang, 2021).

Within this securitized landscape, Binance emerged as a symbolic and material rupture. Founded in 2017 by Chinese-Canadian entrepreneur Changpeng Zhao, Binance was simultaneously born of China's blockchain boom yet structurally and discursively disembedded from it. While Binance formally exited China following the September 2017 crypto ban, evidence suggests continued infrastructural entanglements: payroll routed through Chinese banks, active domain use (binancezh.com), and ambiguous operational footprints long after its official departure (Chipolina, 2023).

Binance's global posture further complicates the landscape. In contrast to its obscured links to China, Binance projects a dissident image in the West. Changpeng Zhao is cast not as a parastatal actor but as a tech exile, a founder who claims to be "escaping authoritarianism" and building a decentralized future. This narrative has gained traction across libertarian crypto circles and US lawmakers seeking non-state-aligned crypto champions ("Binance CEO Changpeng Zhao responds," 2023). Binance thereby performs a double detachment: It distances itself from China's state apparatus while capitalizing on its origin story to claim authenticity in a "Web3 Cold War." Binance is thus more than a financial intermediary; it is a *geopolitical interface* where decentralization and deregulation are framed as resistance against state overreach.

Seen through the lens of governmentality, Binance appears as the object of competing rationalities of rule—securitized by China, problematized by US regulators, courted by libertarian crypto advocates. Yet, in Szonyi's sense, Binance exemplifies an intermediary actor that, like lineage institutions in late imperial China, navigates overlapping regimes of authority through selective entanglement and strategic ambiguity. Maintaining infrastructural ties to China while claiming and performing dissident authenticity in the West, its dual posture illustrates how organizations, no less than individuals, transform regulatory constraint into a resource for legitimacy and expansion. The tension between these two frameworks thus illuminates both the rational logics of state power and the situated practices through which actors like Binance inhabit and reconfigure them.

In 2019, local governments, which had initially incentivized blockchain industrial parks (e.g., Hangzhou's "Blockchain Town"), scaled back subsidies amid concerns about wasted resources. The downturn revealed a structural tension: While blockchain was rhetorically championed as part of China's "digital economy" strategy, its decentralized, permissionless ethos clashed with the state's preference for controlled, institutionally anchored innovation. By 2019, the surviving blockchain ecosystem had largely reoriented toward state-sanctioned use cases, such as government-backed consortium chains for bureaucratic record-keeping, signaling a retreat from the earlier vision of blockchain as a disruptive, market-driven force.

In January 2019, the Cyberspace Administration of China issued the Regulations on the Management of Blockchain Information Services, stating that blockchain technology, while offering innovative potential, carries security risks of being used in "criminal activities to spread illegal and harmful information" (Zhuang, 2019, Article 10). Although the regulation does not explicitly target political activism, its release followed a period in which blockchain platforms had been explored by activist communities as tools for building encrypted, censorship-resistant networks (Zhai & Chen, 2018). This regulatory move might reflect a broader effort to preemptively assert oversight over emerging infrastructures, particularly as their affordances intersect with contentious forms of information dissemination.

The *formal elevation* of blockchain to be co-opted as a strategic priority in China's national development, particularly following the president's endorsement in October 2019, subsumes blockchain's technological innovation into the state's broader geopolitical agenda. While blockchain was initially framed as a tool for digital transformation, its institutionalization within state-controlled initiatives such as the Blockchain-based Service Network suggests a concerted effort to align its development with China's national security, economic sovereignty, and global influence strategies. This alignment merits scrutiny, particularly in relation to two key dimensions: (a) the US–China technological rivalry and (b) China's digital infrastructure expansion under the BRI.

By embedding blockchain into BRI-linked projects, such as cross-border payment systems or smart logistics networks, China can export its digital governance model to partner nations, particularly in regions like Southeast Asia, Africa, and the Middle East, where BRI investments are concentrated. This not only reduces reliance on Western financial systems (e.g., SWIFT) but also creates dependencies on Chinese technological ecosystems, insulating these regions from US regulatory pressure (Xu Elegant, 2019). Therefore, blockchain's institutionalization reflects a calculated convergence of economic defensiveness (evading US sanctions) and geopolitical assertiveness (expanding BRI's digital footprint). Through BRI-linked digital infrastructure, China is not merely building roads and ports but constructing a parallel digital order—one where it holds the architectural and geopolitical blueprints.

Thus, the Chinese state's response to this emerging contradiction was bifurcated. On one hand, it celebrated blockchain as an infrastructural solution, integrating it into policy discourse via the 13th Five-Year Plan (China's State Council, 2016) and subsequent white papers on smart cities and digital governance. On the other, it drew a hard line against cryptocurrencies, culminating in the September 2017 ban on ICOs and domestic exchanges. This split mirrors the state's attempt to retain control over financial sovereignty while appropriating only the politically productive aspects of technological decentralization.

#### 4.1.4. Resilience and Reincorporation: The Art of Being Governed in Post-Crypto Hype China (Since 2019)

Industry observers, including the prominent Chinese "TechCrunch" media 36Kr (2018), documented this downturn, noting that over 80% of blockchain projects launched during the peak of the 2017–2018 "blockchain bubble" had either collapsed or pivoted to non-blockchain ventures by late 2018, and investors thus shifted focus to less speculative sectors like AI and semiconductors (Musharraf, 2019).

However, the mainland Chinese crypto "hype" communities still manage to carve out operational space within a restrictive, and often prohibitive, digital governance landscape.

As early as 2020, some Weibo users, seeking alternatives to platform censorship, migrated to decentralized platforms like Mastodon, framing these moves as aligned with blockchain's decentralized ethos. Media organizations also attempted to formalize decentralized models through DAOs (TechFlow, 2023). However, the National Development and Reform Commission intervened, barring non-public capital from news production and rendering DAO-based media structurally illegal (Feng, 2021). In 2023, Damus (a DAO) was removed from the China App Store due to its potential to create a censorship-resistant global social network (Feng & Haldane, 2023). However, despite increasing regulatory constraints, a significant number of Chinese users remain active participants in the global InterPlanetary File System (IPFS) network, leveraging its decentralized infrastructure to circumvent censorship (Haldane, 2022). Likewise, in DAOs, underground cryptocurrency activities have persisted. Between July 2022 and June 2023, China's crypto market recorded an estimated $86.4 billion in transaction volume, indicating robust activity despite official bans (Ranganathan & Zhen, 2024).

Likewise, despite regulatory expulsion, traces of China's crypto legacy persist in platforms like Binance, whose operations remain tethered both culturally and materially to the Chinese digital sphere. Even amidst the 2021 nationwide ban on crypto trading and mining (M. Chen, 2023) evidenced by "5·19 大血洗" ("the big crypto purge on 19 May") when Bitcoin, Ethereum, Dogecoin, and other altcoins fell sharply by 50–60% (Pound, 2021), the persistence of Chinese-language access guides, Telegram communities, and dedicated customer service teams highlights the continued salience of the mainland Chinese user base. While precise figures remain opaque, comparative metrics such as FTX's bankruptcy disclosures—which revealed that 8% of its users were located in China—suggest that Binance's Chinese clientele, though officially disavowed, remains significant (Broersma, 2025).

The dynamics of symbolic flexibility and institutional adaptation are particularly evident in the evolving public reception of Yuchen (Justin) Sun. Once a prominent figure in China's early crypto entrepreneurial scene, Sun was charged in 2023 by the U.S. Securities and Exchange Commission (2023) for alleged violations involving the unregistered sale of digital assets and extensive wash trading practices. While these allegations positioned him as a controversial figure in international regulatory discourse, his trajectory within China evolved along a different path. By 2025, Sun appeared as an invited speaker at a national conference hosted by the Southwest University of Political Science and Law, joining discussions alongside legal scholars, prosecutors, and judicial officials (Southwest University of Political Science and Law, 2025).

This episode reflects a broader feature of China's utilitarian approach to digital governance: Individuals with complex or contested reputations may be re-engaged in public discourse, particularly when their experiences offer insights into the regulatory, legal, and economic challenges of emerging technologies. Sun's reappearance in such a setting does not indicate uncritical endorsement, but illustrates how governance systems can draw selectively on diverse forms of expertise to inform ongoing legal and institutional development.

More broadly, this case points to the differentiated modes of participation available within China's evolving blockchain policy ecosystem. While regulatory measures have tightened around speculative retail activities and unauthorized platforms, actors with institutional visibility or transnational experience may be incorporated into dialogues on rule-making and techno-legal reform. Rather than a straightforward narrative of rehabilitation or endorsement, Sun's case illustrates the complex interplay between regulation, symbolic capital, and policy experimentation within a fast-moving and strategically governed digital landscape.

#### 4.1.5. Summary

China's blockchain trajectory cannot be adequately understood through a binary of initial hype and subsequent repression. Rather, what this section reveals is a more complex interplay between technological imaginaries, speculative logics, and contested infrastructuring practices, in which state agendas, geopolitical pressures, and market actors collide. From early P2P platforms to ICO frenzies and the rise, and partial fall, of Binance, blockchain in China has not followed a linear arc of innovation, but has functioned as a discursive battleground, where truth claims about value, sovereignty, and decentralisation are continuously produced, contested, and reassembled.

Framed through a Foucauldian lens, the blockchain sector in China has operated as an assemblage where power circulates not only through regulation but through infrastructural design, media discourse, and speculative affect. Alternating between endorsement and crackdowns, the state's ambivalent governance should not be read as inconsistent, but as an evolving strategy of *governmentality*, in which decentralisation is tolerated, even nurtured, insofar as it can be selectively repurposed toward strategic ends. The institutionalisation of the Blockchain-based Service Network exemplifies this: Blockchain's disruptive affordances are translated into state-aligned infrastructure, and subsumed into a vision of digital sovereignty and global projection under BRI's "Digital Silk Road."

Yet this is not simply a story of co-optation. Drawing on Michael Szonyi's (2017) notion of "the art of being governed," the crypto sector in China also reveals how actors at the margins, including developers, influencers, VC investors, and techno-entrepreneurs, adapt, recalibrate, and even exploit the elasticity of official discourse to advance their own agendas. These actors navigate the blurry space between compliance and resistance, performing decentralisation as a cultural and economic script even as they embed themselves within the hierarchies they rhetorically oppose. Whether through DAO experiments, IPFS file-sharing, or cross-border arbitrage, these everyday infrastructural practices represent modes of situated agency, not outside the system but *within and through* its contradictions.

Even amidst industry winters, crypto communities persist, sometimes rebranding themselves around AI or Web3, other times operating underground but globally networked. Their strategies are neither heroic nor entirely cynical but instead reflect the ambivalent subjectivity of being governed in a techno-political regime that rewards calculated opacity, instrumental alignment, and entrepreneurial risk. Binance's post-2017 transformation into a transnational crypto empire, simultaneously disavowing and benefiting from its Chinese origins, demonstrates how decentralization itself can become a rhetorical resource for the performance of geopolitical power, mobilized differently across ideological contexts but always embedded in power.

Ultimately, China's blockchain story is not one of failed decentralization, but of discursively reconfigured decentralization, a political imaginary that remains potent, mutable, and strategically actionable. What this analytical section has shown is that blockchain's life in China is not over, but unfolding across infrastructural margins and epistemic thresholds, shaped as much by crypto dissidents and influencer-entrepreneurs as by cadres and regulators. Blockchain, like AI, is no longer a frontier to be just governed, but a terrain through which governance is imagined, contested, and reassembled, mirroring China's broader digital statecraft, and a reminder that technologies never simply disrupt or empower; their meanings and affordances are constantly performed, negotiated, and reconfigured by actors embedded within power-laden infrastructures.

### *4.2. Reassembling Power: Blockchain's Afterlife in China's AI Turn*

By 2023, China's state-approved blockchain market had been rendered largely stagnant. Yet rather than reassess its rigid stance, the state doubled down on control, relegating blockchain to the sidelines while championing AI as the next strategic frontier, an arena where centralized oversight could be embedded from the outset.

#### 4.2.1. Innovation Emerging From Market Competition

China's first AI move in the private sector was Baidu's establishment of its Deep Learning Institute in 2013, focusing on AI research, including speech recognition and autonomous driving. In 2014, Baidu recruited prominent AI researcher Andrew Ng to lead its AI efforts, drawing global attention. Companies like SenseTime (founded 2014) and Megvii (best known for its product Face++. Face++ is the world's largest computer vision platform founded in 2011, which pivoted to AI in 2014) began gaining traction in facial recognition and computer vision, attracting significant VCs. In March 2016, Lee Sedol's defeat at the hands of Google's AlphaGo ignited widespread interest in AI across China, particularly due to Go's cultural significance. This event catalyzed public and private investment, with tech giants like Alibaba, Baidu, and Tencent accelerating AI R&D (see "PaddlePaddle receives full upgrade," 2021; Simonite, 2019). In 2017, China accounted for 48% of the world's total AI startup funding, compared to America's 38% (Diamandis, 2018). This hype echoes the way influential AI researcher Andrew Ng described AI as the "new electricity," forecasting it would transform industries much like electricity did in the 20th century (Ng, 2017, as cited in Lynch, 2017).

#### 4.2.2. Contested Process of AI's Institutionalization

##### 4.2.2.1. Strategical Securitization of AI: A Frontline in a New Epistemic Cold War

Far from being merely a domestic response to innovation cycles, the rise of AI—and before it, blockchain—constitutes a strategic recalibration of state power in the context of intensifying Sino-American technological decoupling, geopolitical rivalry, and epistemic sovereignty struggles.

2017 was a critical moment when the state bet on both blockchain technologies and AI, yet its scale of policy preferences began tipping in favor of AI. The trajectory of China's digital economy, shaped by intensifying US–China technological competition, reveals a strategic interplay between blockchain governance, AI development, and geopolitical maneuvering. While not AI-specific, the state-led initiatives "Internet Plus" ("Premier Li and Internet Plus," 2015) and "Made in China 2025" (China's State Council, 2015) emphasized advanced technologies, laying the groundwork for AI integration (Central People's Government of the People's Republic of China, 2022). The Chinese government unveiled a national AI strategy called Next Generation AI Development Plan (July 2017; see translation in Webster et al., 2017), aiming to make China the global AI leader by 2030. This policy included massive funding, talent recruitment, and industrial goals, positioning AI as a top priority. Following this initiative, cities like Beijing, Shanghai, and Shenzhen launched AI industrial parks and funding programs post-2017, aligning with central government directives (Xiao, 2024).

Since 2018, when Xinhua News (2018) framed China's AI progress as advancing "amidst controversies," the state has grappled with balancing innovation against persistent risks like data leaks and privacy violations. Post-2018, state investment shifted toward industrial applications, with over $15 billion allocated to healthcare and manufacturing AI (China's National Development and Reform Commission, 2024), directly aligning with the Made in China 2025 agenda. This pivot reveals a deliberate bifurcation: While consumer-facing generative AI faced scrutiny regarding ethics, industrial AI gained legitimacy as a productivity enhancer.

These tensions have only deepened as China confronts US semiconductor sanctions and the capital-intensive demands of AI research. The US government's sanctions against Chinese chipmakers, including SMIC, and restrictions on advanced AI chip exports (such as Nvidia's high-performance GPUs) have forced China to explore alternative approaches. These constraints have catalyzed domestic efforts to integrate blockchain with AI to optimize computational efficiency, facilitate distributed data training, and mitigate reliance on US chip technology. By 2024, initiatives such as the national "AI+" proposal introduced by Premier Li Qiang (see Jiang, 2024) underscore efforts to consolidate domestic AI infrastructure while addressing cybersecurity and circumventing Western tech dependencies. This dual imperative (innovation alongside control) reflects a broader reimagining of technological self-reliance, where blockchain emerges as both a tool for decentralization and an instrument of state power. Therefore, this pivot to AI, which replicates blockchain's infrastructuring playbook, reflects a governance model that privileges technologies with legible, centralized utility.

Along the same lines, AI is securitized for military purposes. Under the "civil-military fusion" (军民融合) strategy, explicitly institutionalized in the broader national defense modernization agenda, the boundaries between civilian innovation and military application are deliberately blurred, ensuring that advances in commercial AI feed directly into strategic defense capabilities. In this context, AI research has been increasingly oriented toward dual-use applications, including autonomous weapons systems, military logistics optimization, surveillance infrastructure, and wargaming simulations (Kania, 2020). The boundary between civilian and military use remains deliberately blurred, allowing frontier innovation, particularly in natural language processing, computer vision, and reinforcement learning, to flow *seamlessly* into defense-oriented laboratories and procurement chains. In this sense, China's AI governance is not simply a national industrial policy, but a frontline in a new epistemic Cold War, where infrastructures are both weapons and targets. Technologies like AI and blockchain are not merely being developed—they are being securitized, symbolically charged with national survival, and deployed as tools of soft and hard sovereignty in a fractured global order. This demands an analytical framework that asks: Whose future, whose security, and whose power is embedded in these technologies?

Admittedly, China's DeepSeek, a very geopolitically impactful move, is an open-source model—challenging the dominance of the US AI companies and shifting the industry. However, in the case of DeepSeek, open-sourcing may appear to signal a departure from state-centric control. Yet it also functions as a geopolitical maneuver that enhances China's soft power and technical legitimacy in global AI discourse (Z. Yang, 2025a). In this sense, DeepSeek represents not an erosion of the playbook, but a strategic deployment of openness as state-aligned infrastructure, a recalibration of the same logic that once governed China's internet expansion.

#### 4.2.2.2. Entangled and Pragmatically Profiting Stakeholders That Tried to Revalorize Blockchain in China's AI Hype

Under the banners of AI revolution and digital economy China has launched an ambitious array of state-backed initiatives—including numerous state-backed tenders, pilot zones, and industrial parks in China. While many of these programs have contributed meaningfully to digital infrastructure and talent cultivation, some have evolved into hybrid spaces where strategic ambition intersects with discretion and speculative opportunism. In the effort to foster national champions and enhance digital sovereignty, public investment has supported a wave of AI–blockchain integration projects. Yet in some cases, such initiatives have exhibited limited transparency and uneven outcomes, raising questions about how innovation discourse is mobilized in practice. As revealed in the aforementioned exposé on the Fuzhou mining scandal, the legitimizing discourse of, and the symbolic alignment with, cutting-edge technologies can, under certain circumstances, create space for speculative behavior, resource misallocation, or policy–market frictions.

Yet more striking is blockchain's rhetorical resurrection under AI-centric development discourse. Far from a principled return, this revival is better understood as techno-nostalgic arbitrage: Blockchain is not re-emerging for its original decentralized affordances, but for its speculative and legitimizing potential in a moment of infrastructural strain. As AI development encounters challenges in data sovereignty, energy consumption, and regulatory scrutiny, blockchain is repurposed—as back-end infrastructure, as aesthetic veneer, as speculative narrative. Reports from firms like IBM and KPMG (2023) reframe blockchain as an "efficiency layer" for federated learning and as a tool to secure intellectual property rights and ensure compliance. Chinese media platforms such as *The Paper*, *TechFlow*, and *36Kr* amplify these claims, hailing a revolutionary fusion of cryptographic infrastructure and autonomous AI agents. What emerges is not a roadmap for innovation but a speculative hedge that converts ideological incoherence into asset value. Blockchain is remembered, rebranded, and reinserted as part of a broader elastic choreography of state–capital relations. While blockchain entrepreneurs once symbolized risky speculation and were cast outside the regulatory fold, they were reintegrated under the rubric of legal rationalization and AI–blockchain "integration."

In this sense, blockchain's reappearance under the AI umbrella is a reminder that technologies do not simply die or survive; they are repositioned within power-laden discursive infrastructures, the institutionalized systems of meaning-making—including media, policy, legal frameworks, industrial discourse, and platform governance—that structure how technologies are talked about, imagined, legitimized, and operationalized. What seems like a technological revival is, in fact, a strategic realignment of interests, where ideological contradictions are capitalized upon, and legitimacy is fungible, exchangeable across legal, financial, and political registers. Blockchain, once sidelined, now lives on as ghost infrastructure in the AI age: animated not by its decentralized promise, but by its utility as speculative rhetoric and techno-political currency.

Furthermore, local governments, incentivized by promotion metrics tied to "AI innovation," channel resources into constructing AI industrial parks and pilot zones. In doing so, they push regional enterprises to adopt immature AI systems, such as automated customer service or AI-driven factory upgrades, not out of operational need but to meet project indicators and attract investment. This often imposes high maintenance costs, disrupts existing workflows, and converts small firms into testing grounds in state-led digital modernization. The phenomenon of firms coerced by local performance metrics or investor pressure

into adopting AI systems prematurely illustrates how state-led innovation agendas often prioritize appearances of progress over practical viability, leaving smaller firms especially vulnerable (Z. Yang, 2025b). The Beijing and Shenzhen governments launched multi-million-yuan robotics funds, only accessible to firms meeting high production/usage thresholds. While this provision spurs development, it also creates pressures. Smaller enterprises must deploy or upgrade to costly robot systems to access government subsidies, with operating costs often ballooning post-adoption. These mandates force firms to undertake premature AI adoption, on pain of losing funding (Goh et al., 2025).

At the enterprise level, the speculative burden is passed downward: to workers whose repetitive jobs are displaced (e.g., translators, customer service agents, even journalists), and to workers expected to shoulder the costs of "reskilling" in response to top-down automation, not as a right or guarantee, but as an individual responsibility. The promise of AI, including efficiency and national power, thus obscures an extractive structure of techno-governance that might reshuffle risk downward while concentrating symbolic capital upward (Olcott, 2024).

This dynamic is illustrative of this article's conjunctive framework by epitomizing the tension between governmentality and the art of being governed: while the state operationalizes innovation through metrics, subsidies, and discursive promises of AI as a symbol of modernization, enterprises and workers must inhabit these demands tactically, often at great cost. Their sometimes coerced compliance reveals how governance rationalities translate into everyday negotiations of survival, illustrating the gap between the symbolic capital of "AI progress" and the precarious realities it produces for the wider range of stakeholders.

#### 4.2.3. Summary

This case study examines China's pivot from blockchain to AI not as a linear progression of technological development, but as a paradigmatic shift in building the infrastructure of state power. Drawing on Foucauldian concept of governmentality, science and technology studies (STS) scholarship on hype cycles, and infrastructural imaginaries, this sub-section argues that while early AI innovation emerged from private-sector competition, the post-2017 institutionalization of AI—through national policy, military-civil fusion, and local government's performance metrics—reveals a techno-political choreography in which centralized control and decentralized experimentation are not contradictory but co-constitutive. In this landscape, blockchain reappears not as a disruptive alternative, but as a symbolic and infrastructural supplement to AI development, legitimizing state-led projects and masking elite rent-seeking. The result is a techno-governance regime in which emerging technologies serve as instruments of epistemic sovereignty, where infrastructural hype justifies extractive practices and where the burden of automation risks being redistributed downward onto precarious workers, small enterprises, and workers tasked with self-reskilling under the banner of national innovation.

## 5. Conclusion: Technologies of Governance, Infrastructures of Power

This article has traced the entangled trajectories of blockchain and AI in China not as isolated episodes of innovation and repression, but as iterative moments in a deeper political logic of infrastructural governance. It argued that neither blockchain's ethos of decentralization nor the centralizing logic of AI can be understood apart from the discursive regimes and institutional choreographies that govern their adoption, reinvention, and

symbolic utility. Both technologies function less as tools of liberation or control per se, and more as discursive assemblages, arenas in which truth claims, moral legitimacy, and political authority are produced, contested, and reassembled.

China's digital governance strategy does not suppress decentralization outright, nor does it simply instrumentalize AI as a neutral administrative upgrade. Rather, it cultivates a techno-political ecology in which disruption is tolerated, sometimes even encouraged, so long as it can be rendered legible, governable, and ideologically useful. The fate of blockchain exemplifies this: hyped as a vehicle for financial emancipation, criminalized in the name of state sovereignty, and ultimately reborn as ghost infrastructure within AI-centric narratives of productivity and geopolitical resilience. The return of blockchain is thus not a technological renaissance, but a discursive realignment, an example of what this research terms "paradoxical infrastructuring" where symbolic capital is extracted from the ruins of prior disruption.

Crucially, this logic is sustained not only by the state but by a constellation of intermediary actors, such as crypto entrepreneurs, influencer-developers, local officials, and VC-backed firms, who navigate the blurry terrain between compliance and autonomy. Drawing on Szonyi's (2017) "art of being governed," these actors advocate for decentralization while reinforcing the very hierarchies they claim to oppose, thus thriving on ambiguity and instrumental alignment.

The shift from blockchain to AI hype, then, should not be seen as a pivot from chaos to order, but as a recursive rearticulation of governance through infrastructural opacity, opportunistic rent-seeking and redistribution of burden to less advantaged socioeconomic groups, based on what it can be made to signify for the state, for markets, and for the subjects who navigate their contradictions. The case of China is not an exception, but a particularly vivid instance of how emerging technologies are governed through a fusion of infrastructural seduction (where digital systems promise efficiency, control, and innovation), discursive elasticity (where terms like "blockchain," "AI," or "decentralization" are stretched to serve shifting political and economic agendas), and strategic ambiguity (where state actors deliberately blur boundaries between promotion and prohibition, openness and restriction, in order to retain maximum flexibility and authority). It serves as a mirror, reflecting both China's evolving digital infrastructures and regulatory practices and the global condition where innovation is inseparable from struggles over political authority and market control.

## Acknowledgments

I am deeply grateful to my friend David Chu, researcher at the University of Western Ontario, for his incisive and generative feedback. His insights offered a new analytical lens that significantly enriched the scope of this article. In particular, he encouraged me to move beyond conventional readings of state-centric governance by engaging more critically with tech journalism and the discourse of investor communities online. This shift allowed me to better understand the tactical and often ambivalent responses of non-state actors navigating digital and infrastructural governance. His intellectual generosity and sharp editorial sensibility were instrumental to the development of this article.

## Conflict of Interests

In this article, editorial decisions were undertaken by Chang Zhang (Communication University of China) and Denis Galligan (University of Oxford).

## Data Availability

This article draws on policy documents, journalistic reports, industrial reports, and online community discussions, and which are available both in the bibliography and the supplementary file.

## LLMs Disclosure

LLMs were used only for proofreading.

## Supplementary Material

Supplementary material for this article is available online in the format provided by the author (unedited).

## References

36Kr. (2018). Qu Kuai Lian Mei You Wei Lai, Shi Shi Hou Pao Qi Ta Le. https://36kr.com/p/1722491813889

Bauer, M. W., & Schiele, B. (Eds.). (2023). *Science communication: Taking a step back to move forward*. CNRS Editions.

Binance CEO Changpeng Zhao responds to CCP affiliation claims. (2023, March 10). *Binance Square*. https://www.binance.com/en/square/post/291845

Bowker, G. C., Baker, K., Millerand, F., & Ribes, D. (2009). Toward information infrastructure studies: Ways of knowing in a networked environment. In J. Hunsinger, L. Klastrup, & M. Allen (Eds.), *International handbook of internet research* (pp. 97–117). Springer. https://doi.org/10.1007/978-1-4020-9789-8_5

Broersma, M. (2025, January 9). China ex-official publicly shamed over crypto corruption. *Silicon UK*. https://www.silicon.co.uk/e-marketing/epayment/china-crypto-crackdown-492205

Central People's Government of the People's Republic of China. (2022). *Notice of the State Council on the publication of "Made in China 2025"—Translation*. Centre for Security and Emerging Technologies. https://cset.georgetown.edu/publication/notice-of-the-state-council-on-the-publication-of-made-in-china-2025

Chen, M. (2023). Guo Qi De Qu Kuai Lian, Hang Ye Han Dong Li De Kuang Gong. *Jiemian Media*. https://m.jiemian.com/article/10268856.html

Chen, L. Y., & Lee, J. (2017, September 4). Bitcoin tumbles as PBOC declares initial coin offerings illegal. *Bloomberg*. https://www.bloomberg.com/news/articles/2017-09-04/china-central-bank-says-initial-coin-offerings-are-illegal?embedded-checkout=true

China's National Development and Reform Commission. (2024). Zhuan Jia Guan Dian: Jia Kuai Xing Cheng Xin Zhi Sheng Chan Li: Shi Shen Me, Wei Shen Me, Zuo Shen Me? https://www.ndrc.gov.cn/wsdwhfz/202402/t20240206_1363980.html

China's State Council. (2015). *Guo Wu Yuan Guan Yu Yin Fa Zhong Guo Zhi Zao 2025 De Tong Zhi*. https://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm

China's State Council. (2016). *Shi San Wu Guo Jia Xin Xi Hua Gui Hua*. https://www.gov.cn/zhengce/content/2016-12/27/content_5153411.htm

Chipolina, S. (2023, March 29). Binance hid extensive links to China for several years. *Financial Times*. https://www.ft.com/content/4d011d5a-37ae-435a-9c7d-a163b4c92308

Chorzempa, M. (2018, August 21). Massive P2P failures in China: Underground banks going under. *China Economic Watch*. https://www.piie.com/blogs/china-economic-watch/massive-p2p-failures-china-underground-banks-going-under

Cossu, A. (2022). Cultures of digital finance: The rise of the financial public sphere. *International Journal of Cultural Policy*, *28*(7), 845–857. https://doi.org/10.1080/10286632.2022.2137158

Crawford, K. (2021). *Atlas of AI*. Yale University Press.

Cyzone. (2020). *Qu Kuai Lian, Shanghai You Diao Dui Le Ma*? https://m.cyzone.cn/article/571634

Diamandis, P. H. (2018, August 29). China is quickly becoming an AI superpower. *SingularityHub*. https://singularityhub.com/2018/08/29/china-ai-superpower

Feng, C. (2021, October 9). Beijing reiterates ban on private capital in news media, updating it to prohibit hosting events. *South Morning China Post*. https://www.scmp.com/tech/policy/article/3151778/beijing-reiterates-ban-private-capital-news-media-updating-it-prohibit

Feng, C., & Haldane, M. (2023, February 6). Apple's removal of Damus social media platform from China App Store was 'expected' by developers amid Beijing's strict censorship. *South Morning China Post*. https://www.scmp.com/tech/policy/article/3209265/apples-removal-damus-social-media-platform-china-app-store-was-expected-developers-amid-beijings

Foucault, M. (1977). *Discipline and punish: The birth of prison*. Vintage Books.

Foucault, M. (1981). The order of discourse. In R. Young (Ed.), *Untying the text: A post-structuralist reader* (pp. 48–51). Routledge; Kegan Paul.

Foucault, M. (1994). *The order of things: An archaeology of the human sciences*. Vintage Press.

Foucault, M. (2008). *The birth of biopolitics. Lectures at the College de France, 1978-1979*. Palgrave Macmillan.

Gallagher, J. C. (2022). *U.S. restrictions on Huawei Technologies: National security, foreign policy, and economic interests*. Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R47012/2

Goh, B., Baptista, G., & Li, Q. (2025, May 13). China's AI-powered humanoid robots aim to transform manufacturing. *Reuters*. https://www.reuters.com/world/china/chinas-ai-powered-humanoid-robots-aim-transform-manufacturing-2025-05-13

Groden, C. (2017). Understanding China's crackdown on Bitcoin and ICOs. *Lawfaremedia*. https://www.lawfaremedia.org/article/understanding-chinas-crackdown-bitcoin-and-icos

Haldane, M. (2022, April 16). Web3 tech helps banned books on piracy site Library Genesis slip through the Great Firewall's cracks, but for how long? *South Morning China Post*. https://www.scmp.com/tech/tech-trends/article/3172431/web3-tech-helps-banned-books-piracy-site-library-genesis-slip

Hanifin, B. C., Seelinger, S., & Siegle, E. (2017, September 18). CFIUS continues to present an obstacle to Chinese acquisitions. *Ropes & Gray*. https://www.ropesgray.com/en/insights/alerts/2017/09/cfius-continues-to-present-an-obstacle-to-chinese-acquisitions

Hartong, S., & Piattoeva, N. (2021). Contextualizing the datafication of schooling—A comparative discussion of Germany and Russia. *Critical Studies in Education*, *62*(2), 227–242. https://doi.org/10.1080/17508487.2019.1618887

Huang, E. (2022, July 21). China is now policing cryptocurrency by targeting WeChat accounts. *Quartz*. https://qz.com/1365874/china-cracks-down-on-cryptocurrency-by-shuttering-wechat-accounts

Isachenkov, V., & Tong-hyung, K. (2023, March 10). Xi awarded 3rd term as China's president, extending rule. *AP*. https://apnews.com/article/xi-jinping-china-president-vote-5e6230d8c881dc17b11a781e832accd1

Jiang, B. (2024, March 11). 'Two sessions' 2024: China's lawmakers call for more AI development to catch up with US, while keeping it under regulatory control. *South Morning China Post*. https://www.scmp.com/tech/policy/article/3254851/two-sessions-2024-chinas-lawmakers-call-more-ai-development-catch-us-while-keeping-it-under

Kania, E. (2020). *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

Kharpal, A. (2022, August 21). Report finds $50 billion of cryptocurrency moved out of China hinting at capital flight against Beijing rules. *CNBC*. https://www.cnbc.com/2020/08/21/china-users-move-50-billion-of-cryptocurrency-out-of-country-hinting-at-capital-flight.html

Kitchin, R. (2015). Making sense of smart cities: Addressing present shortcomings. *Cambridge Journal of Regions, Economy and Society*, *8*(1), 131–136. https://doi.org/10.1093/cjres/rsu027

KPMG. (2023). *Responsible AI and the challenge of AI risk*. https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2023/ai-risk-survey.pdf

Larkin, B. (2013). The politics and poetics of infrastructure. *Annual Review of Anthropology*, *42*, 327–343. https://doi.org/10.1146/annurev-anthro-092412-155522

Lin, Y. J., & Wang, X. (2021). Dual circulation: A new structural economics view of development. *Journal of Chinese Economic and Business Studies*, *20*(4), 303–322. https://doi.org/10.1080/14765284.2021.1929793

Lynch, S. (2017, March 11). Andrew Ng: Why AI is the new electricity. *Insights by Stanford Business*. https://www.gsb.stanford.edu/insights/andrew-ng-why-ai-new-electricity

Mourya, E. (2025, April 2). Is Dogecoin hype dead? Elon Musk says DOGE not in US plans. *Crypto News*. https://crypto.news/is-dogecoin-hype-dead-elon-musk-says-doge-not-in-us-plans

Musharraf, M. (2019, July 22). VC investment in blockchain sees steep decline, down 60% in comparison to 2018. *Be(in)crypto*. https://beincrypto.com/vc-investment-in-blockchain-sees-steep-decline-down-60-in-comparison-to-2018

Olcott, E. (2024, November 14). 'Robot revolution' forces China's human workforce to adapt. *Financial Times*. https://www.ft.com/content/dc7e1117-11d1-4da4-8af0-931fe967f548

PaddlePaddle receives full upgrade to facilitate integrated innovation and lower thresholds. (2021, May 27). *Baidu Research*. https://research.baidu.com/Blog/index-view?id=157

Pound, J. (2021, May 19). The crypto collapse: Here's what's behind bitcoin's sudden drop. *CNBC*. https://www.cnbc.com/2021/05/19/the-crypto-collapse-heres-whats-behind-bitcoins-sudden-drop.html

Ranganathan, V., & Zhen, S. (2024, January 25). Bruised by stock market, Chinese rush into banned bitcoin. *Reuters*. https://www.reuters.com/technology/bruised-by-stock-market-chinese-rush-into-banned-bitcoin-2024-01-25

Rozas, D., Tenorio-Fornés, A., Díaz-Molina, S., & Hassan, S. (2021). When Ostrom meets blockchain: Exploring the potentials of blockchain for commons governance. *Sage Open*, *11*(1). https://doi.org/10.1177/21582440211002526

Schneider, N. (2019). Decentralization: An incomplete ambition. *Journal of Cultural Economy*, *12*(4), 265–285. https://doi.org/10.1080/17530350.2019.1589553

Shao, S., & Bo, H. (2021). Behavioural aspects of China's P2P lending. *The European Journal of Finance*, *28*(1), 30–45. https://doi.org/10.1080/1351847X.2021.1880459

Shen, X. (2023, August 23). Crypto-mining Chinese official given life in prison for scheme involving bribes and support for a cryptocurrency firm. *South Morning China Post*. https://www.scmp.com/tech/policy/article/3232044/crypto-mining-chinese-official-given-life-prison-scheme-involving-bribes-and-support-cryptocurrency

Simonite, T. (2019, September 3). Behind the rise of China's facial-recognition giants. *Wired*. https://www.wired.com/story/behind-rise-chinas-facial-recognition-giants

Southwest University of Political Science and Law. (2025). Ju Jiao Qian Yan! She Xu Ni Huo Bi Fan Zui De Zhen Cha, Qi Su He Gu Ding Zheng Ju Gu Ding Yan Tao Hui Zai Xi Zheng Ju Ban. https://news.swupl.edu.cn/zhxw/f2d9b9d167e84e7eafd1819ce5c28cdd.htm

Star, S. L., & Ruhleder, K. (1996). Steps toward an ecology of infrastructure: Design and access for large information spaces. *Information Systems Research*, *7*(1), 111–134. https://doi.org/10.1287/isre.7.1.111

Steer, G. (2025, June 14). Donald Trump discloses $57mn earnings from crypto venture. *Financial Times*. https://www.ft.com/content/1508d831-60bb-4287-9c76-da7d730cf584

Szonyi, M. (2017). *The art of being governed*. Princeton University Press.

Tang, Z., Lahiri, T., & Huang, E. (2022, July 21). How peer-to-peer lending turned middle-class Chinese dreamers into angry protesters. *Quartz*. https://qz.com/1351198/how-p2p-lending-turned-middle-class-chinese-dreamers-into-angry-protesters

TechFlow. (2023, April 4). Shen Ru Qu Zhong Xin Hua Mei Ti: Qu Kuai Lian Ji Shu Yu Di Si Chan Ye De Guo Qu, Xian Zai He Wei Lai. https://www.techflowpost.com/article/detail_11650.html

The State Council of the People's Republic of China. (2015, December 31). *Premier Li and Internet Plus*. https://english.www.gov.cn/policies/infographics/2015/12/31/content_281475263938767.htm

U.S. Securities and Exchange Commission. (2023, March 22). *SEC charges crypto entrepreneur Justin Sun and his companies for fraud and other securities law violations* [Press release]. https://www.sec.gov/newsroom/press-releases/2023-59

Webster, G., Creemers, R., Kania, E., & Triolo, P. (2017, August 1). *Full translation: China's 'New Generation Artificial Intelligence Development Plan.'* DigiChina. https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017

Wong, J., & Wong, J. I. (2017, July 21). The world's oldest bitcoin exchange is shutting down in China. *Quartz*. https://qz.com/1077545/bitcoin-btc-price-is-down-because-btcc-is-closing-its-china-exchange

Xiao, T. (2024, September 3). Exploring China's leading AI hubs: A regional analysis. *China Briefing*. https://www.china-briefing.com/news/exploring-chinas-leading-ai-hubs-a-regional-analysis/#:~:text=Leading%20the%20charge%20in%20AI,lead%20in%20AI%20industry%20development

Xinhua News. (2018, December 24). Nian Zhong Pan Dian: Zhe Yi Nian, Ren Gong Zhi Neng Zai Zheng Yi Zhong Qian Xing http://www.xinhuanet.com/politics/2018-12/24/c_1123892918.htm

Xu Elegant, N. (2019, December 16). China's big blockchain bet aims for an early advantage over the U.S. *Fortune*. https://fortune.com/2019/12/16/china-blockchain-tech-us-war

Yang, Z. (2025a, January 31). Here's how DeepSeek censorship actually works—and how to get around it. *Wired*. https://www.wired.com/story/deepseek-censorship

Yang, Z. (2025b, March 12). Chinese companies rush to put DeepSeek in everything. *Wired*. https://www.wired.com/story/deepseek-china-nationalism

Yang, Y., & Liu, X. (2018, August 6). Police lock down Beijing's financial district to thwart protests. *Financial Times*. https://www.ft.com/content/58728458-9943-11e8-9702-5946bae86e6d

Zhai, K., & Chen, L. Y. (2018, April 24). Chinese #MeToo student activists use blockchain to fight censors. *Bloomberg*. https://www.bloomberg.com/news/articles/2018-04-24/chinese-metoo-student-activists-use-blockchain-to-fight-censors?embedded-checkout=true

Zhou Xiao Chuan Wei P2P Dian Zan. (2015, October 12). *China Daily*. https://finance.chinadaily.com.cn/2015-10/12/content_22163475.htm

Zhuang, R. (2019). *Qu Kuai Lian Xin Xi Fu Wu Guan Li Gui Ding*. https://www.cac.gov.cn/2019-01/10/c_1123971164.htm

## About the Author

Zichen Hu is a PhD researcher in the Department of Media and Communications at London School of Economics and Political Science (LSE). She also works as a research associate for Oxford Global Society and Digital Futures for Children. Her research focuses on how emerging digital platforms selectively mobilize Web3 and AI technologies, creating governance challenges that are deeply situated in the power relations between state and non-state actors, and the consequences of these entanglements for a transnational ecosystem, where disinformation is both mobilized as a strategic resource and used to catalyze social and political mobilization.

Politics and Governance
2025 • Volume 13 • Article 10234
https://doi.org/10.17645/pag.10234

cogitatio

ARTICLE

Open Access Journal

# Data Flows Meet Great Power Politics: The Emerging Digital Security Dilemma Between China and the US

Ziyuan Wang

Institute of International Relations, China Foreign Affairs University, China

**Correspondence:** Ziyuan Wang (wangziyuan@cfau.edu.cn)

**Submitted:** 28 February 2025 **Accepted:** 25 August 2025 **Published:** 5 November 2025

**Issue:** This article is part of the issue "Technology and Governance in the Age of Web 3.0" edited by Chang Zhang (Communication University of China), Zichen Hu (London School of Economics and Political Science), and Denis Galligan (University of Oxford), fully open access at https://doi.org/10.17645/pag.i443

## Abstract

This article employs security dilemma theory to probe the geopolitical implications of state intervention in the digital realm. Its central argument is that with cross-border data flows being conducive to subversive actions, governments have grown wary of rival states leveraging control over data flows to advance strategic objectives. Therefore, when a government tightens its domestic regulation over data flows, its actions could trigger a spiral of suspicions and countermeasures with other states. Such a security dilemma fosters the technology rivalry between China and the United States. As Beijing became sensitive to unrestricted flows of information and data, it set out to exert tighter control over data flows within and across Chinese borders. But Beijing's move aggravated US perceptions of subversive threats, prompting Washington to try to drive Chinese entities out of the US-centric technology ecosystem. Washington's actions signaled hostile intent to China, which in turn decided to build alternative digital infrastructures. Given that state intervention in the digital realm could exacerbate great power rivalry, Web 3.0 will likely perpetuate security dilemma dynamics by shifting the battlefield from corporate platforms to protocol layers, from data ownership to infrastructure sovereignty.

## Keywords

data flows; digital infrastructure; security dilemmas; subversion; US–China relations

## 1. Introduction

Web 3.0 technologies such as blockchain and generative artificial intelligence sharply increase the importance of data for socioeconomic life. Widely expanding the use of data in productive and commercial fields, those technologies not only boost market efficiency but also enable commercial actors to evade government scrutiny. In turn, governments are devising policies to regulate unrestricted data flows. China,

for its part, went beyond regulating market-oriented blockchain applications. It made massive state-led investments in blockchain technology as part of its broader ambition to build a sovereign digital ecosystem. This project was designed to lessen China's dependence on Western digital infrastructures and deepen its ties with the Global South (Kumar, 2025). Beijing's digital strategy has aroused Washington's concerns. The White House's *National Cybersecurity Strategy* claims the following:

> The People's Republic of China now presents the broadest, most active, and most persistent threat to both [US] government and private sector networks….Having successfully harnessed the Internet as the backbone of its surveillance state and influence capabilities, the PRC is exporting its vision of digital authoritarianism, striving to shape the global Internet in its image and imperiling human rights beyond its borders (White House, 2023).

Ostensibly, Beijing's perceived success in harnessing blockchain would be instrumental in extending its geopolitical reach and reshaping norms in the digital realm. But whether this scenario materializes depends not only on China's digital policy but also on the US approach to Chinese challenges. Notably, the Obama administration did not endeavor to limit China's access to international markets for digital technologies after it realized the expansion of China's surveillance apparatus. In contrast, officials of the Trump and Biden administrations frequently pointed to China's surveillance system as a threat to American interests. This dramatic policy shift invites the following questions: Why did the US become sensitive to the evolution of China's digital development? Is Beijing's digital strategy driven by an impulse to compete with the US for technological supremacy? And what are the implications of data flows for US–China relations?

Security dilemma theory offers an important perspective. From it, some analysts suggest that because China is deeply integrated into global networks, its domestic practice could generate considerable security externalities. As a result, even the policy measures China undertook to enhance its domestic security could pose a threat to countries embedded in global supply chains (Pearson et al., 2022). Still, China's initial motives in strengthening its regulation of data flows and the concomitant security risks to the US are underexplored. Specifically, it is unclear why Chinese leaders adopted a heavy-handed regulatory approach to their own digital economy, which risked jeopardizing market stability in China as a crucial source of regime legitimacy. On the other hand, since the US was and still is a dominant player in the global flows of data, why it became concerned over China's digital policy is worth investigating.

In response, this article focuses on the subversive threats of data flows as a crucial source of security dilemmas among states (Section 2). Sections 3–5 illustrate this argument through a case study of the rise of the US–China technology rivalry. Section 3 discusses how the Snowden revelations, cyberattacks, and Russian interference in the 2016 US election heightened awareness in Washington of the subversive potential of data flows. Section 4 explores how concerns about subversion shaped Chinese regulation of data flows. Section 5 shows how the two sides' security-enhancing measures produced a spiral of tensions by fostering mutual perceptions of hostile intent. Section 6 contrasts my account with the zero-sum competition model and underscores the former's explanatory leverage. The article concludes by considering the implications of Web 3.0 for digital security dilemmas.

## 2. Security Dilemmas in the Digital Realm

The security dilemma is a central dynamic in international politics. Whereas states must strive to enhance their security in the anarchic international system, measures undertaken by states to bolster their self-defense can still inspire reciprocal fears and fuel interstate rivalry accordingly (Jervis, 1978). Nevertheless, security dilemma theory posits that international conflict is not inevitable but occurs or escalates in situations wherein state actors lack confidence in the prospects for cooperation (Glaser, 1997). Offense dominance and perceptions of hostile intent may create such situations. Offense dominance means the acquisition of territory and strategic resources is relatively easy. It is, in general, characterized by large offensive opportunities or defensive vulnerabilities (Evera, 2001, pp. 160–166). In such circumstances, offensive actions can yield considerable benefits; accordingly, state actors may perceive each other as prone to aggression. Such perceptions, moreover, can be bolstered by the human cognitive tendency to see threatening behavior as intentional (D. Johnson, 2020, pp. 118–120). Once convinced of each other's hostile intent, state actors may feel compelled to adopt hardline policies and hence find themselves in a spiral of tensions.

The digital realm can foster offense dominance by lowering the barriers to subversive actions. By definition, subversion refers to "targeted, hostile action within another state to weaken it or cause it to alter its policy" (Kastner & Wohlforth, 2025, p. 1). This is a distinct form of offense. Unlike diplomatic and military activities, subversion operates inside the territory of other states. Subversion also goes beyond espionage in its intended effects—namely, reshaping the domestic political dynamics of target states. Extensive espionage, though, may arouse fears of subversion by revealing the capacity of a rival state to carry out unlawful operations abroad.

Data flows tend to facilitate subversion. Through online propaganda, co-option, and cyberattacks, foreign governments could exploit data flows to undermine or manipulate the domestic institutions of target states. Alarmingly, the same data that allow companies to tailor products to user preferences may also be weaponized to mobilize societal groups against a state's domestic order. Likewise, foreign adversaries may engage in cyber espionage to access private data and identify vulnerable individuals in the target country's government institutions. The adversaries then would manipulate financial and career incentives to co-opt those individuals to undertake activities contrary to that country's interests. Finally, data flows enable hackers to exploit systems' vulnerabilities. Hackers do not traverse land, sea, or air to mount an attack; rather, they can infiltrate target systems through technical backdoors or by altering data. Cyberattacks thereby play a crucial role in the theft of valuable data and the erosion of public trust in the domestic institutions of target countries (Maschmeyer, 2023).

The offensive opportunities in the digital realm—such as online propaganda, co-option, and cyberattacks—correspond to the defensive vulnerabilities of target systems. Because the internet is an open and virtual space, it is easy for threat actors to conceal their identities as they undertake subversive actions. Further, the layered design of digital infrastructures inevitably contains critical flaws ripe for exploitation. As digital systems become increasingly interdependent, every driver, cloud service, and Application Programming Interface used by customers is a potential vector of attack. Although the strategic implications of cyber intrusions and algorithm manipulations are debatable (Gartzke & Lindsay, 2015), the capacity of adversaries to infiltrate critical infrastructures and institutions undetected is sufficiently worrisome to national security decision-makers. Crucially, subversive actions violate sovereignty as the basis of state survival.

Inasmuch as cyber intrusions can erode public trust in domestic institutions, they are a legitimate national security concern.

Since subversive threats foster offense dominance in the digital realm, governments' exertion of direct control over data flows can aggravate fear and competition among states. For example, if state A tries to enhance administrative oversight over commercial actors operating under its jurisdiction, such measures could lead other states to worry that it will obtain valuable data. In response, state B will try to curtail its market ties with state A, but such a move may signal hostile intent and fuel A's pessimism about its international environment (Copeland, 2016). This pattern of interactions would encourage technology rivalry, as state actors harbor security concerns regarding their interconnections in the digital realm.

The rise of the technology rivalry between China and the US provides a crucial case to examine the argument laid out above. Given that the US and China are now engaged in a systemic competition for global leadership, it is tempting to see their technology rivalry as an extension of the ongoing bipolar struggle. However, if the evidence presented in the case study convincingly challenges this assumption, it will boost the plausibility of my argument derived from security dilemma theory.

## 3. Internet Openness, Subversive Threats, and US National Security

The internet is a public domain. Its openness enables frequent and rapid data flows across disparate systems and devices. Over decades, a few tech giants have become dominant over data resources by acting as key nodes in data flows. This structural reality enabled the US government to exploit the internet for intelligence advantages. Through the tech companies and related digital infrastructures operating under its jurisdiction, the US government could access users' data and track their activities. After 9/11, for instance, the US government demanded that the Society for Worldwide Interbank Financial Telecommunication share data to help it track terrorist financing (Farrell & Newman, 2019, p. 61).

The US's exploitation of global digital infrastructures for espionage became widely known after the Snowden files exposed the US National Security Agency's collection of vast amounts of private data of American and foreign citizens. In the shadow of the Snowden revelations, Washington was hard-pressed to reassure the public. Although the US government subsequently enacted new legislation and regulations to oversee federal data usage, public distrust made American tech companies less willing to cooperate with the government (Sanger, 2018, pp. 85–99). The growing rift between the US government and tech firms made it more challenging to defend against cyberattacks, rendering the US vulnerable to digital subversion. In 2014–2015, the US Office of Personnel Management suffered a series of cyberattacks, leading to the leak of personal data of millions of federal employees. According to the Committee on Oversight and Government Reform under the House of Representatives, this leak exposed a vast number of US government officials to foreign influence operations, including blackmail and family threats. The Committee in turn emphasized that the US "has never been more vulnerable to cyberattacks" (Committee on Oversight and Government Reform, 2016, p. v).

The 2016 election interference by Russia raised widespread anxiety in the US about the threats of subversion of its democratic institutions. During the campaign period, Russia's government agencies and related organizations spread disinformation, stole and leaked email information associated with the Hillary

campaign, and created myriad false accounts to spread anti-democracy narratives (Kastner & Wohlforth, 2025, pp. 151–167; Sanger, 2018, pp. 201–235). In the aftermath of the presidential election, the bipartisan committee led by Robert Mueller ascertained the fact that Russia's intelligence agency managed to exfiltrate a massive amount of data from the computer networks of the Democratic National Committee, an operation that enabled Moscow to disrupt the 2016 US election (Mueller, 2019, pp. 94–107). Although it is not clear whether such operations were decisive in altering the election outcome, they surely disrupted the democratic process and sowed chaos in the US.

The events described above highlight how data exfiltration has increased subversive threats. Because of its centrality to digital networks, the US fell victim to such threats even though Washington also managed to exploit internet openness for strategic and intelligence advantages. China's domestic regulatory measures were motivated by similar fears of subversion, as it has long been concerned with ideological influence from abroad.

## 4. China's Sensitivity to Subversive Threats

Since the end of the Cold War, fears about subversion have been deeply rooted in Beijing's preoccupation with "political security" (*zhengzhi anquan*). In the official discourse, political security means "national sovereignty, government power, political systems, political order, and ideologies are protected from threats, infringements, subversion, and destruction" (Yang, 2018). This concept is identical to regime security. Chinese concerns for regime security stemmed from anxiety over the perceived US strategy of "peaceful evolution" (Zhang, 2023). In the post-Cold War years, Beijing's security anxiety was deepened by the fact that liberal ideology served as the normative foundation for US hegemony. Hu Jintao, the General Secretary of the Communist Party of China (2002–2012), stated that "the struggle in the international ideological and cultural sphere remains profound and complex" (Hu, 2006, p. 1). In 2008–2012, a series of ideological disputes between China and the West, combined with the Jasmine Revolution in North Africa and the Middle East, led China to introduce a surveillance system known as the Great Firewall, which enabled the regime to track and filter the data flowing across its borders.

Subsequently, the Snowden revelations drove home the urgency of strengthening regulatory measures, as they confirmed that Washington had been exploiting global data flows for strategic purposes. Snowden thus aggravated Chinese perceptions of subversive threats from a weaponized internet. According to the Cyberspace Administration of China, the Snowden incident sounded the alarm around the world to the effect that "without cybersecurity, there is no national security" ("Xuezhe jiedu," 2014; also see Pearson et al., 2022, p. 146).

Consequently, Chinese leaders decided to exercise direct control over data flows across and within Chinese borders. In February 2014, China announced the establishment of the Central Leading Group for Cybersecurity and Informatization, unifying the functions of various network management departments under the State Council and the Propaganda Department of the Chinese Communist Party. Under this central authority, China undertook to curtail foreign access to Chinese data. In 2015, the State Council issued guiding suggestions and action plans regarding the use of data in the market, enhancing government oversight of enterprise data. Article 25 of the 2015 National Security Law emphasizes that "maintaining cyberspace sovereignty, security, and development interests" is a major task of national security (People's

Central Government, 2015). Article 37 of the Cybersecurity Law further clarified that operators of critical information infrastructure must store personal information and important data within the country and that domestic commercial entities must have government approval before they transfer data abroad (Cyberspace Administration of China, 2016). Didi, China's largest ride-hailing company, was punished by this law, which forced it to delist from the New York Stock Exchange in 2021. The localization of data storage thus became a central feature of Chinese governance of the digital realm.

Establishing stringent oversight over tech companies has also better positioned the Chinese government to censor societal information. Early in 2016, the Chinese government began to pursue "special management shares," which would allow government agencies to participate in major decision-making of private companies through small shareholding. Specifically, the State Administration of Press, Publication, Radio, Film, and Television suggested that state-owned special management shares account for at least 1% of a company's shares, an arrangement that would give government agencies board seats and the right to review media content (Jin, 2016). By 2021, ByteDance, TikTok's parent company, had accepted the special-management-shares arrangement (De Mott, 2023). Tencent—the parent company of WeChat (arguably the most popular messaging app in China)—appears not to have done so, but it is widely known that its headquarters in Shenzhen city "has at least one floor exclusively reserved for internet inspectors composed of state security police, national security staff, and online censors" (Walker, 2021). These regulatory measures have given China's government privileged access to data, allowing it to monitor the society, deter potential challengers, and shape the domestic information environment more effectively.

## 5. The Spiral of Suspicions and Decoupling Between the US and China

This article suggests that security dilemma dynamics in the digital realm contribute to the US–China technology rivalry. Thanks to internet openness, data flows become central to socioeconomic development; accordingly, data flows assume strategic importance in enabling threat actors to subvert the domestic institutions of nations connected to the internet. Policymakers in Beijing and Washington thus became concerned about subversive threats. As a result, although China's strengthening of regulation over its tech companies was driven by the defensive motives of safeguarding regime security, Washington has come to consider China's domestic policy a subversive threat and undertake assertive actions in response.

### *5.1. The Trump Administration's Concerns for Chinese Subversion*

As Donald Trump's first administration was poised to escalate trade conflict with China, economic security became a top priority for US officials. This policy stance helped intensify Washington's scrutiny of Beijing's data regulation practice and the US's domestic vulnerabilities. The White House noted that "China gathers and exploits data on an unrivaled scale and spreads features of its authoritarian system" (Trump, 2017, p. 25). In early October 2018, Vice President Mike Pence delivered a landmark speech outlining a shift in US policy, wherein he characterized China as an "unprecedented surveillance state." Pence then suggested that China's attempted control over data flows signaled its revisionist ambition. As he put it, "a country that oppresses its own people rarely stops there. And Beijing also aims to extend its reach across the wider world" (Pence, 2018).

Pence's speech was indeed motivated by the cabinet's decision to counter China's subversive behavior. When Trump's national security team gathered to prepare that speech, they were preoccupied with Chinese attempts

to influence the 2018 Congressional elections. According to John Bolton, then National Security Advisor, Trump's officials believed that "China could bring considerably greater resources to bear on this effort [election meddling] than Russia" (Bolton, 2024, p. 262). In their view, China had both the capability and intention to subvert the US political institutions. To deprive Beijing of subversive means, Washington undertook to curtail America's commercial and societal ties with China.

### *5.2. US Decoupling Measures Against China*

Just a month after Pence's speech, the US Department of Justice launched the China Initiative, a program designed to prosecute cases related to Chinese economic espionage and data security threats (US Department of Justice, 2021). Toward the end of the first Trump administration, this program had publicized nearly 60 significant cases (US Department of Justice, 2021), with FBI Director Christopher Wray claiming that 2,000 cases related to China had been under investigation (Lucas, 2022). While the China Initiative was primarily directed against economic espionage activities, it showed the tendency of US leaders to assume the worst about Chinese intentions in collecting data. This very perception of threat led the US to decouple its technology ecosystem from China.

The US-led sanctions against Huawei and the Clean Network program are notable examples in this regard. Both policy actions were designed to curtail the access of Chinese data service providers to the markets of the US and its allies. Initially, the US government accused Huawei of providing technical support to Iran through fraudulent means. Based on this charge, the US demanded that Canadian authorities arrest and extradite Huawei Chief Financial Officer Meng Wanzhou. Shortly thereafter, the US government imposed comprehensive sanctions on Huawei. In May 2019, the US Department of Commerce designated Huawei to the Entity List subject to specific license requirements for certain transactions, which significantly restricted Huawei's business dealings with American companies. Secretary of State Mike Pompeo justified this move by claiming that "if the Chinese Communist Party wants to obtain information through the Huawei technology, Huawei will certainly give it to them" (Segal, 2021, p. 157). Arguably, Huawei's perceived association with the Chinese government aroused concerns in Washington that Beijing could use this company as a vehicle for subversion. According to the US Department of Commerce, Huawei posed a threat to US national interests due to its perceived ties to the Chinese military, its involvement in stealing trade secrets from US companies, and its ability to covertly access mobile phone networks around the world through "back doors" (Fitzgerald, n.d.). The last charge underscored Washington's misgivings over China weaponizing data for subversive actions.

The Clean Network initiative signified a crucial move by the Trump administration toward technology decoupling. Initially, the Department of State committed to provide a "clean pathway" for all 5G traffic passing through US diplomatic facilities. Several countries, including Japan, Australia, the Czech Republic, Norway, and Israel, joined the US in the 5G Clean Path initiative. Traditional allies including the UK, France, and Canada also announced that they would exclude Huawei from their 5G suppliers. Building on this practice, the Department of State officially launched the Clean Network initiative in August 2020, a program committed to establishing international trust standards for digital infrastructure (US Department of State, n.d.). Targeting Chinese network carriers, app downloads, mobile apps, cloud storage, and undersea cables, this initiative aimed to prevent Chinese-related commercial entities from accessing US citizens' information through digital infrastructures (Pompeo, 2020). The Council on Foreign Relations compared the Clean

Network program to the Long Telegram of the 21st century (Fidler, 2020). It suggested that the US had set out to hinder China from using data flows to undermine democratic institutions—just as after WWII the US became wary of the Soviet Union's subversion against European countries.

Meanwhile, the first Trump administration issued executive orders to prohibit transactions with the parent companies of two popular Chinese apps (WeChat and TikTok). The orders highlighted the potential for the Chinese government to access personal data of American citizens, which could be used to facilitate subversive actions. As TikTok was on its way to becoming the most popular entertainment platform in American society, the Trump administration claimed that data collection via this platform "threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information—potentially allowing China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage" (Trump, 2020). Trump also pointed to the censorship practice of TikTok regarding information related to China's crackdowns on Hong Kong protests and extensive human rights violations in Xinjiang. Hence, his administration was concerned that TikTok might be "used for disinformation campaigns that benefit the Chinese Communist Party" (Trump, 2020).

Joseph Biden's administration inherited Trump's concerns for subversive threats in the digital realm, but modified Trump's approach to national security. Whereas Trump tried to confront China with unilateral sanctions, the Biden administration sought to build a technology ecosystem among US allies by tightening restrictions on critical technology transfers to China. In an elaboration on Biden's technology strategy, National Security Advisor Jack Sullivan vowed that the US must lead the revolution in digital technology, promote American values (notably privacy rights and intellectual property), and work with its allies and partner countries to promote competitiveness and prosperity (Sullivan, 2021). Under this policy, the Biden administration established the Critical and Emerging Technology Working Group with Japan, South Korea, Australia, and India, four regional powers with technological potentials to compete with China. With its Asian and European allies, the Biden administration also created a series of mechanisms for coordination on a series of economic security measures, such as developing common standards for emerging technologies, implementing export controls, and enhancing supply chain resilience and cybersecurity (White House, 2023, p. 30). Washington's actions aggravated Chinese perceptions of hostility. President Xi openly stated that "Western countries led by the United States have carried out all-around containment, blockade, and suppression against us, which presents unprecedentedly severe challenges to our development" (State Council of China, 2023). By that time, China's leadership had adopted new macroeconomic policies designed to reduce its reliance on the American market. Then Vice-Premier Liu He interpreted China's policy approach as a necessary response to de-globalization and the restructuring of industrial and supply chains (Liu, 2020).

### *5.3. China's Quest for Alternative Digital Infrastructures*

As China was braced for a long-term struggle with the US, it sought to develop a technology ecosystem independent of the US-centered digital infrastructure. Blockchain technology served this end. Back in 2016, China began to incorporate blockchain technology into its grand plan for national development. The 13th Five-Year National Informatization Plan initiated an industrial policy aimed at developing "revolutionary technologies" (*dianfuxing jishu*; People's Central Government, 2016). Consequently, blockchain came to figure prominently in China's development strategy. In late 2019, against the backdrop of escalating tensions in US–China relations, Xi convened a politburo meeting to focus on blockchain as a

national strategic priority. On that occasion, he stressed the need to "accelerate the deep integration of blockchain with cutting-edge information technologies such as artificial intelligence, big data, and the Internet of Things," because blockchain could help achieve a "breakthrough in driving independent innovation of core technologies" ("Xi Jinping zai," 2019).

Notably, China unequivocally rejected the decentralization principle of blockchain technology. The Chinese authorities went out of their way to limit the use of cryptocurrencies in the domestic market, culminating in a comprehensive ban on all cryptocurrency transactions in 2021 ("China declares all crypto-currency," 2021). Consistent with its stringent regulatory policy over private digital platforms, Beijing endeavored to prevent commercial actors from accessing blockchain. Still, it wanted to harness this technology to strengthen its control over digital infrastructures. Around 2020, the Chinese government stepped up efforts to promote the digital version of its currency (known as e-CNY). While the central ledger of e-CNY is under the control of Chinese authorities, the tamper-resistance of blockchain offers a technical guarantee that Beijing cannot secretly alter the ledger. This lends credibility to e-CNY among international banks. Thus, blockchain technology enables state-led digital payment systems, which helps reduce China's reliance on Western-dominated financial infrastructures.

Building on this initiative, China elevated cooperation with Russia. The Sino-Russian digital collaboration made significant progress in the wake of China's diplomatic fallout with the Biden administration in Alaska. In March 2021, Chinese Foreign Minister Wang Yi met with his Russian counterpart Sergei Lavrov, who called for a shift "away from using international payment systems controlled by the West" (Tétrault-Farber & Osborn, 2021). In turn, Wang Yi proposed that China and Russia work together to "bolster the security of each other's regime and institution" ("Wang Yi tong," 2021). The Chinese and Russians thus found a common interest in the joint development of digital infrastructures, which served to resist Western geopolitical and ideological pressures. By the end of 2021, the two governments had agreed to "give full play to the role of infrastructure organizations and financial institutions of both countries, including the RMB clearing bank in Russia" (Ministry of Foreign Affairs of the People's Republic of China, 2021). This initiative gained traction after the outbreak of the Russia–Ukraine War. By mid-2025, major Russian banks had introduced a netting payments system dubbed the China Track, which could help Russia circumvent the sanctions imposed by the US and the European Union ("Exclusive," 2025).

In sum, with both Washington and Beijing fearing subversion through data flows, each explored paths toward digital decoupling. This process soon became self-reinforcing. In Washington, concerns over digital subversion prompted policy measures designed to curtail market ties. The US sanctions on Chinese firms spurred Beijing to build alternative digital infrastructures aimed at the creation of an autonomous technology ecosystem, as China's leaders interpreted Washington's actions as evidence of hostile intent. In this context, China has tried to harness Web 3.0 technologies such as blockchain to enhance its autonomy within global infrastructure networks. What is clear is that regime security concerns have propelled Beijing to elevate blockchain technology to a national strategic priority.

## 6. A Contest for Technological Supremacy? Evaluating an Alternative Argument

This article suggests that when American and Chinese leaders became sensitive to subversive threats in the digital realm, they adopted policies that fueled a spiral of mutual suspicions and led to technology decoupling

and rivalry. Grounded in security dilemma theory, this argument stands in contrast with the model of zero-sum competition espoused by several leading experts on US–China relations. In their view, China has been pursuing a grand strategy of displacing the US from its hegemonic position (Doshi, 2023; Friedberg, 2011; Mastro, 2024). As a corollary, the emerging technology rivalry is merely an extension of the broader competition for global power between a rising China and the US, the established hegemon.

The zero-sum competition model, however, falls short in two respects. First, it overlooks the defensive motives of Beijing in formulating its digital policies. Certainly, China's approach to data reflected Xi Jinping's personal vision for national development, which was premised on the idea that the Chinese practice of Marxist ideology would prove its superiority vis-à-vis Western liberalism (Shirk, 2023, p. 184). But this does not mean Xi would necessarily pursue an offensive strategy. Quite the contrary, Xi's policies were in large part defensive, as they highlighted the need to safeguard China's domestic regime. Since 2014, Xi has envisioned China becoming an "Internet strong country" (*wangluo qiangguo*), while emphasizing that "if we can't pass the test of the Internet, we can't pass the test of holding [domestic] power for a long term" (Cyberspace Administration of China, 2024). Internationally, China has sought to justify its defensive approach to data security by promoting "cyber sovereignty" (*wangluo zhuquan*). This concept was officially proposed by Xi at the 2015 World Internet Conference, where he claimed that "cyber surveillance, cyber espionage, and cyber terrorism have become global public hazards" ("Xi Jinping," 2015). Cyber sovereignty was, therefore, designed to address the "global public hazards" posed by the US's exploitation of the internet. According to Xi, the norm of cyber sovereignty meant "respecting the rights of each country to independently choose its internet development path [and] internet management model" (Xi, 2015). Because this norm upheld the state's role in the management of cybersecurity, it served to shield China from hostile ideologies from abroad.

Apparently, the norm of cyber sovereignty is contrary to the internet freedom promoted by the US. But it is worth noting here that the norm of cyber sovereignty does not prescribe any concrete path of technological development for other countries. While China has been intent on localizing data storage and limiting data flows across its borders, this practice would hinder China from shaping global norms for data flows. China expert Matthew Johnson notes that "the Party's strategy for data accumulation through multilateral trade agreements is intentionally offset by domestic laws making the vast majority of China's data a protected resource" (Johnson, 2023, p. 33). If foreign governments embrace this model of cyber sovereignty, they will have to accept asymmetric access to data flows, and it is doubtful that they are willing to do so. However, since the norm of cyber sovereignty does not specify the terms for an alternative internet order, it could legitimize the heterogeneous strategies that various authoritarian regimes may adopt to safeguard their domestic political order. Along with those regimes, China will likely use cyber sovereignty as window dressing for its continued exploitation of the open internet for access to data that could yield economic and intelligence advantages (Lindsay, 2015).

Put simply, the zero-sum competition model tends to overstate China's ambitions in the digital realm. There is no denying that China's privileged access to data would enable its technological innovation. Xi compared data to "the oil of the 21st century," asserting that "whoever masters big data technology will hold the resources and maintain the initiative for development" ("Laolao bawo," 2016). However, the use of data is non-rivalrous—one's use does not diminish others' use; rather Xi's remark may well reflect his sensitivity to regime survival. Indeed, authoritarian regimes have long grappled with the dilemma of maintaining social

control and fostering a dynamic economy. Digital technologies offer a way out. By enabling the micro-targeting of individual behaviors, digital technologies promise to lower the costs of surveillance and boost market efficiency (Wright, 2018). For that matter, Xi mobilized the country to "leverage big data to enhance the modernization of national governance" ("Xi Jinping," 2017). Furthermore, when the Central Leading Group for Cybersecurity and Informatization was elevated to the status of full commission in 2018, Xi took the occasion to provide comprehensive guidance on China's cyber sector with a focus on regime security. In his words, "it is necessary to enhance the overall governance capability of cyberspace…[and] to consolidate the ideological foundation for the unity and struggle of the entire Party and the Chinese people" (People's Central Government, 2018).

In contrast to the model of zero-sum competition, security dilemma theory underscores the defensive motives of China in promoting the norm of cyber sovereignty and developing digital infrastructures—namely, Beijing's anxiety for regime security. This raises a second issue: Why did China's domestic regulatory policy arouse security anxiety on the US part? Security dilemma theory answers this question by underscoring US fears of subversion. That is, it was not until US leaders became sensitive to subversive threats in the digital realm that they became determined to restrict the access of Chinese entities to the American market.

While differences over internet governance had emerged during the Obama years as an outstanding dispute, that did not derail US–China technology relations. In 2010 when Google declared its withdrawal from Mainland China, then Secretary of State Hillary Clinton stressed the need for dialogue and communication in promoting China's internet openness (Clinton, 2010). Even an escalation of cyber disputes did not lead to the technology rivalry between the two countries. In the aftermath of the Snowden revelations, US leaders felt compelled to reaffirm their commitment to data security. They in turn tried to distinguish between cyber espionage for commercial gain and cyber operations conducted for national security purposes (Lindsay, 2015, p. 26). To vindicate this point, the Obama administration in May 2014 indicted five Chinese officers linked to the People's Liberation Army for stealing commercial sector data. Counterintuitively, this move helped elicit Beijing's cooperation, as Chinese leaders put a premium on maintaining stable relations with Washington (Sanger, 2018, pp. 121–123). In September 2015, the US and China reached a bilateral agreement on cyber behavior during the state visit by President Xi. The agreement led to serious bilateral negotiations about cyber norms and a sharp decline of Chinese cyberattacks (Hvistendahl, 2016). This outcome is contrary to the zero-sum competition model that considers a US–China technology rivalry inevitable.

Although the dispute over cyber norms signified US–China antagonism in the digital realm, it was not sufficient to bring about technology rivalry, as neither Washington nor Beijing pursued a policy of technology decoupling during the Obama years. The turning point instead occurred in the aftermath of Russian interference in the US election of 2016. Prior to that, the US had been solely focused on China's cyber espionage. In the shadow of Russian interference, however, the Trump administration began to move beyond this focus and frame China's cyber threats in terms of subversion. It noted in particular that China was "improving its cyber attack capabilities and altering information online, shaping Chinese views and potentially the views of US citizens" (Coats, 2019, p. 5). Linking this issue with "online influence operations" and "election interference," Trump's officials considered China a major source of subversive threats alongside Russia (Coats, 2019, p. 5). Similarly, during the Biden years, the US intelligence community stated that "Beijing's growing efforts to actively exploit perceived US societal divisions using its online personas move it

closer to Moscow's playbook for influence operations" (Office of the Director of National Intelligence, 2023, p. 10). It was in this context that Washington resolved to restrict the access of Chinese entities to the American market. Sensitivity to subversive threats thereby intensified security dilemma dynamics between China and the US.

## 7. Conclusion

In the digital realm, security dilemma theory suggests that the defensive measures undertaken by a state to govern its domestic digital environment could pose subversive threats to other states, which would in turn pursue technology decoupling. However, decoupling measures could signal malign intent and help escalate interstate tensions into technology rivalry. Security dilemma theory helps explain the emerging technology rivalry between the US and China. As Beijing became alert to unrestricted flows of information and data, it pursued stringent control over tech companies in charge of managing cross-border data flows. This measure was largely defensive in that it was primarily designed to fend off subversion by Western liberal ideology. Still, China's regulatory policies aggravated American perceptions of subversive threats, prompting Washington to limit the access of Chinese entities to its market. For China, Washington's actions likewise signaled hostile intent; thus, Beijing decided to undertake preventive measures to develop separate digital infrastructures. Hence, a digital security dilemma has emerged between the US and China, wherein efforts by one side to tighten regulatory control over data flows are perceived as threatening by the other.

Investigating the causal dynamics behind the US–China technology rivalry is crucial to understanding the geopolitical risk of Web 3.0. China's active use of blockchain technology could shift the arena of contestation to more foundational layers of the internet—the protocol layers that underpin decentralized systems. Unlike the earlier era dominated by corporate digital platforms, the new competition will likely be focused on infrastructure sovereignty—that is, who controls the rules, protocols, and standards that structure digital interactions on a global scale. In turn, governments would seek to protect their technology ecosystems, develop indigenous digital infrastructures, and align protocols with state interests. As demonstrated, this trend had its origins in great powers' fears of subversion via data flows. Web 3.0 technologies seem to help mitigate such fears by enhancing infrastructure resilience. However, when governments manage to develop their own digital infrastructures using Web 3.0 technologies, their direct involvement in digital governance and infrastructure-building could signal competitive intentions and exacerbate international perceptions of threat. As security dilemma theory suggests, even if state intervention in the digital realm is initially intended as a defensive regulatory act, that could still intensify the dynamics of great power rivalry.

## Acknowledgments

I would like to thank Coh Chong Chen and Xue Gong for inviting me to present this article at the 2025 workshop "Economic Statecraft in U.S.–China Tech Competition" held by the S. Rajaratnam School of International Studies at Nanyang Technological University. I am especially indebted to Miles Evers and Kai He for their invaluable feedback. Thanks also go to Tianjiao Jiang, Nan Yang, and Yue Yuan for their professional advice that encouraged me to explore cybersecurity as an emerging topic in international security studies. Needless to say, I am accountable for all errors and flaws in the article.

## Funding

This research was supported by the Fundamental Research Funds for the Central Universities, project "Political Infiltration and Subversion in Great Power Competition" (大国竞争中的政治渗透和颠覆; 3162023ZYKC03).

## Conflict of Interests

The arguments made in this article do not represent the official position of the Ministry of Foreign Affairs or any other government authorities in China.

## References

Bolton, J. (2024). *The room where it happened: A White House memoir*. Simon & Schuster.

China declares all crypto-currency transactions illegal. (2021, September 24). *BBC*. https://www.bbc.com/news/technology-58678907

Clinton, H. (2010). *Remarks on internet freedom*. U.S. Department of State. https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm

Coats, D. (2019). *Worldwide threat assessment of the US intelligence community*. Office of the Director of National Intelligence.

Committee on Oversight and Government Reform. (2016). *The OPM data breach: How the government jeopardized our national security for more than a generation*.

Copeland, D. (2016). *Economic interdependence and war*. Princeton University Press.

Cyberspace Administration of China. (2016). *Zhonghua renmin gongheguo wangluo anquan fa*. https://www.cac.gov.cn/2016-11/07/c_1119867116.htm

Cyberspace Administration of China. (2024). *Shi nian qian, Xi Jinping shou ti cong 'wangluo daguo' dao 'wangluo qiangguo'*. https://www.cac.gov.cn/2024-03/08/c_1711570533840069.htm

De Mott, F. (2023, March 29). TikTok parent ByteDance has special stock owned by China's government: Here's how 'golden shares' give Beijing influence over the social-media giant. *Markets Insider*. https://markets.businessinsider.com/news/stocks/tiktok-ban-bytedance-golden-shares-chinese-government-communist-party-board-2023-3

Doshi, R. (2023). *The long game: China's grand strategy to displace American order*. Oxford University Press.

Evera, S. (2001). *Causes of war: Power and the roots of conflict*. Cornell University Press.

Exclusive: 'China Track' bank netting system shields Russia–China trade from Western eyes. (2025, April 22). *Reuters*. https://www.reuters.com/business/finance/china-track-bank-netting-system-shields-russia-china-trade-western-eyes-2025-04-22

Farrell, H., & Newman, A. (2019). *Of privacy and power: The transatlantic struggle over freedom and security*. Princeton University Press.

Fidler, D. P. (2020, October 5). The Clean Network program: Digital age echoes of the "long telegram"? *Council on Foreign Relations*. https://www.cfr.org/blog/clean-network-program-digital-age-echoes-long-telegram#:~:text=The%20U.S.%20State%20Department's%20Clean,%22long%20telegram%22%20in%201946

Fitzgerald, S. (n.d.). *Fact sheet—Huawei & entity list*. https://fitzgerald.house.gov/sites/evo-subsites/fitzgerald.house.gov/files/evo-media-document/FINAL%20Fact%20Sheet%20%E2%80%93%20Huawei%20%26%20Entity%20List%202.2.21.pdf

Friedberg, A. (2011). *A contest for supremacy: China, America, and the struggle for mastery in Asia*. WW Norton.

Gartzke, E., & Lindsay, J. (2015). Weaving tangled webs: Offense, defense, and deception in cyberspace. *Security Studies*, *24*(2), 316–348.

Glaser, C. (1997). The security dilemma revisited. *World Politics*, *50*(1), 171–201.

Hu, J. (2006, August 24). *Jianchi heping fazhan daolu tuidong jianshe hexie shijie*. *People's Daily*, 1–2.

Hvistendahl, M. (2016, October 25). The decline in Chinese cyberattacks: The story behind the numbers. *MIT Technology Review*. https://www.technologyreview.com/2016/10/25/156465/the-decline-in-chinese-cyberattacks-the-story-behind-the-numbers

Jervis, R. (1978). Cooperation under the security dilemma. *World Politics*, *30*(2), 167–214.

Jin, X. (2016, December 6). Woguo chuanmei lingyu youxiao tuijin teshu guanli gu zhidu de sikao. *People's Daily Online*. http://theory.people.com.cn/n1/2016/1206/c83865-28928486.html

Johnson, D. (2020). *Strategic instincts: The adaptive advantages of cognitive biases in international politics*. Princeton University Press.

Johnson, M. (2023). *China's grand strategy for global data dominance*. Hoover Institute.

Kastner, J., & Wohlforth, W. (2025). *A measure short of war: A brief history of great power subversion*. Oxford University Press.

Kumar, A. (2025, May 5). China's blockchain playbook: Infrastructure, influence, and the new digital order. *Center for Strategic and International Studies*. https://www.csis.org/blogs/strategic-technologies-blog/chinas-blockchain-playbook-infrastructure-influence-and-new

Laolao bawo keji jinbu da fangxiang. (2016, December 13). *Communist Party Member Network*. https://fuwu.12371.cn/2016/12/13/ARTI1481594800256510.shtml

Lindsay, J. (2015). The impact of China on cybersecurity: Fiction and friction. *International Security*, *39*(3), 7–47.

Liu, H. (2020). *Jiakuai goujian yi guonei da xunhuan wei zhuti, guonei guoji shuang xunhuan xianghu cujin de xin fazhan geju*. People's Central Government. https://www.gov.cn/guowuyuan/2020-11/25/content_5563986.htm

Lucas, R. (2022, February 22). The Justice Department is ending its controversial China Initiative. *NPR*. https://www.npr.org/2022/02/23/1082593735/justice-department-china-initiative

Maschmeyer, L. (2023). A new and better quiet option? Strategies of subversion and cyber conflict. *Journal of Strategic Studies*, *46*(3), 570–594.

Mastro, O. (2024). *Upstart: How China became a great power*. Oxford University Press.

Ministry of Foreign Affairs of the People's Republic of China. (2021). Zhong-er zongli di ershiliu ci dingqi huiwu lianhe gongbao. https://www.mfa.gov.cn/web/ziliao_674904/1179_674909/202112/t20211201_10460421.shtml

Mueller, R. (2019). *Report on the investigation into Russian interference in the 2016 presidential election*. US Department of Justice.

Office of the Director of National Intelligence. (2023). *Annual threat assessment of the US intelligence community*.

Pearson, M., Rithmire, M., & Tsai, K. (2022). China's party-state capitalism and international backlash: From interdependence to insecurity. *International Security*, *47*(2), 135–176.

Pence, M. (2018). *Remarks by Vice President Pence on the administration's policy toward China*. White House. https://trumpwhitehouse.archives.gov/briefings-statements/remarks-vice-president-pence-administrations-policy-toward-china

People's Central Government. (2015). *Zhonghua renmin gongheguo guojia anquan fa*. https://www.gov.cn/zhengce/2015-07/01/content_2893902.htm

People's Central Government. (2016). *Guowuyuan guanyu yinfa 'Shisanwu' guojia xinxihua guihua de tongzhi*. https://www.gov.cn/zhengce/content/2016-12/27/content_5153411.htm

People's Central Government. (2018). *Xi Jinping chuxi quanguo wangluo anquan he xinxihua gongzuo huiyi bing fabiao zhongyao jianghua*. https://www.gov.cn/xinwen/2018-04/21/content_5284783.htm

Pompeo, M. (2020). *Announcing the expansion of the Clean Network to safeguard America's assets*. https://2017-2021.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets

Sanger, D. (2018). *The perfect weapon: War, sabotage, and fear in the cyber age*. Scribe.

Segal, A. (2021). Huawei, 5G, and weaponized interdependence. In D. Drezner, H. Farrell, & A. Newman. (Eds.), *The uses and abuses of weaponized interdependence* (pp. 149–165). Brookings Institution Press.

Shirk, S. (2023). *Overreach: How China derailed its peaceful rise*. Oxford University Press.

State Council of China. (2023). *Xi Jinping kanwang canjia zhengxie huiyi de minjian gongshanglian jie weiyuan shi qiangdiao: zhengque yindao minying jingji jiankang fazhan, gao zhiliang fazhan*. https://www.gov.cn/xinwen/2023-03/06/content_5745092.htm

Sullivan, J. (2021). *Remarks by National Security Advisor Jake Sullivan at the National Security Commission on Artificial Intelligence Global Emerging Technology Summit*. White House. https://bidenwhitehouse.archives.gov/nsc/briefing-room/2021/07/13/remarks-by-national-security-advisor-jake-sullivan-at-the-national-security-commission-on-artificial-intelligence-global-emerging-technology-summit

Tétrault-Farber, G., & Osborn, A. (2021, March 22). Russia's top diplomat starts China visit with call to reduce U.S. dollar use. *Reuters*. https://www.reuters.com/article/world/russias-top-diplomat-starts-china-visit-with-call-to-reduce-us-dollar-use-idUSKBN2BE0XG

Trump, D. (2017). *National security strategy of the United States*.

Trump, D. (2020). *Executive order on addressing the threat posed by TikTok*. https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok

US Department of Justice. (2021). *Information about the Department of Justice's China Initiative and a compilation of China-related prosecutions since 2018*. https://www.justice.gov/archives/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related

US Department of State. (n.d.). *Building a clean network: Key milestones*. https://2017-2021.state.gov/building-a-clean-network-key-milestones

Walker, J. (2021, July 30). How the Chinese government controls Tencent, the seventh largest company in the world. *Vision Times*. https://www.visiontimes.com/2021/07/30/how-the-chinese-government-controls-tencent-the-seventh-largest-company-in-the-world.html

Wang Yi tong eluosi waizhang juxing huitan [Wang Yi holds talks with Russian Foreign Minister Lavrov]. (2021, March 23). *Xinhua*. https://www.xinhuanet.com/world/2021-03/23/c_1127246950.htm

White House. (2023). *National cybersecurity strategy*.

Wright, N. (2018, July 10). How artificial intelligence will reshape the global order: The coming competition between digital authoritarianism and liberal democracy. *Foreign Affairs*. https://www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order

Xi Jinping: Shishi guojia dashuju zhanlue jiakuai jianshe shuzi zhongguo. (2017, December 9). *Xinhua*. http://www.xinhuanet.com//politics/2017-12/09/c_1122084706.htm

Xi Jinping zai dier jie shijie hulianwang dahui kaimu shi shang de jianghua (quanwen). (2015, December 16). *Xinhua*. http://www.xinhuanet.com//politics/2015-12/16/c_1117481089.htm

Xi Jinping zai zhongyang zhengzhiju di shiba ci jiti xuexi shi qiangdiao ba qukuailian zuowei hexin jishu zizhu chuangxin zhongyao tupo kou, jiakuai tuidong qukuailian jishu he chanye chuangxin fazhan. (2019, October 25). *Xinhua*. https://www.xinhuanet.com/politics/2019-10/25/c_1125153665.htm

Xuezhe jiedu: Zhongguo chutai wangluo anquan shencha zhidu sida jiaodian. (2014, May 23). *CCP News Network*. http://theory.people.com.cn/n/2014/0523/c40531-25054345.html

Yang, D. (2018). *Zhengzhi anquan shi guojia anquan de genben*. Ministry of National Defense of the People's Republic of China. http://www.mod.gov.cn/gfbw/jmsd/4809950.html

Zhang, Y. (2023). Strategic vigilance: Mao's 'anti-peaceful evolution' strategy and China's policy toward the United States. *Journal of Cold War Studies*, *25*(2), 93–111.

## About the Author

Ziyuan Wang (also professionally known as William Z. Y. Wang) is an associate professor at the Institute of International Relations, China Foreign Affairs University. He completed his PhD at the London School of Economics and Political Science. His research interests include international relations theory, political psychology, China's security environments, and international history. His academic works are published in *International Security*, *Journal of Chinese Political Science*, and *Chinese Journal of International Politics*, along with several leading Chinese journals.

Politics and Governance
2025 • Volume 13 • Article 10218
https://doi.org/10.17645/pag.10218

ARTICLE

Open Access Journal

# The Social Movement Evolution of Non-State Armed Groups in the Web 3.0 Era

Yaohui Wang † and Yang Qiu †

Zhou Enlai School of Government, Nankai University, China

† The two authors contributed equally to this article and therefore share co-first authorship

**Correspondence:** Yang Qiu (yang.qiu12@mail.nankai.edu.cn)

**Submitted:** 27 February 2025 **Accepted:** 18 September 2025 **Published:** 27 November 2025

**Issue:** This article is part of the issue "Technology and Governance in the Age of Web 3.0" edited by Chang Zhang (Communication University of China), Zichen Hu (London School of Economics and Political Science), and Denis Galligan (University of Oxford), fully open access at https://doi.org/10.17645/pag.i443

## Abstract

How do the emerging Web 3.0 technologies affect the survival of non-state armed groups (NSAGs) in their violent struggles vis-à-vis state entities? While techno-optimists argue that Web 3.0 can democratize the internet and curb monopolistic practices, its decentralized features, such as enhanced privacy, data ownership, and personalization, also present significant security challenges. These technologies can be weaponized by NSAGs to promote their efficiency and resilience. Borrowing insights from social movement theory, we construct a theoretical framework to explain how Web 3.0 applications affect the dynamics of NSAGs by impacting their organizational modes and strategies. It is argued that blockchain-based platforms, metaverse projects, and other Web 3.0 technologies promote the efficiency of the recruitment, training, financing, purchasing, and communication processes of NSAGs, increasing their capacities as social organizations, and thereby render these groups more resilient to collapse. We illustrate and corroborate our theoretical claims by examining the cases of how NSAGs such as the Islamic State utilize decentralized crypto exchanges and the Dark Web in their operations.

## Keywords

blockchain; cryptocurrency; non-state armed groups; Web 3.0

## 1. Introduction

Over the past several decades, a growing consensus has emerged among scholars and industry experts that the rise of Web 3.0 represents a transformative force poised to revolutionize digital life (Barassi & Treré,

2012; Lassila & Hendler, 2007). In contrast to the Web 2.0 era, where powerful internet conglomerates dominate the digital landscape, Web 3.0 promises to decentralize control and empower users. During the contemporary Web 2.0 age, tech giants such as Facebook and Amazon wield unprecedented influence over the digital ecosystem, compelling users to rely on their proprietary platforms and algorithms. This dominance not only stifles competition from smaller innovators but also enables giant corporations (e.g., Facebook and Amazon) to amass vast amounts of user data, which they leverage to maximize profits and shape online behavior. Importantly, this practice significantly increases the risk of data leaks and illicit data manipulation for political objectives. In the infamous Facebook–Cambridge Analytica data scandal, for instance, whistleblowers revealed that approximately half a billion Facebook users' profile data had been secretly harvested to manipulate US presidential election outcomes (Cadwalladr & Graham-Harrison, 2018; Hinds et al., 2020). Indeed, one can argue that the integrity of democratic governance and the preservation of civil liberties may be significantly undermined by these big techs' interferences.

Thanks to recent advancements in internet technology, Web 3.0—the third generation of the internet—appears poised to address and potentially eliminate these concerning abusive practices. Cutting-edge technologies, particularly blockchain, cryptocurrencies, generative AI tools (such as ChatGPT and Sora), and the metaverse, have brought the foundational structure of the internet to a critical juncture of transformation. These innovations empower web users to maintain ownership of their data, effectively merging their roles as internet consumers and profit generators. This integration transforms consumption and production into a unified process, redefining the dynamics of digital interaction (Hyzen, 2023). In this way, the Web 3.0 trend not only enhances web users' financial gains but also curbs the dominance of powerful centralized corporations and their associated mega-platforms over the internet ecosystem. This shift fosters a more decentralized, personalized, and resilient digital environment, less susceptible to top-down interference. As highlighted by a policy paper published by the Tony Blair Institute for Global Change, Web 3.0 "would mark a departure from the centralized mega platforms and corporations that dominate the ecosystem currently and, proponents claim, fix what's wrong with the internet of today along with reversing the erosion of democracy" (Johnson, 2022).

Despite these advanced technological innovations, a small but increasing number of scholars and policymakers have begun to voice concerns about the potential challenges posed by Web 3.0 technologies. Professionals in STEM (Science, Technology, Engineering, and Mathematics) fields argue that while Web 3.0 may disrupt the existing power asymmetry between large corporations and individual users, it also introduces a range of cybersecurity threats, including fraud and the theft of user information (Bharadiya, 2023). Flash loan attacks, for example, are an increasingly frequent type of exploitation that takes place in decentralized finance (DeFi) ecosystems—operators utilize uncollateralized lending to carry out attacks. On May 12, 2021, for example, cyberthieves perpetrated a strike against the DeFi protocol xToken and took away USD 24.5 million (Copeland, 2021). The severity of these crimes is particularly concerning, as users themselves may now bear the responsibility for safeguarding their own data, making them potentially accountable for any breaches or losses.

Unsurprisingly, these novel forms of crime have led some scholars to highlight the unprecedented complexity of cybercrime in the Web 3.0 era. Zuo (2023) argues that the decentralization and anonymity features of Web 3.0 may provide illicit actors with opportunities to evade government regulations, particularly in activities such as underground fundraising and money laundering. Vayadande et al. (2024)

note that the decentralized nature of Web 3.0 poses significant challenges for account recovery, because the loss of internet keys in this new era is likely to be irreversible. Additionally, Zhu et al. (2024), utilizing survey methods, find that the technical barriers for users adapting to the Web 3.0 ecosystem can be prohibitively high. They also emphasize that effective online identity management becomes particularly challenging, as users no longer rely on traditional usernames and passwords to establish their digital identities. In a recently published article, O'Brien (2023) outlines several security concerns associated with Web 3.0, including smart contract vulnerabilities, private key management issues, phishing and scams, and the lack of user-friendly interfaces. O'Brien (2023) notes that these concerns "must be addressed to ensure a safe and secure Web3 ecosystem for all stakeholders involved." Outside academia, there have also been increasing doubts cast on the utility of the Web 3.0 movement. Elon Musk, the founder, CEO, and chief engineer of SpaceX, and Jack Dorsey, the chairman of payments company Block, for example, both assert that there is an urgent need to put the brakes on the momentum around the Web 3.0 trend (Shead, 2021).

While the Web 3.0 trend has gained significant prominence in STEM fields and industrial sectors, there remains a notable gap in the political science literature regarding the political risks associated with these advanced technologies. For instance, to what extent, and through which causal mechanisms, does Web 3.0 influence the use of political violence by non-state actors? Given that Web 3.0 has the potential to fundamentally reshape the online landscape, it raises the question of whether political actors seeking to consolidate and expand their power might also exploit these technologies. If so, how does Web 3.0 impact the strategies employed by these actors? Despite the clear importance of understanding the relationship between Web 3.0 and political violence, there has been a striking lack of political science research dedicated to exploring these puzzles.

To address this research gap, this article seeks to bridge existing scholarship on the security challenges posed by Web 3.0 with political science research on non-state armed groups (NSAGs). The focus here is specifically on NSAGs, as they are generally at a military disadvantage compared to nation-states (Podder, 2013). Consequently, these groups are likely to have strong incentives to conceal their operations by operating underground. This aligns with the core feature of Web 3.0—decentralization—which suggests that Web 3.0 technologies may exert a particularly significant influence on the organizational structures and strategies of NSAGs.

Drawing on insights from social movement theory, this article investigates the channels through which cutting-edge Web 3.0 technologies enable NSAGs to function more effectively and resiliently as social organizations. Specifically, it argues that Web 3.0 applications, such as blockchain-based platforms, metaverse projects, and decentralized data storage, simultaneously enhance the recruitment, training, purchasing, financing, and communication processes of NSAGs, thereby rendering these groups more decentralized and better equipped to confront their rivals. Here, it should be carefully noted that NSAGs typically refer to domestic and transnational resistant organizations, rebel groups, and insurgent groups (Englehart, 2016). In this article, however, we deliberately avoid using these more conventional terms, as they are often criticized for being overly subjective, politicized, and weaponized by Western political actors to delegitimize their opponents (LeVine, 1995). Therefore, we opt to use the term NSAG as a more neutral and technical designation.

The remainder of this article is structured as follows. First, we provide a comprehensive review of the background and characteristics of the Web 3.0 trend. Second, drawing on social movement theory, we

propose a causal mechanism to explain how these advanced technologies influence the organizational structures and strategies of NSAGs. Next, we conduct empirical analyses to illustrate and validate our theoretical claims, using two qualitative case studies on the use of cryptocurrencies and the Dark Web by NSAGs. Finally, we offer concluding remarks and discuss the policy implications.

## 2. A Review of the Development of Web 3.0 Technologies

Web 3.0, often referred to as the semantic web or decentralized web, is regarded as a significant milestone in the historical development of network technology (Nasar, 2023). Web 3.0 is defined by decentralization and user sovereignty, with core technologies like blockchain and cryptocurrencies enabling its functionality, while auxiliary innovations such as non-fungible tokens (NFTs) and DeFi expand its practical applications. In the Web 3.0 era, users no longer need to create multiple identities across different centralized platforms; instead, they can establish a single, decentralized universal digital identity system that operates across various platforms. Given the technical complexity of Web 3.0 technologies, it is essential to first provide a brief overview of the development from Web 1.0 to Web 3.0 before presenting our theoretical framework.

### *2.1. The Internet System Before Web 3.0 (1989–2013)*

Historically, the internet has gradually evolved from Web 1.0 to Web 3.0. During the Web 1.0 era, information access was one-directional as users could only retrieve static content updated solely by webmasters, leaving them passive network nodes without interactive capacity (Tekdal et al., 2018). The business model was equally restrictive, relying primarily on click-through rates, with profit dependent solely on the frequency of user clicks. This model persisted until the turn of the millennium, when the emergence of Web 2.0 prompted leading network companies to shift their focus toward portal sites.

Although coined in the 1990s, the term "Web 2.0" only attracted much attention after the O'Reilly Media Web 2.0 Conference in 2004 (Prandini & Ramilli, 2012). Conceptually, Web 2.0 is characterized by the widespread use of mobile internet technologies, fostering a user-centric and collaborative environment (Jacksi et al., 2020). In this era, users could not only search and review information but also act as content providers and interact with other users. Unlike Web 1.0's static platforms for texts, images, and videos, Web 2.0 enabled multidimensional information exchange, significantly enhancing user experience.

### *2.2. The Contemporary Web 3.0 Era*

The evolution from Web 2.0 to Web 3.0 marks a significant milestone in the history of the online world. The defining characteristic of Web 3.0 is the effective interconnection between users, facilitating the creation of user profiles (Jacksi, 2019). In comparison to Web 2.0, which often failed to reflect netizens' values, Web 3.0 introduced a new, decentralized ecosystem that shifts resources from large tech companies to individuals. This transition brought three key features: user interactions and personalized experiences, the rise and widespread adoption of virtual currencies and exchanges, and the growing recognition of the internet's value alongside demands for financial security (Rathor et al., 2023). Fundamentally, Web 3.0 rests on ideological rather than purely technological innovation.

On a macro level, Web 3.0 represents the current phase of the internet ecosystem—an increasingly "decentralized" online world driven by blockchain technology. Online content providers can now interact seamlessly across different websites, enabling more efficient information integration and freer flow of digital assets through decentralized platforms. Users can now access various nodes without compromising their data. Most notably, there has been a rise in Web 3.0 applications that allow users to input labor values and generate revenue from their digital assets (data). Data created by users are synchronized instantaneously across the internet (Kurilovas et al., 2014), making data inherently decentralized, interconnected, and structured for easier storage and use. This more personalized form of data creation and transfer enhances users' ability to communicate and access information.

Web 3.0 incorporates the concept of the semantic web, linking data across web pages to enable more efficient information comprehension and utilization, intelligent search, and data-understanding capabilities. In this way, the semantic web allows computers to better understand human languages and intentions. By promoting open standards, interoperability, and system flexibility, Web 3.0 fundamentally transforms both the mechanisms of individual online interactions and the business models of web companies (Murray et al., 2023).

### *2.3. Main Types of Web 3.0 Application Technologies*

There are over 20 types of Web 3.0 application technologies, including blockchain, smart contracts, decentralized storage, artificial intelligence (AI), encryption, distributed storage, big data, cloud computing, and the Internet of Things (IoT). Specifically, blockchain, smart contracts, encryption, and the IoT are closely tied to online transactions, digital currencies, and digital finance (Wan et al., 2024).

Blockchain technology, perhaps the most well-known of Web 3.0 technologies, embodies the core operational characteristics of Web 3.0: decentralization, security, and transparency (Zhang et al., 2023). It ensures the security and consistency of data by storing transaction information in record boxes (blocks) and linking multiple blocks to form a chain structure within peer-to-peer (P2P) networks, thereby providing a reliable platform for transactions and data storage. Additionally, smart contracts, self-executing computer programs that operate on the blockchain, are particularly relevant for businesses like digital asset management. Similarly, encryption technology, a critical security feature of Web 3.0, is used to protect user privacy and secure transaction information. Finally, the IoT is an indispensable component of Web 3.0. In the Web 3.0 era, the IoT not only facilitates the connection of different devices but is also integrated with blockchain, AI, and other technologies to deliver more efficient, secure, and intelligent internet services. As a result, the IoT plays a pivotal role in Web 3.0, especially in areas such as privacy protection, digital currencies, and digital finance. See Figure 1 for a visualization of Web 3.0 application technologies.

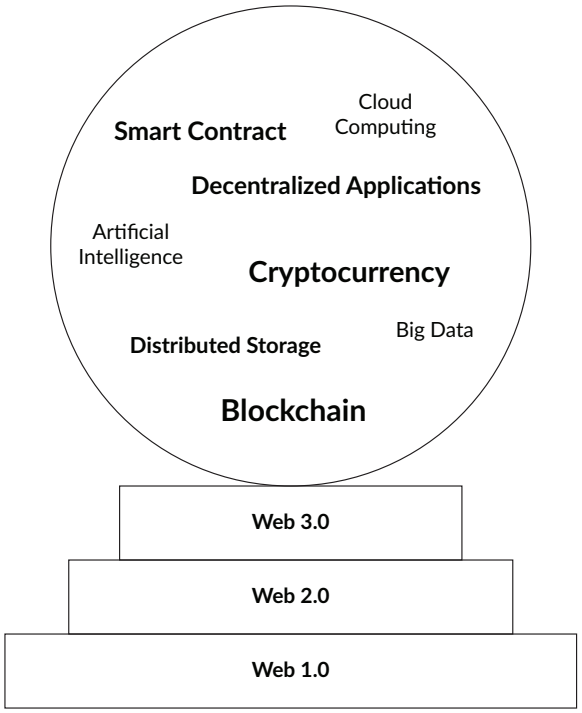



**Figure 1.** Main types of Web 3.0 application technologies. Note: Web 3.0 application technologies vary in prevalence, so the more commonly used ones are shown in larger font.

## 3. NSAGs in the Web 3.0 Era: A Social Movement Perspective

While the political actions of NSAGs can be aggressive and intimidating, a surprising scholarly consensus holds that these groups are, in fact, quite vulnerable, as they are inherently subject to risks of internal dysfunction (McLean et al., 2018; Vittori, 2009). From a political sociology perspective, NSAGs are not fundamentally different from legitimate, non-violent social groups—such as environmental NGOs, yoga clubs, athletic teams, and music bands. Regardless of their aims or scope, all such groups need well-designed organizational structures and secure resources to survive and sustain themselves. In this sense, like all other social organizations, NSAGs must first and foremost function as organizations: NSAGs must recruit members, propagate their political ideologies, secure stable and protected spaces in which to undertake their activities, establish effective communication channels, and raise funds (Wang et al., 2022).

Furthermore, in their struggle against nation-states, NSAGs must also engage in activities such as purchasing and transporting weapons and equipment, and maintaining confidentiality to evade government crackdowns (Jacobson, 2010). Unsurprisingly, the political science literature has consistently shown that most NSAGs have notably short lifespans and often fail to achieve their intended objectives. For example, early quantitative studies by Rapoport (1983) found that approximately 90 percent of certain types of NSAGs do not survive their first year, and of those that do, 50 percent do not last more than a decade. More recent empirical studies suggest that Rapoport's (1983) estimate may be overly pessimistic, but they nonetheless confirm the broader finding that most NSAGs are inherently short-lived (McLean et al., 2018).

Despite the conventional wisdom that NSAGs are unlikely to survive for long or achieve their objectives, this observation may be subject to revision in the context of the contemporary Web 3.0 era. Conceptually,

the decentralization inherent in Web 3.0 could inadvertently empower NSAGs, especially those seeking to conceal their operations from their adversaries—nation-states and rival governments. As such, this logic raises a crucial theoretical and policymaking question: How do Web 3.0 technologies impact the operations and internal functions of NSAGs? In other words, how and through what mechanisms does Web 3.0 influence the organizational structures and strategies of NSAGs? To address this question, we draw on insights from social movement theory within the field of sociology to construct a comprehensive analytical framework.

### *3.1. A Social Movement Theory of NSAGs*

Across various fields of social science, there has been abundant literature on the formation, development, and impact of social organizations (Morris, 2000). Yet, the research to date has been characterized by a distinct lack of knowledge on how NSAGs function as social organizations. In this regard, social movement theory is uniquely well-positioned to serve as the theoretical ground for our conceptual framework, which examines the dynamics of NSGAs in the Web 3.0 era, inasmuch as the theory places a particular emphasis on the micro-level elements that constitute the political mobilizations of the violent actors. As famously put by Beck (2008) nearly two decades ago, "[social movement theory] sees tactics, movements, and actors arrayed along a spectrum of related phenomenon rather than boxed in by formal, discrete categories" (p. 1566). Thus, before presenting our analytical framework, we first offer a brief review of the key concepts that have shaped social movement theory over the past 40 years.

Social movement theory is a school of sociological thought that examines the processes behind social movements. While it is true that numerous factors contribute to the dynamics of social groups, this does not necessitate a lengthy list of control variables. Rather, the focus should be on identifying the most fundamental variables that directly shape collective social actions. As such, social movement theory has predominantly concentrated on three key variables: (a) the framing process (perception, interpretation, and cognitive attribution) of political affairs; (b) mobilizing resources; and (c) political opportunities. Originating in the US and Western Europe over the past several decades, this threefold framework aims to explain when and how social movements emerge and evolve (Beck, 2008).

The first array of the tripartite model emphasizes the rhetorical and symbolic elements in social collective actions, which, as noted by McAdam (2017), are "the shared meanings and cultural understandings that people bring to any instance of potential mobilization" (p. 194). Logically, for a political movement to gain public endorsement, it needs to echo some widespread pre-existing sentiments among the general population. The sense of grievances, in this regard, often stands out as a pivotal magnet to attract people's support for NSAGs, because the organizers need to construct strategic narratives and frame political violence in a way that significantly resonates with some shared values in society (Ghatak et al., 2019). In doing so, organizers strive to convince disgruntled citizens and would-be fighters that the key solution to redress the problem they face is to act in groups and participate in violent campaigns. In this process, the media and other propaganda tools are important channels for NSAGs to disseminate their doctrines (rhetoric and claims) and recruit fighters. Indeed, framing has long been a major organizational effort in many NSAGs such as al-Qaeda, the Islamic State of Iraq and Syria (ISIS), and South American narco-NSAGs.

Second, the leadership of NSAGs needs to take control of mobilizing resources in order to sustain collective actions (Jenkins, 1983). By mobilizing resources, we refer to both tangible (funds, weapons, equipment) and

intangible resources such as training, transportation, and communication methods. Financing, in particular, is a critical material component for NSAGs (Freeman & Ruehsen, 2013). Here, it is worth noting that political violence is a costly venture. For NSAG organizers, securing reliable financial channels is crucial to purchasing arms and intelligence, paying bribes to corrupt officials, propagating their ideologies, and carrying out violent operations. Without these resources, NSAGs would be unable to function as organizations and would struggle to survive under government crackdowns.

The final pivotal factor that directly impacts the success or failure of NSAGs is the political opportunity external to the groups (Suh, 2001). Political opportunity, in this context, refers to sudden changes that dramatically alter the general environment for NSAGs, particularly events that shift the balance of power between NSAGs and the government in favor of the former. These shocks may include war, international sanctions, fiscal crises, changes in political leadership, natural disasters, and major technological innovations, among others. In the absence of political opportunities, governments typically hold an unbalanced advantage over non-state organizations, making it easier to eliminate NSAGs. However, sudden political shocks can instantly alter the bargaining structure, providing a unique "window of opportunity" for challengers (Meyer & Staggenborg, 1996). Thus, the likelihood of success in organizing collective actions can be significantly increased for certain movements shaped by the broader international and domestic political environment.

### *3.2. How Web 3.0 Technologies Impact the Organization of NSAGs: A Theoretical Framework*

Based on social movement theory, Web 3.0 technologies directly impact the organizational modes and strategies of NSAGs, mostly on three aspects: (a) perception, interpretation, and cognitive attribution, (b) mobilization of resources, and (c) propaganda and communications. Taken together, these aspects construct political opportunities for NSAGs to survive and proliferate. For concreteness, we visualize our theoretical framework in Figure 2.

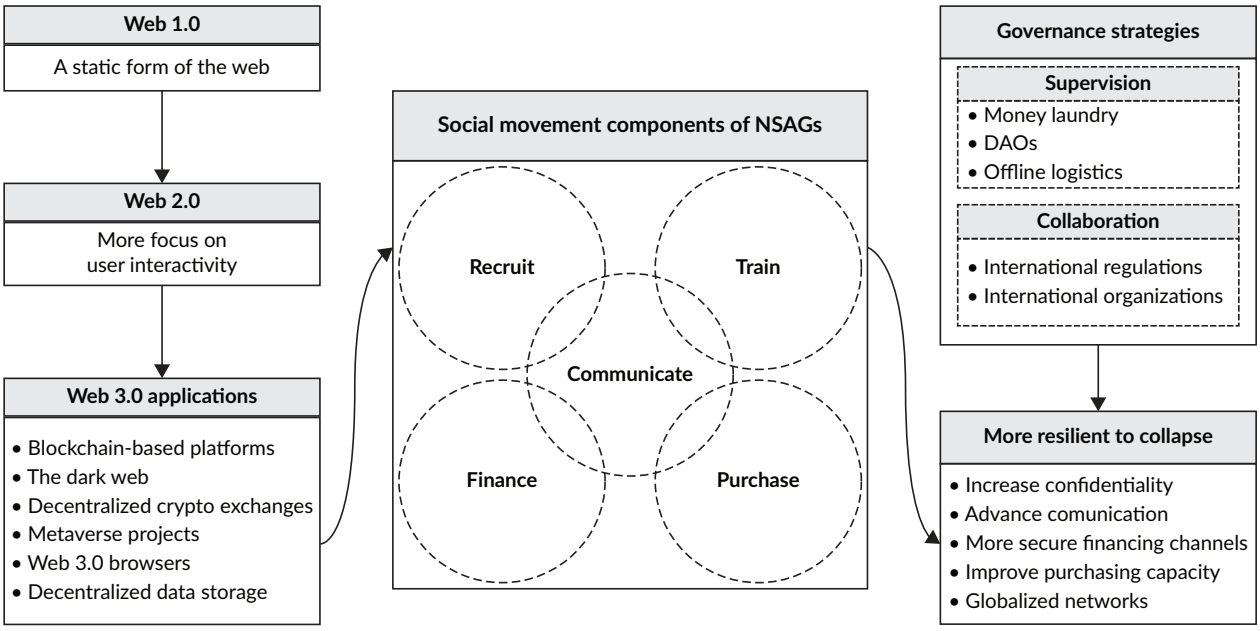



**Figure 2.** A social movement model of NSAGs in the Web 3.0 era. Note: DAOs = Decentralized Autonomous Organizations.

Firstly, leveraging their powerful transmission capacity, encrypted networks can influence the perception, interpretation, and cognition of NSAG members and potential recruits. This transmission process involves communication, the formation of ideological beliefs and action goals, the pursuit of recognition, and the promotion of training. Such processes can evoke resonance among netizens, who may then support the values of NSAGs. In the Web 3.0 era, NSAGs often seek to gain citizens' emotional endorsement through cyber technologies. By utilizing encrypted chat rooms and communication systems, NSAGs spread and infiltrate their violent ideologies, seeking both material and spiritual support from netizens. Scholarly works have demonstrated that some NSAG campaigns in sub-Saharan Africa exploit Web 3.0 applications to convey messages to potential fighters. For example, al-Shabaab in Somalia utilizes encrypted networks to deploy its fighters (Pearlman & Cunningham, 2012). Al-Shabaab is an Islamic fundamentalist NSAG primarily operating in Somalia, but also active in the broader East African region. Historically, the group has expressed support for Osama bin Laden and al-Qaeda. Despite bin Laden's death, al-Shabaab has continued launching attacks in Kenya, Libya, and Uganda, and has murdered numerous civilians, particularly women and children. Their violent campaign targets the Somali government and the African Union, and the group controls a significant portion of territory in south-central Somalia. Similarly, encryption technologies are embedded in the daily communication of ISIS, primarily through Web 3.0 apps. ISIS fighters have been known to download these apps onto their devices to store and exchange NSAG-related information. In some lone wolf attacks, there is evidence that NSAGs have used Web 3.0 apps for communication. For instance, Anwar al-Awlaki, a member of al-Qaeda, collaborated with Rajib Karim, a British Airways employee, to set up an encrypted communication system for planning attacks on British Airways (Dodd, 2011).

Second, extensive studies have shown that NSAGs use cryptocurrencies to finance their operations. Theoretically, NSAGs can generate resources through both external and internal channels. External channels typically include state sponsorship, while internal channels often involve taxation, public donations, and kidnapping. Regardless of the sources of financing, NSAGs must secure stable channels to collect resources and make payments when purchasing intelligence or equipment. With the rise of Web 3.0 technologies, cryptocurrencies have become a major financing tool for NSAGs. Since cryptocurrencies offer anonymity and untraceability for monetary transactions, they are highly favored by NSAGs, who use Bitcoin and other open-source P2P currencies for transactions. For example, ISIS, which has seen its traditional revenue sources such as oil and taxes diminish in recent years, now relies on cryptocurrencies like Bitcoin, Dash, Ethereum, Monero, Verge, and Zcash for a significant portion of its financial assets. Similarly, al-Shabaab, the NSAG mentioned earlier, has also begun to use cryptocurrencies to raise funds and make payments. Hassan Afgooye, a member of al-Shabaab's leadership, oversees a complex financial network based primarily on cryptocurrencies. This network raises funds through fake charities, extortion, and kidnapping, which are then converted into cryptocurrencies. Afgooye uses these funds to support al-Shabaab's violent campaign (U.S. Department of the Treasury, 2022).

Third, propaganda based on Web 3.0 technologies has become central to how NSAGs function as organizations. For decades, NSAGs have sought effective online propaganda tools to convey their messages to the general public, and the development of Web 3.0 applications in recent years has accelerated the weaponization of these cutting-edge technologies. According to scholarly findings, many Web 3.0-based Dark Web platforms and online chatrooms are connected to NSAGs, which often post extremist speeches by their leaders or senior members to propagate violent ideologies (Rusumanov, 2016). For example, both al-Shabaab and Boko Haram have been active on Web 3.0-based Dark Web platforms, using them to sustain

public advocacy and coordinate financial activities to ensure adequate funding. These speeches often justify the excessive use of force, arguing that such actions are righteous if their goals are deemed justified (Rusumanov, 2016). Specifically, NSAGs often employ AI models to generate deepfake content, creating seemingly authentic images and videos to spread their extremist ideologies and convince audiences. In doing so, NSAGs contribute to misinformation, division, and political turmoil among their target populations. In effect, ISIS carried out a deadly attack in Moscow in March 2024, using Web 3.0 technologies to deploy members and materials. The Russian government found evidence that ISIS funded the attack through cryptocurrency transactions and the Dark Web, enabling them to carry out the operation (Huang, 2025).

Taken together, the Web 3.0 technologies discussed above directly impact the organizational modes and strategies of NSAGs, enabling them to survive and operate as social organizations. These technologies facilitate more efficient communication, recruitment, incitement, and propaganda, while also providing clandestine channels for weapons procurement and unregulated financial transactions.

## 4. Case Studies: NSAGs' Engagement With Web 3.0 Technologies

To corroborate and illustrate our theoretical claims, we employ two case studies. The first examines how NSAGs exploit AlphaBay, a notorious Web 3.0-based Dark Web platform, for communication, propaganda, recruitment, member training, and financial transactions. The second case study focuses on how Web 3.0 technologies influence the financing strategies of ISIS, with particular attention to its use of cryptocurrencies for resource collection and payments.

### *4.1. Dark Web Transactions and AlphaBay*

In recent decades, the Dark Web has become a crucial platform for NSAGs to plan and execute violent attacks (Sageman, 2011). Technically, the Dark Web is a subset of the Deep Web, which itself is part of the broader World Wide Web—the publicly accessible internet. Due to its clandestine nature, the Dark Web can only be accessed through specialized software, unique licenses, or specific computer settings. In the Web 3.0 era, the Dark Web's characteristics have been significantly enhanced, as the development of decentralized technologies has further bolstered the anonymity of its users.

In particular, Web 3.0 utilizes decentralized protocols that prioritize individual privacy and resist internet censorship, aligning perfectly with the core characteristics and functions of the Dark Web. As a result, new decentralized marketplaces, forums, and chatrooms have emerged within the Dark Web, facilitated by Web 3.0 technologies. Consequently, NSAGs are increasingly relying on the Dark Web, viewing it as a secure and reliable space that is largely impervious to government crackdowns.

Since the Dark Web operates within the underworld of the regular internet, users need special "keys" to access it, namely the anonymous proxy tool Tor, or "The Onion Router." Tor protects users in a way similar to the layers of an onion, ensuring that their addresses, identities, and the websites they visit remain completely anonymous (Montieri et al., 2018). Paul Syverson, the mathematician from the U.S. Naval Research Laboratory who invented Tor, originally designed the tool to safeguard the privacy of law-abiding individuals (Reed et al., 1998). However, its unintentional benefit has been to support NSAGs. For instance,

Bitcoin, a cryptocurrency frequently traded on the Dark Web, allows NSAGs to conduct financial transactions without relying on credit cards or bank accounts, enabling them to evade government oversight.

Given that the Dark Web offers a safe haven for users to evade government supervision, it has become a hub for numerous illicit activities, including arms deals, drug trafficking, pornography, and financial fraud. For NSAGs, in particular, the Dark Web serves as a crucial underground channel for recruiting members, purchasing weapons, propagating ideologies, and plotting violent attacks. Specifically, NSAGs use chatrooms to spread extremist ideologies, recruit new members, and establish "master-slave" relationships within their networks. Both ISIS and al-Qaeda, for example, are known to utilize the Dark Web to recruit foreign terrorist fighters and organize attacks. Despite global efforts to crack down on these dangerous networks, encrypted communications remain largely impenetrable. Research has shown that ISIS and other jihadist groups have long relied on encrypted mobile apps, such as Telegram, to exchange sensitive information (Bloom et al., 2019; Shehabat et al., 2017). Additionally, these groups often post lectures and tutorials to train their members on how to use the Dark Web effectively to evade government detection (Coker et al., 2015).

To illustrate, a prominent example is the case of AlphaBay. Since its establishment in 2014, AlphaBay facilitated nearly USD 1 billion in illegal transactions involving drugs, firearms, embargoed goods, stolen items, counterfeit products, malware, and NSAG-related activities. According to a RAND report, NSAGs could purchase materials like *The Terrorist's Handbook* and the *Explosives Guide* on AlphaBay (Ryan et al., 2017). Furthermore, the report highlights that AlphaBay also offered a fake documents service, which sold customized fake government-issued documents and passports to NSAGs. More broadly, the illicit activities of NSAGs on AlphaBay included a range of transactions that supported their operations.

First, the Dark Web serves as a platform for member recruitment, communication, and training. On the decentralized AlphaBay platform, NSAGs like ISIS were able to propagate extremist ideologies, recruit new members, allocate funding to followers, and purchase training materials, such as courses on bomb-making. To be more specific, one study by the European Union Institute for Security Studies notes that, on AlphaBay, ISIS sold manuals containing terrorist operational guidance and instructions for manufacturing explosives to jihadist sympathizers (Berton, 2015). Although AlphaBay was not intentionally designed as a communication outlet for NSAGs, its relative anonymity and security nevertheless offered such organizations a platform to disseminate training materials. Moreover, according to the study, AlphaBay's fake document services enabled jihadist members and sympathizers to obtain high-quality counterfeit IDs, allowing them to circumvent legal restrictions and border controls to enter Iraq and Syria (Berton, 2015). Again, such services of AlphaBay facilitated the recruitment and communication activities of NSAGs.

Second, AlphaBay facilitated fundraising and financial transactions. Similar to other Dark Web platforms, it provided NSAGs with secure channels to receive and redistribute digital currencies like Bitcoin (Dilipraj, 2014). On the one hand, with respect to fundraising, supporters of ISIS used Bitcoin (and other cryptocurrencies), transferred via trade or donations, to fund the terrorist organization (Berton, 2015). AlphaBay may have also provided NSAGs with additional sources of funding by selling stolen bank card information and hacked PayPal accounts, which could be exploited by NSAGs with minimal risk of detection by state authorities. On the other hand, with the funds obtained through AlphaBay, NSAGs were able to purchase essential resources for their survival and operations. Notably, AlphaBay's online markets sold computer hacking tools, firearms, and ammunition to groups like ISIS. As a matter of fact, when AlphaBay was taken down, there were over

100,000 listings for stolen documents, firearms, and other illicit goods (U.S. Department of Justice, 2017). All these underscore AlphaBay's significance as a conduit for financing and equipping NSAGs.

Third, AlphaBay was also involved in illicit drug trafficking. According to the U.S. Department of the Treasury (2024), AlphaBay and similar Dark Web platforms employ encryption technologies that shield communications and transactions from state monitoring. This makes them highly attractive to drug cartels, which exploit these sites both to market toxic chemicals and to acquire the raw materials and manufacturing equipment necessary for their production (U.S. Department of the Treasury, 2024). In July 2017, in an international law enforcement investigation, the U.S. Department of Justice took down AlphaBay, which at the time had evolved into one of the world's largest Dark Web platforms. According to a BBC report, approximately USD 450 million was spent on the marketplace between May 2015 and February 2017, with illegal drugs such as heroin and fentanyl listed for sale (Baraniuk, 2017). At the time of its takedown, AlphaBay hosted over 250,000 listings for illegal drugs and toxic chemicals (U.S. Department of Justice, 2017). To further illustrate the Dark Web's critical utility to their operations, take Mexican cartels such as Sinaloa as an example. These cartels exploit the Dark Web by using cryptocurrencies to purchase precursor chemicals and, after processing them into narcotics, relying on the same platforms to traffic drugs to American consumers. Such activities have further exacerbated the US opioid crisis, which claimed more than 107,000 American lives from overdoses in 2023 alone (U.S. Department of the Treasury, 2024).

### *4.2. ISIS's Use of Cryptocurrencies*

For NSAGs, the ideal funding channels should possess six key characteristics: quantity, legitimacy, security, reliability, controllability, and simplicity (Freeman & Ruehsen, 2013). To this end, cryptocurrencies are frequently utilized by NSAGs such as ISIS in their financial activities.

Cryptocurrencies, built on blockchain technology, are typically more reliable and anonymous than conventional currencies. Technically, cryptocurrency can be understood as a medium of exchange that uses cryptographic principles to secure transactions and regulate the creation of transaction units. Bitcoin, introduced in 2009, was the first decentralized cryptocurrency. Unlike traditional banking systems, which depend on centralized regulatory frameworks, cryptocurrencies are based on a decentralized consensus mechanism. In the Web 3.0 era, cryptocurrencies serve as a medium of value exchange, facilitating payments for decentralized applications. Cryptocurrency exchanges in Web 3.0 play a crucial role in asset trading by enabling secure transactions through smart contracts, enhancing both security and transparency. With their decentralization, security, and financial autonomy, cryptocurrencies offer NSAGs an effective means of funding their violent operations. For instance, in January 2017, it was reported by Indonesia's financial transactions agency that Islamic militants in the Middle East used Bitcoin to support terrorist operations in the country (Yuniar, 2017). And in March 2024, the Islamic State – Khurasan Province, ISIS's affiliate in Afghanistan, carried out a terrorist attack in Moscow, partially financed using cryptocurrency ("Category deep-dive," 2025).

ISIS was one of the earliest NSAGs to employ cryptocurrencies. In addition to Bitcoin and Tether, recent evidence demonstrates that Monero has also become a new type of cryptocurrency used by ISIS to collect donation money from its sympathizers (Awasthi, 2024). In a recent policy analysis published by TRM Labs ("TRM finds mounting evidence," 2023), a reputable blockchain intelligence company, increasing ISIS funds

had been transferred using cryptocurrencies throughout Asia. In Tajikistan, most particularly, a number of pro-ISIS organizations raised approximately USD 2 million on Tron (a decentralized blockchain-based operating system) in 2022. These funds were spent on the recruitment of terrorists to join the Islamic State – Khurasan Province. Similarly, other reporters found that ISIS used Bitcoin to fund the bombings in Sri Lanka on April 21, 2019. Before the attack, ISIS used CoinPayments, a payment portal based in Canada, to convert its Bitcoin into paper currency. In March 2020, the US federal court sentenced Zoobia Shahnaz from Long Island, New York, to 13 years in prison for using Bitcoin and other cryptocurrencies to conduct money laundering for ISIS (Saravalle & Rosenberg, 2018). In addition, NSAGs also used social media to process cryptocurrency transactions. For example, in August 2015, Ali Shukri Amin, a 17-year-old from Virginia, US, was sentenced to 11 years in prison for publicly supporting ISIS on his Twitter account (Abutaleb & Cooke, 2016). Under the account name @Amreekiwitness, Ali Shukri Amin posted tutorials on how to use Bitcoin to fund ISIS and other NSAGs.

Several cases in 2015 revealed how ISIS sympathizers experimented with cryptocurrencies to provide material support to the organization. In January, Abu-Mustafa, a known ISIS supporter, successfully raised five Bitcoins (approximately USD 1,000 at the time) before the FBI intervened and shut down his account. This case is widely regarded as the first documented instance of ISIS employing cryptocurrency on the Dark Web. In May, another ISIS supporter dubbed "Abu Ahmed al-Raqqa" issued an appeal on the Dark Web, soliciting donations for ISIS in the form of Bitcoin. Later, in August, an ISIS-affiliated hacker attempted to extort two Bitcoins (roughly USD 500 at the time) from a US internet company, offering in return to remove a bug from their software. Beyond financial extortion, the hacker's far more damaging act was exploiting the internet company's bug to obtain the names of 1,351 US government and military personnel and sharing them with ISIS, which later compiled an assassination list. While these incidents appear largely episodic and suggest that, at least in 2015, ISIS had not yet developed a systematic reliance on Bitcoin for fundraising, they nonetheless demonstrate that NSAGs were beginning to recognize the potential utility of virtual currencies.

## 5. Conclusion and Policy Implications

We start with the observation that Web 3.0 technologies, most prominently decentralized applications, blockchain, and DeFi, function as a double-edged sword for governments and the general public. Importantly, inasmuch as Web 3.0 emphasizes user privacy and the individual control of data, NSAGs and other illicit groups may seek to take advantage of these novel applications to perpetrate terrorist attacks, commit human trafficking, drug trafficking, and other criminal activities. As a result, the absence of government supervision and crackdowns allows Web 3.0 technologies to potentially facilitate the operation of NSAGs on decentralized platforms. While this argument is intuitively compelling, there had yet to be a systematic exploration in political science literature that investigates how, and through which mechanisms, Web 3.0 applications influence the survival and operational strategies of NSAGs.

In this study, drawing upon insights from social movement theory, we develop a theoretical framework to understand how Web 3.0 technologies influence the organizational modes and structures of NSAGs. Specifically, we explore the mechanisms through which digital currencies, decentralized network applications, AI, and the Dark Web enhance key organizational functions of NSAGs, such as communication, recruitment, financing, and propaganda.

This study addresses a critical research gap at the intersection of Web 3.0 studies and political violence research by analyzing how NSAGs strategically exploit emerging digital technologies. Scholarship on Web 3.0 has largely emphasized its emancipatory potential, such as decentralization, personalization, and user empowerment, while overlooking its security implications. By documenting how NSAGs appropriate Web 3.0's core features, particularly anonymity, this study demonstrates that these same attributes enable illicit financing, recruitment, and operational resilience. In doing so, it expands mainstream understandings of Web 3.0 by highlighting the security implications it poses when appropriated by malign actors. At the same time, research on political violence has insufficiently engaged with technological transformations as drivers of organizational and strategic change among NSAGs. By foregrounding the role of Web 3.0, this study reveals how emerging digital technologies have functioned not merely as tools but as structural forces reshaping the dynamics of political violence. This positions technology not as an external variable but as a constitutive element of NSAG resilience and survival strategies. Taken together, the findings bridge a divide between technology studies and political violence scholarship. By focusing on the security implications of Web 3.0, this study aims to enrich our understanding of conflict in the era of Web 3.0, in which technological empowerment and unconventional security threats are deeply intertwined.

This research highlights that, in the Web 3.0 era, intelligence agencies and law enforcement face increasing challenges in tracking and disrupting the activities of NSAGs. Based on our theoretical analysis, two major policy implications reveal themselves.

First, nation-states should consider establishing international institutions to combat the transnational operations of NSAGs through Web 3.0 networks. As our analysis shows, the development of Web 3.0 technologies has significantly facilitated the expansion of NSAGs' digital networks, which can now easily transcend national borders. Notably, the financing channels of NSAGs are often tied to multiple financial institutions across different countries. Therefore, governments facing NSAG threats should collaborate to impose multinational sanctions on Web 3.0 financial services providers found to be facilitating NSAGs' cryptocurrency transactions. These sanctions could be complemented by implementing stricter regulations on cryptocurrency exchanges and, in some cases, limiting the anonymity features of privacy coins. Overall, international cooperation is essential to monitor and regulate DeFi platforms and smart contracts, which NSAGs may exploit for money laundering and financial transactions.

Second, government entities should also explore the potential of Web 3.0 technologies, leveraging these powerful decentralized applications to enhance their efforts against NSAGs. AI-powered threat detection models, in particular, present a promising tool. Given that NSAGs' operations on blockchains are typically anonymous and difficult to track using conventional methods, intelligence agencies and law enforcement can employ machine learning algorithms and AI to identify unusual patterns and trends in transnational financial transactions, communications, and other illicit activities. These AI-driven tools could enable governments to more effectively detect and disrupt NSAGs' clandestine operations. To this end, governments may consider allocating resources and providing policy support to research institutions focused on developing advanced technical tools to monitor NSAG activities on Web 3.0 networks, including their use of blockchain for encrypted communications, propaganda, and decentralized financial transactions.

## Acknowledgments

The authors would like to thank the reviewers and editors for their valuable comments and feedback. They also extend their gratitude to Phillip Kraeter and David An for proofreading the article.

## Funding

This study has received financial support from the National Social Science Fund of China (no. 25CGJ006).

## Conflict of Interests

The authors declare no conflict of interests.

## References

Abutaleb, Y., & Cooke, K. (2016, June 6). A teen's turn to radicalism and the U.S. safety net that failed to stop it. *Reuters*. https://www.reuters.com/investigates/special-report/usa-extremists-teen

Awasthi, S. (2024, May 8). Exploring the nexus: Cryptocurrency, Zakat, and terror funding. *Observer Research Foundation*. https://www.orfonline.org/expert-speak/exploring-the-nexus-cryptocurrency-zakat-and-terror-funding

Baraniuk, C. (2017, July 21). AlphaBay and Hansa dark web markets shut down. *BBC*. https://www.bbc.com/news/technology-40670010

Barassi, V., & Treré, E. (2012). Does Web 3.0 come after Web 2.0? Deconstructing theoretical assumptions through practice. *New Media & Society*, *14*(8), 1269–1285.

Beck, C. J. (2008). The contribution of social movement theory to understanding terrorism. *Sociology Compass*, *2*(5), 1565–1581.

Berton, B. (2015). *The dark side of the web: ISIL's one-stop shop?* European Union Institute for Security Studies. https://www.iss.europa.eu/publications/alerts/dark-side-web-isils-one-stop-shop

Bharadiya, J. P. (2023). Artificial intelligence and the future of web 3.0: Opportunities and challenges ahead. *American Journal of Computer Science and Technology*, *6*(2), 91–96.

Bloom, M., Tiflati, H., & Horgan, J. (2019). Navigating ISIS's preferred platform: Telegram. *Terrorism and Political Violence*, *31*(6), 1242–1254.

Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Category deep-dive: Use of crypto in terrorist financing expanded in 2024. (2025, March 5). *TRM Labs*. https://www.trmlabs.com/resources/blog/category-deep-dive-use-of-crypto-in-terrorist-financing-expanded-in-2024

Coker, M., Schechner, S., & Flynn, A. (2015, November 16). How Islamic State teaches tech savvy to evade detection. *The Wall Street Journal*. https://www.wsj.com/articles/islamic-state-teaches-tech-savvy-1447720824

Copeland, T. (2021, May 12). Attacker uses flash loans in $24.5 million exploit of DeFi protocol xToken. *The Block*. https://www.theblock.co/post/104667/defi-protocol-xtoken-exploit-attack

Dilipraj, E. (2014). Terror in the Deep and Dark Web. *Air Power Journal*, *9*(3), 121–140.

Dodd, V. (2011, February 28). British Airways worker Rajib Karim convicted of terrorist plot. *The Guardian*. https://www.theguardian.com/uk/2011/feb/28/british-airways-bomb-guilty-karim

Englehart, N. A. (2016). Non-state armed groups as a threat to global security: What threat, whose security? *Journal of Global Security Studies*, *1*(2), 171–183.

Freeman, M., & Ruehsen, M. (2013). Terrorism financing methods: An overview. *Perspectives on Terrorism*, *7*(4), 5–26.

Ghatak, S., Gold, A., & Prins, B. C. (2019). Domestic terrorism in democratic states: Understanding and addressing minority grievances. *Journal of Conflict Resolution*, *63*(2), 439–467.

Hinds, J., Williams, E. J., & Joinson, A. N. (2020). "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies*, *143*, Article 102498.

Huang, C. (2025, February 10). Illicit crypto volume drops in 2024, but use in terrorist financing up: Report. *The Straits Times*. https://www.straitstimes.com/business/illicit-crypto-volume-drops-in-2024-but-the-use-in-terrorist-financing-grew-report

Hyzen, A. (2023). Propaganda and the Web 3.0: Truth and ideology in the digital age. *Nordic Journal of Media Studies*, *5*(1), 49–67.

Jacksi, K. (2019). Design and implementation of e-campus ontology with a hybrid software engineering methodology. *Science Journal of University of Zakho*, *7*(3), 95–100.

Jacksi, K., Ibrahim, R. K., Zeebaree, S. R., Zebari, R. R., & Sadeeq, M. A. (2020). Clustering documents based on semantic similarity using HAC and K-mean algorithms. In *2020 International Conference on Advanced Science and Engineering (ICOASE)* (pp. 205–210). IEEE.

Jacobson, M. (2010). Terrorist financing and the internet. *Studies in Conflict & Terrorism*, *33*(4), 353–363.

Jenkins, J. C. (1983). Resource mobilization theory and the study of social movements. *Annual Review of Sociology*, *9*(1), 527–553.

Johnson, G. (2022). *Will Web 3.0 secure a democratic future?* Tony Blair Institute for Global Change. https://institute.global/insights/tech-and-digitalisation/will-web-30-secure-democratic-future

Kurilovas, E., Kubilinskiene, S., & Dagiene, V. (2014). Web 3.0-based personalisation of learning objects in virtual learning environments. *Computers in Human Behavior*, *30*, 654–662.

Lassila, O., & Hendler, J. (2007). Embracing "Web 3.0." *IEEE Internet Computing*, *11*(3), 90–93.

LeVine, V. T. (1995). The logomachy of terrorism: On the political uses and abuses of definition. *Terrorism and Political Violence*, *7*(4), 45–59.

McAdam, D. (2017). Social movement theory and the prospects for climate change activism in the United States. *Annual Review of Political Science*, *20*(1), 189–208.

McLean, E. V., Hinkkainen, K. H., de la Calle, L., & Bapat, N. A. (2018). Economic sanctions and the dynamics of terrorist campaigns. *Conflict Management and Peace Science*, *35*(4), 378–401.

Meyer, D. S., & Staggenborg, S. (1996). Movements, countermovements, and the structure of political opportunity. *American Journal of Sociology*, *101*(6), 1628–1660.

Montieri, A., Ciuonzo, D., Aceto, G., & Pescape, A. (2018). Anonymity services Tor, I2P, JonDonym: Classifying in the Dark (Web). *IEEE Transactions on Dependable and Secure Computing*, *17*(3), 662–675.

Morris, A. (2000). Reflections on social movement theory: Criticisms and proposals. *Contemporary Sociology*, *29*(3), 445–454.

Murray, A., Kim, D., & Combs, J. (2023). The promise of a decentralized internet: What is Web3 and how can firms prepare? *Business Horizons*, *66*(2), 191–202.

Nasar, M. (2023). Web 3.0: A review and its future. *International Journal of Computer Applications*, *185*(10), 41–46.

O'Brien, S. (2023, June 23). How Web3 security concerns might impact you. *IEEE Computer Society*. https://www.computer.org/publications/tech-news/trends/web3-security-concerns

Pearlman, W., & Cunningham, K. G. (2012). Nonstate actors, fragmentation, and conflict processes. *Journal of Conflict Resolution*, *56*(1), 3–15.

Podder, S. (2013). Non-state armed groups and stability: Reconsidering legitimacy and inclusion. *Contemporary Security Policy*, *34*(1), 16–39.

Prandini, M., & Ramilli, M. (2012). Raising risk awareness on the adoption of Web 2.0 technologies in decision making processes. *Future Internet*, *4*(3), 700–718.

Rapoport, D. C. (1983). Fear and trembling: Terrorism in three religious traditions. *American Political Science Review*, *78*(3), 658–677.

Rathor, S., Zhang, M., & Im, T. (2023). Web 3.0 and sustainability: Challenges and research opportunities. *Sustainability*, *15*(20), Article 15126.

Reed, M. G., Syverson, P. F., & Goldschlag, D. M. (1998). Anonymous connections and onion routing. *IEEE Journal on Selected Areas in Communications*, *16*(4), 482–494.

Rusumanov, V. (2016). The use of the internet by terrorist organizations. *Information & Security*, *34*(2), 137–150.

Ryan, N., Persi Paoli, G., Aldridge, J., & Warnes, R. (2017). *Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web*. RAND Corporation. https://policycommons.net/artifacts/4836375/behind-the-curtain/5673069

Sageman, M. (2011). *Leaderless jihad: Terror networks in the twenty-first century*. University of Pennsylvania Press.

Saravalle, E., & Rosenberg, E. (2018, January 9). Bitcoin can help terrorists secretly fund their deadly attacks. *Center for a New American Security*. https://www.cnas.org/publications/commentary/bitcoin-can-help-terrorists-secretly-fund-their-deadly-attacks

Shead, S. (2021, December 21). Elon Musk and Jack Dorsey are talking about 'Web3'—Here's what it is and why it matters. *CNBC*. https://www.cnbc.com/2021/12/21/elon-musk-and-jack-dorsey-are-talking-about-web3-heres-why.html

Shehabat, A., Mitew, T., & Alzoubi, Y. (2017). Encrypted jihad: Investigating the role of Telegram app in lone wolf attacks in the West. *Journal of Strategic Security*, *10*(3), 27–53.

Suh, D. (2001). How do political opportunities matter for social movements? Political opportunity, misframing, pseudosuccess, and pseudofailure. *The Sociological Quarterly*, *42*(3), 437–460.

Tekdal, M., Sayginger, Ş., & Baz, F. Ç. (2018). Developments of web technologies and their reflections to education: A comparative study. *Journal of Educational and Instructional Studies in the World*, *8*(1), 17–27.

TRM finds mounting evidence of crypto use by ISIS and its supporters in Asia. (2023, July 20). *TRM Labs*. https://www.trmlabs.com/resources/blog/trm-finds-mounting-evidence-of-crypto-use-by-isis-and-its-supporters-in-asia

U.S. Department of Justice. (2017, July 20). *AlphaBay, the largest online 'dark market,' shut down* [Press release]. https://www.justice.gov/archives/opa/pr/alphabay-largest-online-dark-market-shut-down

U.S. Department of the Treasury. (2022, October 17). *Treasury designates al-Shabaab financial facilitators* [Press release]. https://home.treasury.gov/news/press-releases/jy1028

U.S. Department of the Treasury. (2024). *Supplemental advisory on the procurement of precursor chemicals and manufacturing equipment used for the synthesis of illicit fentanyl and other synthetic opioids* (FinCEN Advisory FIN-2024-A002). https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2024-a002

Vayadande, K., Baviskar, A., Avhad, J., Bahadkar, S., Bhalerao, P., & Chimkar, A. (2024, June). A comprehensive review on navigating the Web 3.0 landscape. In *2024 Second International Conference on Inventive Computing and Informatics (ICICI)* (pp. 456–463). IEEE.

Vittori, J. (2009). All struggles must end: The longevity of terrorist groups. *Contemporary Security Policy*, *30*(3), 444–466.

Wan, S., Lin, H., Gan, W., Chen, J., & Philip, S. Y. (2024). Web3: The next internet revolution. *IEEE Internet of Things Journal*, *11*(21), 34811–34825.

Wang, Y., Shen, Y., & Han, Z. (2022). Economic sanctions and state-sponsored terrorism: The case of Iran. *Israel Affairs*, *28*(5), 645–660.

Yuniar, R. W. (2017, January 10). Bitcoin, PayPal used to finance terrorism, Indonesian agency says. *The Wall Street Journal*. https://www.wsj.com/articles/bitcoin-paypal-used-to-finance-terrorism-indonesian-agency-says-1483964198

Zhang, X., Min, G., Li, T., Ma, Z., Cao, X., & Wang, S. (2023). AI and blockchain empowered metaverse for web 3.0: Vision, architecture, and future directions. *IEEE Communications Magazine*, *61*(8), 60–66.

Zhu, J., Li, F., & Chen, J. (2024). A survey of blockchain, artificial intelligence, and edge computing for Web 3.0. *Computer Science Review*, *54*, Article 100667.

Zuo, Z. (2023). Development, application, and regulation of Web3.0. *Frontiers in Business, Economics and Management*, *9*(3), 22–27.

## About the Authors

Yaohui Wang is a lecturer at Zhou Enlai School of Government, Nankai University. He has published before in *Politics and Governance*, *Journal of Contemporary China*, *Climatic Change*, and other journals.

Yang Qiu is a PhD candidate at Zhou Enlai School of Government, Nankai University. His research interests include transatlantic relations and security policy.

Politics and Governance
2025 • Volume 13 • Article 10246
https://doi.org/10.17645/pag.10246

cogitatio

ARTICLE

Open Access Journal

# A Tale of Two Metaverses: How America, China, and Europe Are Shaping the "New Internet"

Nora von Ingersleben-Seip

Department of Political Science, University of Amsterdam, The Netherlands

**Correspondence:** Nora von Ingersleben-Seip (n.a.voningerslebenseip@uva.nl)

**Submitted:** 28 February 2025 **Accepted:** 16 July 2025 **Published:** 15 October 2025

**Issue:** This article is part of the issue "Technology and Governance in the Age of Web 3.0" edited by Chang Zhang (Communication University of China), Zichen Hu (London School of Economics and Political Science), and Denis Galligan (University of Oxford), fully open access at https://doi.org/10.17645/pag.i443

## Abstract

The Metaverse, a virtual shared space created by the convergence of physical and virtual reality, is still in its infancy. Yet, China and the EU have already formulated differing visions for the future of the "new internet," and issued policies meant to advance that future. The US has neither articulated a specific vision nor adopted specific policies for the emergent Metaverse but has designated it as a critical technology and promoted its use in military contexts. Additionally, it has implemented a range of policy measures that support the technology industry in general and has therefore allowed its Big Tech companies to make large investments in the Metaverse. In this article, I argue that the divergent stances of the three powers have led to two imagined Metaverses and two actual Metaverses taking shape and competing. In terms of visions, China promotes an industrial Metaverse led by its biggest companies that strengthens the Chinese Communist Party, contributes to economic growth, and to China's geopolitical leadership. In contrast, the EU envisions an open and interoperable Metaverse that respects digital rights and provides opportunities for European companies. Reality contrasts starkly with the European vision, as there is currently a closed, consumer-focused Western version of the Metaverse dominated by American Big Tech and a closed, industry-focused Chinese version dominated by Chinese Big Tech. However, since the Metaverse is still emergent and contested, there is room for policymakers to direct it towards a version that serves more than just commercial or geopolitical interests.

## Keywords

competition; digital platforms; digital sovereignty; geopolitics; Metaverse; political economy

## 1. Introduction

The "Metaverse" has been a buzzword since 2021 (Weinberger, 2022), when American social media company Facebook changed its name to Meta Platforms to reflect its growing focus on becoming a Metaverse company (Meta, 2021). However, there are competing definitions of what the Metaverse actually is (discussed in more detail in Section 2) and—since the Metaverse is still emergent—competing visions of what it ought to become and in what direction its development and use should be steered (discussed in more detail in Section 4). These competing visions are articulated by (potential) users, policymakers in different countries, and individual developers and companies building the Metaverse. Their visions diverge in terms of how open or centralized the Metaverse should be, how it should be governed, who it should benefit, and what role companies and governments should play within it (Gilbert, 2022, p. 1).

In this article, I focus on the competing visions for the Metaverse articulated by policymakers in the US, China, and the EU. I analyze what kind of Metaverse these visions aim to establish, to what extent they have been translated into concrete policies and implemented, and how—and with what consequences—they have shaped current instantiations of the Metaverse. In addition, I analyze to what extent companies, and especially the largest digital platform companies, have shaped the Metaverse—either in alignment or in competition with governments. Thus, in this article, I answer the following research question: *What visions and policies for the development and use of the Metaverse have the US, China, and the EU articulated, and to what extent and with what consequences have these visions and policies shaped the Metaverse?*

I chose the US, China, and the EU as focal points for my analysis. There are certainly other countries that have articulated visions and policies for the Metaverse. Examples are Japan, South Korea, and the United Arab Emirates (Virtual Dimension Center, 2025). My choice is motivated by the fact that the US, China, and the EU (a) are among the most advanced when it comes to formulating policies for the development and use of the Metaverse (in the case of China and the EU); (b) are locked in a fierce rivalry that makes the Metaverse a technopolitical battleground (especially the US and China); and (c) are home to companies that have come the farthest in actually building the Metaverse—in the case of the US and China (Ball, 2022). They are also interesting because they differ widely in terms of the extent to which, and the direction in which, they want to steer the development and use of the Metaverse. The US has not formulated any specific policies for the Metaverse so far (Garcia, 2023) and is letting its domestic digital platform companies develop the Metaverse as they see fit, enabling them to make important decisions about the centralization, governance, and use cases of the Metaverse. The EU, in contrast, has published various policy documents detailing its vision for the Metaverse (European Commission, 2023). All of these documents emphasize that Europe is seeking to build a standards-based, open, and interoperable Metaverse that empowers people, respects the EU's values, and strengthens European industry. China, finally, has both published a detailed strategy for the Metaverse and implemented parts of this strategy. The Metaverse policies of the Chinese Communist Party aim to ensure that Metaverse technologies contribute to China's economic development (Gray & Tang, 2025, p. 2), strengthen the country's technological sovereignty, and cement the power of the Chinese Communist Party (Pohle & Voelsen, 2022).

The US, China, and the EU not only have different visions and policies for the Metaverse but also differ in their ability to shape the development and use of the Metaverse through these policies. The most obvious and important divide among the three powers is the number of domestic Big Tech companies at home in each

geography. This matters because Big Tech companies—such as Alphabet, Amazon, Apple, Meta, and Microsoft in the US and Alibaba, Baidu, Tencent, and Xiaomi in China—are in a prime position to build the Metaverse and make choices about its structure, governance, and use cases (as discussed in Section 4, this is particularly true in the American context, in which the government has so far not put forth any dedicated policies for guiding the development and use of the Metaverse, leaving important decisions to companies). Europe, on the other hand, does not have any Big Tech companies of its own. This means that, at this moment, American and Chinese digital platforms are making crucial decisions shaping the Metaverse, many of which do not align with Europe's vision for this new digital space.

Thus, while policymakers in Brussels envision an open, interoperable Metaverse that safeguards digital rights and empowers the citizenry, American and Chinese Big Tech companies are busy leveraging their dominance in cloud computing, their ownership of data and cutting-edge AI, and their large financial resources to build their own versions of the Metaverse. In the process of colonizing this new digital Frontierland, Big Tech firms are gaining influence over yet another aspect of users' digital lives and building closed technological ecosystems that further increase their ability to collect and monetize user data and suppress market competition.

In what follows, I analyze the visions and policies of the US, China, and the EU regarding the Metaverse. I then explain why these three powers differ in their capabilities to bring these visions to life and how this has shaped the Metaverse, in particular its political economy. Before discussing visions and policies for the Metaverse, however, I will define what the term "Metaverse" means. This is not a straightforward task, as the Metaverse is a complex concept and several competing definitions exist. Rather than adding my own definition to the list, I adopt one of the most widely cited, most complete, and most helpful definitions of the concept, provided by the well-known Metaverse thinker Matthew Ball in his book *The Metaverse: And How It Will Revolutionize Everything* (Ball, 2022, p. 29). I then explain why the US and China are in a much better position to shape the Metaverse than the EU. Finally, I discuss what consequences the influence of the US and China has for the Metaverse.

Efforts to formulate technical standards for the Metaverse, predominantly driven by the EU, may lead the Metaverse down a different path. Right now, however, such efforts are still in their infancy, and it is unclear how impactful they will be (Gilbert, 2022, p. 3). By explaining who is currently shaping the Metaverse, and with what consequences, I contribute to a better understanding of the emerging political economy of the Metaverse. I show that American and Chinese Big Tech companies dominate current instantiations of the Metaverse. European companies play a less prominent role in the Metaverse, and those that thrive do so by using the infrastructures created by American Big Tech, further entrenching the dominance of these US tech giants in the digital economy, with attendant consequences for openness, interoperability, and market fairness.

## 2. Theorizing the Metaverse and the Role of Digital Platform Companies Within It

In this section, I first define what the Metaverse is and how it is currently being used. I then explain how large digital platforms shape the Metaverse and what consequences their involvement has for the political economy of the Metaverse.

### 2.1. Understanding the Metaverse: Definitions, Current Instantiations, and Use Cases

The simplest definition of the Metaverse is that it is a virtual shared space created by the convergence of physical and virtual reality. However, while this definition is brief and provides some insight into the meaning of the term, it fails to capture some important aspects of what the Metaverse really is. Given the complex, multifaceted nature of the concept, defining it is no easy task. Different academic disciplines, such as economics, business, and sociology, offer different definitions (Dwivedi et al., 2022). Recognizing this diversity, Weinberger (2022, p. 322) formulates the following definition based on a meta-analysis of scientific articles from all fields:

> The Metaverse is an interconnected web of ubiquitous virtual worlds partly overlapping with and enhancing the physical world. These virtual worlds enable users who are represented by avatars to connect and interact with each other, and to experience and consume user-generated content in an immersive, scalable, synchronous, and persistent environment. An economic system provides incentives for contributing to the Metaverse.

Weinberger's definition contains many elements of the definition offered by Ball (2022), who writes that the Metaverse is:

> [A] massively scaled and interoperable network of real-time rendered 3D virtual worlds that can be experienced synchronously and persistently by an effectively unlimited number of users with an individual sense of presence, and with continuity of data, such as identity, history, entitlements, objects, communications, and payments. (Ball, 2022, p. 29)

Because the definition by Ball is shorter but at the same time more complete than Weinberger's (for example, it explicitly recognizes that there is continuity of data), I use Ball's definition for the remainder of this article.

It is worth pointing out that the Metaverse, as defined by Ball (or Weinberger for that matter), does not currently exist (Egliston et al., 2024, p. 11). Rather, Ball is describing what the Metaverse *could* be if it reaches its full potential. This does not make his definition any weaker, however. Rather, it aids an understanding of what private companies and, to a certain extent, governments are trying to achieve in this space and why there are such widely differing visions and policies with regard to the Metaverse. It is also notable that Ball speaks of a "network of…virtual worlds," i.e., the Metaverse is not just one virtual world. This reflects the reality that there are currently a number of different virtual worlds for gaming and entertainment purposes as well as for more "serious" pursuits, such as education and training (Buchholz et al., 2022)—which, however, will become interoperable and will allow for continuity of data if Ball's vision is fully realized. At the moment, these virtual worlds are mostly self-contained and non-interoperable (see the last paragraph of the present section for some exceptions). Thus, a Metaverse that is an "interconnected web of…virtual worlds" (Weinberger, 2022, p. 322) does not yet exist (Gilbert, 2022). Instead, as will be discussed in more detail in the case studies in Section 4, there are a number of virtual worlds built atop the infrastructure of the dominant American and Chinese companies that are popular with users in Western markets and in the Chinese market, respectively. The most sensible conceptualization, then, is that of a Western Metaverse underpinned by the infrastructure of American Big Tech and a Chinese Metaverse underpinned by the infrastructure of Chinese Big Tech. It nevertheless makes sense to speak of "the

Metaverse" (singular), just as we speak of "the internet" (singular), despite the existence of billions of websites set up by governments, companies, and individuals (Ball, 2022). While the EU has expressed a strong vision for the Metaverse, there are no Metaverse companies from Europe that could play a leading role in realizing that vision (Gilbert, 2022).

Currently, various activities take place in the Metaverse. These activities can take the form of social, political, or cultural interactions. Some of the most famous events that have taken place in the Metaverse to date include a concert by American musician Travis Scott in Fortnite, which attracted over 12 million live participants (Haasch, 2020); a Metaverse Fashion Week (McKinsey, 2022b); a Sotheby's virtual art auction (Jhala, 2021) in Decentraland; and a Gucci virtual exhibition (McDowell, 2021) in Roblox. Beyond cultural and social events, the Metaverse has also served as a site for political protests. Thus, in 2020, Hong Kong pro-democracy activists set up memorials and created protest art on the platform Animal Crossing: New Horizons to commemorate China's Tiananmen Square massacre (Borak, 2020). This led to China banning Animal Crossing shortly after ("Animal Crossing removed from sale," 2020), showing that beyond being a "playground" for fun social and cultural events, the Metaverse is also a contested political space. This contestation is exemplified by researchers' warning that extremists and terrorist groups are using the Metaverse to spread propaganda and recruit users for their respective causes (Schlegel & Kowert, 2024).

In general, people "use the Metaverse to work, socialize, and play" (Gilbert, 2022, p. 2)—much like the internet. However, the Metaverse provides a user experience that is different from the current internet in that users interact in three-dimensional (3D) immersive digital spaces that fuse the physical and virtual worlds. This allows users to take on different identities and engage in life-like activities in which they would not necessarily partake in the real world. Examples include conducting archival research, racing motorbikes, and fighting with samurai swords (Gilbert, 2022, p. 2). The Metaverse has therefore also opened new revenue streams for businesses and content creators, who can, for example, offer training and education in the Metaverse or make new forms of art and entertainment (Bowles, 2022). It has also enabled new forms of economic transactions utilizing digital currencies and new business models (Ahn et al., 2024)—e.g., the hosting of virtual events and the sale of non-fungible tokens (NFTs) and digital items. Thus, the Metaverse "presents a promising new arena of economic opportunity" for businesses that create "experiences and worlds in a way that platforms currently do not allow" (Bowles, 2022).

It bears repeating that the Metaverse as an "interconnected web of…virtual worlds" (Weinberger, 2022, p. 322) does not currently exist. Instead, the Metaverse at this point comprises both open, decentralized, and closed, self-contained virtual worlds (examples of the former are Decentraland, Somnium, and Fortnite; while examples of the latter are Minecraft and IMVU). These virtual worlds are characterized not only by different levels of centralization but also by different governance models. Thus, Decentraland (owned by the Decentraland Foundation) and Somnium (owned by Somnium Space) are part of the so-called "Web3" movement (Ray, 2023), using blockchain to enable cross-platform identity and ownership of NFTs. In addition, Decentraland is governed by its users through a decentralized autonomous organization. Fortnite is privately owned (by Epic Games) but offers interoperability with other platforms and brings in content from other franchises such as Marvel and Star Wars (Fang, 2024). Decentraland, Somnium, and Fortnite are therefore part of an interconnected virtual ecosystem in which integration with other platforms, applications, or services is the norm. Minecraft (owned by Microsoft) and IMVU (owned by Together Labs), in contrast, are self-contained digital spaces, where most of the content and interactions stay within the

platform itself. Thus, Minecraft and IMVU do not natively support integration with other platforms or persistent digital identities outside their own virtual worlds. This points to a larger rift in the Metaverse: while some companies and users in the Web3 movement would like the Metaverse to be an open, interconnected, and interoperable web of virtual worlds based on the blockchain and governed by users, others are content for the Metaverse to be a collection of self-contained digital spaces that are owned and governed (mostly) by large corporations. The visions of policymakers in China and the EU also diverge on these points, while the US government has not expressed a vision for the Metaverse.

### *2.2. Theorizing the Role of Big Tech Firms in the Metaverse*

Both American and Chinese Big Tech companies are devoting significant resources in the form of engineering talent and financial capital to building the Metaverse, "with an expectation of returns in much less time than it will take to complete the Metaverse" (Gilbert, 2022, p. 4). Venture capitalists have also poured large amounts of money into Metaverse startups (McKinsey, 2022b), but Big Tech firms have several competitive advantages when it comes to capturing opportunities in the Metaverse. For one, given their trillion-dollar market capitalizations, they have the money to continuously make large investments into what some believe will be the "next iteration of the Internet" (Weinberger, 2022, p. 310; see also McKinsey, 2022b), without worrying about whether the Metaverse will quickly gain traction (Kaplan & Haenlein, 2024). Unlike firms that have fewer resources or investors with short time horizons, Big Tech can simply make the necessary (risky) investments to try and capture the significant revenue potential associated with the Metaverse (Dalton, 2024; McKinsey, 2022a; Vigkos et al., 2022), even if this potential takes years to materialize.

Big Tech firms can also leverage their existing users and the data they have collected about them to easily expand into adjacent markets and new technologies, such as the Metaverse. Thus, "network effects and asymmetrical power over data" (Cioffi et al., 2022, p. 821; Kenney & Zysman, 2016), combined with their large financial resources, allow these firms to (a) recognize when a new technology becomes popular; (b) copy the "hot" new technology or buy up the firm(s) that built it; (c) effectively market the new technology to existing users; and (d) squash emerging competitors. Digital platforms generally benefit from both direct network effects, which occur when new users make the platform more valuable for existing users (Grewal, 2008) and data network effects, which stem from the fact that more data—at least up to a point—allow for constant improvements to the algorithms underlying apps, digital services, and smart devices (von Ingersleben-Seip & Georgieva, 2024, p. 333). In other words, digital platforms' "distinctive attributes endow them with extraordinary capacities for expansion" (Cioffi et al., 2022, p. 820).

When it comes to capturing opportunities in the Metaverse, Big Tech firms are further helped by their "infrastructural power" (Kelton et al., 2022; Plantin & Punathambekar, 2019), established most lastingly through their dominance in cloud computing and by their ownership of cutting-edge AI. As Plantin and Punathambekar (2019, p. 164) point out, Big Tech firms have made massive investments in infrastructure projects in recent years, including in "building and maintaining data centers, enhancing telecommunications networks, and [entering] the business of Internet service provision." This, in turn, has enabled them to increase and entrench their power "at every imaginable layer of digital culture" (Plantin & Punathambekar, 2019, p. 164). Particularly their ownership of data centers and their build-up of cloud computing capacity have enabled them to rapidly scale (which has led them to become known as "hyperscalers") and build out the fundamental "socio-technical infrastructures" (van der Vlist et al., 2024, p. 1) supporting their massive

growth and the establishment of "platform capitalism" (Narayan, 2022). Amazon Web Services (AWS), which is the world's most-used cloud platform along with Microsoft Azure and Google Cloud Platform, has been called the "primary operating system of the Internet" (van der Vlist et al., 2024, p. 2). Cloud computing is likely to play a similarly important role in the "new internet"—i.e., the Metaverse—because persistent, immersive, and interactive digital worlds rely on the horsepower, scalability, and flexibility provided by cloud computing (Sundaravadivazhagan et al., 2025). Thus, ownership of cloud platforms provides companies with significant advantages in the Metaverse. Cloud computing also supports the integration of AI and machine learning in Metaverse applications, which in turn allows for the creation of more interactive and responsive environments (Sundaravadivazhagan et al., 2025, p. 88). Given that Big Tech firms are the main developers of cutting-edge AI (van der Vlist et al., 2024, p. 2), they can leverage both their cloud computing capacities and AI prowess to extend their dominance to the Metaverse.

The problems raised by Big Tech's excessive power in Web 2.0 have been extensively debated in the literature. "Platformization" (van Dijck et al., 2018) and "platform capitalism" (Narayan, 2022) actively drive the massive collection and monetization of data (van Dijck et al., 2018), entrench "surveillance capitalism" (Zuboff, 2019), and exploit "data labor" (Jonker, 2025). They further fuel the spread of fake news (e.g., Aïmeur et al., 2023) and political manipulation (e.g., Woolley & Howard, 2018), consolidate market power (e.g., Nuccio & Guerzoni, 2019), and systematically undermine market contestability and fairness (e.g., Tombal, 2022). The digital platforms owned by Big Tech have moreover acquired such power that not having access to them severely limits our social and cultural life (Plantin & Punathambekar, 2019, p. 164) and that they can influence political decisions (Wen, 2023), without democratic accountability.

Until recently, there was a general lack of awareness among policymakers about the negative effects of digital platforms' "rapid rise, expansion, and growing asymmetric power" (Cioffi et al., 2022, p. 820). This has, however, changed in the last few years, resulting in increased scrutiny of digital platforms' role in Web 2.0. In some geographies, notably in the EU, this scrutiny has led to regulatory interventions (such as the EU Digital Markets Act and Digital Services Act) that aim to curb the power of Big Tech. These interventions indicate "a shift in regulatory emphasis from competition (and antitrust) policy and law towards more intensive and encompassing forms of socioeconomic regulation" (Cioffi et al., 2022, p. 820).

Thus, while Big Tech firms are in a prime position to extend their dominance from the context of Web 2.0 into the Metaverse, this is not an inevitability. As of now, the Metaverse is still in its infancy and policymakers have a chance to shape it to ensure it serves the common good rather than just the interests of a few Big Tech firms. As Pohle and Voelsen (2022, p. 13) explain, the "techno-political configuration" of the current internet is the outcome of struggles between different stakeholder groups with different visions. Thus, the internet is a product of the choices that arose from "continuous tensions between processes of centralization and decentralization of the Internet's technical foundations and its governance" (Pohle & Voelsen, 2022, p. 13). Similarly, Greenstein (2015) notes that the transformation of the internet from an academic and military network to a widely used commercial technology was not inevitable but rather resulted from a series of strategic decisions, innovations, and collaborations between public and private actors. Similar dynamics are at work when it comes to the Metaverse. Right now, the deliberate choices of a handful of private firms (predominantly the Big Tech platforms and a number of gaming companies) are decisively shaping the way the "new internet" is developed and used, hampering visions for an open, interconnected Metaverse. However, policymakers can steer the Metaverse in a different direction through

policies that foster openness, interoperability, decentralization, and digital rights. Multi-stakeholder consultations and standard setting play particularly important roles here, as recognized by the European Commission (2023).

In Section 3, I describe my research design and methods. In Section 4, I lay out the Metaverse visions and policies of the US, China, and the EU, explaining how each shapes the Metaverse and with what consequences for openness, interoperability, decentralization, and digital rights.

## 3. Research Design and Methods

This article draws on a comparative qualitative analysis of policy documents and related materials produced by governmental bodies in the EU, the US, and China between 2012 and 2025. The goal was to identify each jurisdiction's vision and governance strategy, particularly because the Metaverse, to a large degree, has not materialized yet (Martini, 2025), and policies can therefore decisively shape how it is developed and used. Thus, the analysis I conducted focused on the frames, strategic priorities, regulatory models, and institutional approaches in each jurisdiction.

For the EU and the US, I included official strategy papers, communications, and regulatory initiatives. In the case of China, due to language limitations, I relied on high-quality secondary sources and English-language reports from think tanks and research institutes. These were cross-referenced with translations and translated summaries of primary Chinese government statements, white papers, and provincial Metaverse industry plans to mitigate potential bias. A summary of key documents analyzed for all three jurisdictions is provided as a Supplementary File.

Additionally, in order to understand how each jurisdiction's vision and policies, as well as the actions of Big Tech, affect the development and use of the Metaverse, I conducted a systematic analysis of the Metaverse technology stack. In line with Narang (2023), who draws on a study by the strategy consulting firm McKinsey (2022b), I conceptualize the stack as consisting of four core layers with several components each (as depicted in Figure 1). The first layer is the Content and Experience Layer, which includes content, applications (apps), and virtual meeting spaces. The second layer is the Platform Layer, which encompasses platforms for those

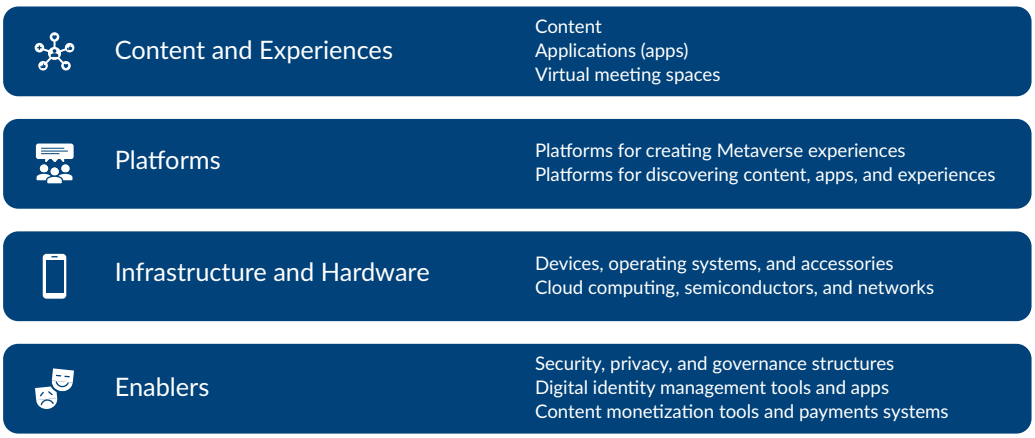



**Figure 1.** The Metaverse technology stack.

creating experiences in the Metaverse and platforms for discovering the content, apps, and experiences in the first layer. The third layer is the Infrastructure and Hardware Layer. This layer consists of the devices, operating systems, and accessories that people use to interact with the Metaverse. It also consists of the infrastructure powering the Metaverse, e.g., cloud computing, semiconductors, and networks. The fourth layer consists of the enablers. Examples include security, privacy, and governance structures; tools and apps for managing digital identities; and tools for accessing the Metaverse economy, monetizing content and experiences, and making payments (McKinsey, 2022b; Narang, 2023). The Metaverse technology stack is depicted in Figure 1.

For each layer, I analyzed which companies from the US, China, and the EU are especially dominant in the layer in question. This analysis allows for a structured assessment of the actors who currently shape the Metaverse and the ways in which they do so. Understanding which actors currently shape the Metaverse, and how, enables me to explain how government visions and policies for the Metaverse either entrench or challenge current power structures and shape the future of this emerging digital space.

To find out which companies currently dominate the Metaverse, I systematically analyzed competition in each layer by studying company reports and press releases of the American Big Tech firms, as well as the Chinese digital giants. To gain insights into the role of smaller companies—as well as European companies—in the Metaverse, I additionally looked at a wide range of industry reports, newspaper articles, and market research describing who does what in the Metaverse. Doing so provided me with an in-depth understanding of the role of American Big Tech companies, Chinese digital giants, European tech firms, and of startups and SMEs from all three jurisdictions, in all four layers of the Metaverse tech stack.

## 4. A Tale of Two Metaverses: American, Chinese, and European Visions and Policies for the "New Internet"

In 2023, the European Commission announced in its Initiative on Virtual Worlds and Web 4.0 (European Commission, 2023) that it seeks a prominent role for European companies in the Metaverse in order to foster the digital sovereignty of the EU. However, it might be difficult for European companies to fulfill the hopes of the Commission. European firms are seeking to carve out a space for themselves, but might find it challenging to compete with American and Chinese platform firms due to their incumbent advantages. American platforms hold significant sway over the development and governance of the Metaverse in markets outside China, while large Chinese platforms dominate the Metaverse in their home market.

### *4.1. America's Vision and Policies for the Metaverse*

In line with its free market ethos (Lippit, 2007) and "market-driven regulatory model" (Bradford, 2023; Lippit, 2007), the US has not adopted a centralized federal policy or articulated a clear vision for the Metaverse (Garcia, 2023). Nonetheless, the Metaverse has been recognized as a critical technology by both the National Science and Technology Council and the Department of Defense, which has begun using Metaverse simulations in training exercises (Aaronson et al., 2023; Copeland et al., 2022). Broader US industrial policies supporting AI, semiconductor design, supply chains, and digital infrastructure indirectly strengthen Big Tech's role in shaping the Metaverse. The absence of a unified federal Metaverse strategy, combined with strong industrial policy in adjacent areas, effectively delegates authority to large platform companies, allowing them to define the "new internet."

American Big Tech firms dominate every layer of the Metaverse stack. In the Content and Experience Layer, Google and Meta leverage their user-generated content (Alphabet, Inc., 2024; Google Ireland Limited, 2024; Thompson, 2022) and recommendation algorithms to build immersive, closed ecosystems that limit competition and centralize control. They also control app ecosystems—Google via Google Play and Apple via the App Store, Apple Music, and other proprietary channels (Apple, 2021; Thompson, 2025). Virtual environments like Meta's Horizon store and Microsoft's Mesh allow these firms to promote their own content and apps over third-party alternatives, reinforcing their dominance. These advantages are bolstered by AI capabilities that drive content personalization, monetization, and advertising (Chen & Huang, 2024; Patel et al., 2023), as well as by closed ecosystems that raise entry barriers (Birch & Cochrane, 2022). US dominance in this layer is further reflected in the role of prominent gaming firms like Epic Games, Electronic Arts, Valve, and Roblox (Radoff, 2024). In the Platform Layer, firms like Meta, Google, and Apple exploit data network effects enabled by user activity data and recommendation algorithms, allowing them to shape visibility and monetization while suppressing rival content (Khanal et al., 2024; Mayer-Schönberger & Ramge, 2018; von Ingersleben-Seip & Georgieva, 2024). In the Infrastructure and Hardware Layer cloud and AI providers such as AWS, Microsoft Azure, and Google Cloud play a central role by offering the compute power and tools needed for Metaverse applications (Sastry et al., 2024). AI models like OpenAI's GPT rely on these services (Microsoft, n.d.), increasing developer dependency on Big Tech. While Nvidia currently dominates AI chips, Big Tech is shifting towards in-house chip design (Mann, 2024; Siegel, 2023), further consolidating control. VR/AR hardware is similarly led by Meta (Quest), Apple (VisionPro), and Microsoft (HoloLens), whose devices collect behavioral and biometric data to enhance user profiling and personalization (Reid, 2022; Tiwari, 2025; Wheeler, 2024). Operating systems like iOS, Android, and Windows provide additional chokepoints, especially as devices like VisionPro and Quest run on proprietary operating systems that restrict interoperability. In the Enablers Layer—covering security, privacy, identity, payments, and governance—Big Tech controls key infrastructure such as login systems (Google, Meta, or Apple), payments (Apple Pay and Meta Novi), and cybersecurity (Google or Microsoft). Their AI capabilities enhance fraud detection and lock-in. With no widespread decentralized identity systems to rival these (Ghosh et al., 2024), the US firms maintain control over user access and data flows across the Metaverse.

Thus, US Big Tech firms are firmly entrenched in all layers of the Metaverse. And while the federal government has not articulated a vision for the Metaverse or issued any specific Metaverse policies, it has implemented over the last few years a whole host of policies that support the development and use of the Metaverse—and the position of American firms within it—in indirect ways. These include, first, President Trump's Executive Orders on AI (The White House, 2020, 2025), which reduce regulatory oversight of AI companies and accelerate the build-out of AI infrastructure. This enables Big Tech companies, which currently lead in AI, to charge ahead unconstrained, which further cements their AI-driven advantages in the Metaverse. Second, the US government has implemented several initiatives, such as the CHIPS and Science Act of 2022 to bolster its semiconductor industry. These have a significant impact on Metaverse development, as advanced chips are foundational to the development and maintenance of immersive virtual environments. Third, the US has implemented a whole host of initiatives to secure and strengthen its supply chains. The most prominent of these is the National Strategy for Global Supply Chain Security, which aims to foster a global supply chain system resilient to evolving threats and hazards (The White House, 2012). Since the Metaverse relies heavily on advanced technologies, such as high-performance computing and graphics processing units, securing the supply chain and ensuring consistent access to the hardware necessary to develop Metaverse companies provides American firms with an edge vis-à-vis foreign competitors who face

challenges in accessing such advanced technologies. Fourth, and importantly, the US has expanded broadband access across the nation, secured digital infrastructure against evolving threats (National Telecommunications and Information Administration, n.d.), and promoted cloud adoption across federal agencies (Digital.gov, 2020). Taken together, these policies expand the potential user base and therefore the demand for the Metaverse; ensure that the foundational networks supporting the Metaverse are robust, reliable, and secure; and create enhanced cloud services that offer scalable and efficient computing resources essential for hosting complex virtual environments. These policies, therefore, further support the leading position of American companies in the Metaverse.

### *4.2. China's Vision and Policies for the Metaverse*

The Chinese government has made the Metaverse one of its technology policy priorities for the coming years. As US think tank New America points out, "China has the most robust metaverse plan backed by significant resources and government intent to be a global leader in this space" (Garcia, 2023). In November 2022, the Chinese Ministry for Industry and Information Technology (MIIT) released a five-year plan solely dedicated to virtual reality (Garcia, 2023), a key tool for creating immersive Metaverse experiences. In addition, China is investing in 100 "core companies" and forming 10 "public service platforms" by 2026 in order to make progress in extended reality (XR, an umbrella term that refers to all immersive technologies that blend the digital and physical worlds) in various industries such as tourism, education, and media (Ye, 2022). At the same time, the Chinese Communist Party is wary of the Metaverse undermining the party's control of the citizenry and has cracked down on the domestic gaming industry to ensure video games do not lead young Chinese people astray (Ball, 2022, p. XIII). Thus, China's main focus is the creation of an industrial Metaverse. Beyond economic opportunities, China's quest for leadership is driven by geopolitical competition: The China Academy of Information and Communications, a state-sponsored think tank, wrote in 2022 that China's Metaverse ambitions should be seen in the context of the US government having designated virtual reality an important industry (Ye, 2022).

Chinese firms have made significant advances in the Metaverse, with Huawei at the technological forefront (Hurun Research Institute, 2024). In the Content and Experience Layer, Tencent and Bytedance dominate domestically through platforms such as WeChat, QQ, and Douyin, while other firms such as NetEase and miHoYo are also active (Radoff, 2024). In the Platform Layer, Tencent is central to content discovery and gaming, with strategic investments in Epic Games and Roblox China, as well as full ownership of Riot Games and the streaming platform Tencent Video (Hou & Gafni, 2022; Wei, 2019). ByteDance combines its AI-powered recommendation engines with its 2021 acquisition of VR company Pico (Kamath, 2022), competing with Meta Quest's ecosystem. Bilibili, a major video streaming platform, supports Metaverse content in ways akin to YouTube or Twitch (Liao, 2017). Alibaba, by contrast, focuses on enterprise Metaverse solutions, developing AI-generated 3D content and infrastructure (Fang, 2023). However, while China has strong players in the Platform Layer, their influence is largely confined to the domestic market due to regulatory and censorship barriers (Global Times, 2021; Kai, 2017) that limit their influence abroad.

In the Infrastructure and Hardware Layer, Alibaba Cloud and Huawei Cloud are key players within China but face bans abroad due to security concerns ("US official says Chinese cloud companies," 2023). Despite homegrown semiconductor firms like SMIC and Cambricon, US sanctions restrict China's access to cutting-edge chipmaking technology. Huawei leads globally in 5G networking and is investing

heavily in low-latency Metaverse infrastructure (Huawei, 2024; Peng, 2023), but its presence is limited in Western markets due to bans in the US, UK, and parts of the EU (Cerulus et al., 2023). Thus, while Chinese firms control critical domestic Metaverse infrastructure—cloud, chips, and 5G—they face major hurdles internationally.

The Enablers Layer in China is shaped by extensive state control (Allen et al., 2022; Guluzade, 2019). Platforms like WeChat and Alipay require real-name verification and use government-approved AI models to monitor transactions and content ("Huawei, Alibaba among companies," 2023; Humphries, 2023). The Chinese government also enforces financial control via the digital yuan (e-CNY), which enables full traceability of Metaverse payments (Huld, 2022). As a result, no user is anonymous, and no Metaverse economy can operate beyond government oversight. These structural differences illustrate how China's Metaverse is shaped by centralized control in contrast to the market-led model of the US.

In line with its "state-driven regulatory model" (Bradford, 2023), the Chinese government has formulated and is in the process of implementing a range of federal policies for the Metaverse. According to Gray and Tang (2025, p. 1), "China's policy agenda for XR is strikingly ambitious." China expects breakthroughs in Metaverse technologies, industrial and administrative applications by 2025, including immersive digital life applications in healthcare, tourism, and education (MIIT, 2023). The Metaverse is seen by Chinese authorities not just as a technological evolution but as a geostrategic opportunity to shape the next generation of the internet on Chinese terms (Faggella, 2022).

Already in 2016, the MIIT founded the Industry of Virtual Reality Alliance (IVRA), a public-private initiative aimed at securing a strategic position for China in the evolving Metaverse (Gray & Tang, 2025, p. 10). The IVRA and other industry alliances aim to create a collaborative ecosystem between government, industry, and academia to accelerate innovation in Metaverse technologies (MIIT, 2023). Thus, the launch of the IVRA was merely the first of several initiatives aimed at fostering industry development of the Metaverse, supported by government investments and incentives. In the years after the IVRA was established, China opened several industry parks and innovation centers aimed at accelerating the development of the Metaverse. Examples include the National Manufacturing Innovation Center for VR, established by the Ministry in 2022, and the Metaverse Industrial Innovation Parks created by the Shanghai Municipal Government. Metaverse-focused industry parks established under the Ministry's guidance aim to foster integration of XR and AI in key sectors, including automotive and aerospace (MIIT, 2023; Tan, 2023).

China is also actively engaged in standard setting for the Metaverse. It is working to create a comprehensive system of national, industry, and group standards for the Metaverse, and encourages international harmonization of these efforts (MIIT, 2023). In line with this ambition, Chinese companies and experts are participating in the Metaverse Standards Forum (The Metaverse Standards Forum, n.d.), which is supposed to play a key role in fostering interoperability in the Metaverse. Additionally, the Chinese government aims to speed up the development of the industrial Metaverse by integrating XR with other advanced technologies such as AI, blockchain, and cloud computing (Gray & Tang, 2025, p. 4). This provides an edge to China's biggest tech companies, which are already leaders in AI and cloud computing.

In September 2023, the MIIT unveiled the ambitious Three-Year Action Plan for the Industrial Innovation and Development of the Metaverse (2023—2025; Interesse, 2023). The plan outlines China's vision for Metaverse

industry development, with one key catalyst being the establishment of three to five clusters that revolve around emerging technologies. The plan details the potential applications of the Metaverse across almost all sectors of the Chinese economy and lays out five key task areas: technology integration, 3D industrial Metaverse, immersive applications, industrial support, and governance mechanisms (MIIT, 2023).

Major initiatives for achieving these objectives include the establishment of a regulatory framework for the Metaverse, the creation of an evaluation and testing system for Metaverse products, and the development of advanced computing infrastructure. While the Chinese government intends to closely guide and oversee developments in the Metaverse (Gray & Tang, 2025, p. 10), the action plan promotes engagement in international standard setting to achieve congruence between global Metaverse governance frameworks and domestic regulations for the Metaverse. It further emphasizes the need for the growth of diverse market players in the Metaverse ecosystem, including innovative small and medium-sized enterprises. Success in aligning global governance frameworks and domestic regulations for the Metaverse would create better conditions for Chinese companies to expand their influence in the Metaverse from the Chinese market (where they currently dominate) to international markets.

### *4.3. Europe's Vision and Policies for the Metaverse*

The European Commission in 2023 proactively adopted a strategy on Web 4.0—the immersive, spatial, AI-driven internet—and virtual worlds (European Commission, 2023). In line with the European "rights-driven regulatory model" (Bradford, 2023) and Europe's quest for digital sovereignty, the strategy emphasizes the importance of interoperability, inclusivity, and respect for digital rights within the emerging Metaverse. The explicit aim of the Commission is to "ensure an open, secure, trustworthy, fair and inclusive digital environment for EU citizens, businesses, and public administrations" (European Commission, 2023). In addition, the Commission emphasizes the business opportunities for European companies, pointing out that the market size for global virtual worlds is expected to grow from €27 billion in 2022 to over €800 billion by 2030.

The European Commission's ambition to ensure that the EU becomes a "world leader" in the Metaverse faces significant challenges, as European firms currently play a limited role across the Metaverse stack. In the Content and Experience Layer, companies like Ubisoft (from France) and Spotify (from Sweden) hold strong positions in gaming and audio content, respectively (Radoff, 2024). Yet, they depend on infrastructure owned by US Big Tech—namely AWS (Amazon), Azure (Microsoft), and Google Cloud—creating structural dependencies that constrain competition and innovation.

In the Platform Layer, Europe lacks major consumer-facing Metaverse platforms. While it is home to firms such as Steam (a firm from the UK focused on gaming discovery), Unity (a game engine from Denmark), and Ubisoft (a Metaverse gaming company from France; Radoff, 2024), these do not match the scale or influence of dominant US or Chinese platforms. In the *Infrastructure and Hardware* Layer, Europe's cloud capabilities remain modest, with OVH Cloud (from France) representing Europe's largest cloud provider (Expert Market Research, 2024). Europe's strengths lie in telecom and chip design: Ericsson (from Sweden) and Nokia (from Finland) are global 5G leaders (Ericsson, 2025; Kadia, 2025) and Nokia also excels in cloud connectivity and AI-driven edge computing (Uitto, 2024), while Graphcore (from the UK) and Arm (originally from the UK but now majority-owned by Japanese investor Softbank) contribute to AI chip architecture and innovation (Silver,

2019; Tarasov, 2023). ST Microelectronics (from France and Italy) specializes in AI chips for automotive and IoT use cases (STMicroelectronics, n.d.). However, none of these firms offer full-stack capabilities comparable to Nvidia or US cloud giants, leaving Europe reliant on American firms for cloud AI processing which is key for a scalable, intelligent, and dynamic Metaverse.

In the Enablers Layer, European companies such as Darktrace (from the UK) and Atos (from France) offer cybersecurity solutions that are compliant with Europe's General Data Protection Regulation (Saunders, 2025), while Thales (from France) and IDNow (from Germany) focus on digital identity and biometric verification (Tanner, 2023). Still, these firms lack the global consumer reach of US competitors (Saunders, 2025). In payments, fintechs like Adyen (from the Netherlands), Klarna (from Sweden), and Revolut (from the UK) lead in real-time and cross-border transactions, but they operate within infrastructures controlled by traditional and US-based financial networks (Farrell & Newman, 2019). In sum, while Europe shows strength in niche areas—particularly in telecom and fintech—its dependence on US infrastructure and platforms constrains its ability to lead in the Metaverse.

The Metaverse is thought to provide massive financial opportunities for companies. As strategy consultancy McKinsey (n.d.) puts it: "With its potential to create up to $5 trillion in value by 2030, the [M]etaverse is too big for companies to ignore." Policymakers similarly have recognized the potential associated with the Metaverse and are seeking to support domestic companies in capturing opportunities related to the development and use of the "new internet." According to Martini (2025, p. 852), European policymakers view the creation and development of the Metaverse as a chance to "secure a leading role in global standards-setting for digital environments." Beyond identifying opportunities, however, policymakers also perceive risks inherent in companies' forays into the Metaverse. Thus, the European Commission's strategy states that Web 4.0 and virtual worlds should respect EU values and principles, creating environments "where people's rights fully apply and where European businesses can thrive" (European Commission, 2023). To achieve these aims, the Commission has identified four key strategy pillars that foster European norms and interests in the Metaverse. The first pillar focuses on empowering people and reinforcing skills through projects funded by the Digital Europe Program (European Commission, 2025a) and, for creators of digital content, the Creative Europe program (European Commission, 2025b).

The second pillar focuses on businesses and aims to support a European Web 4.0 industrial ecosystem. The Commission seeks to address fragmentation by creating an EU ecosystem that brings together the different players of the value chain on virtual worlds and Web 4.0. Likely this year, the Commission will start a Partnership on Virtual Worlds under Horizon Europe to foster excellence in research and draw up an industrial and technological roadmap for virtual worlds. The Commission also aims to empower European creators and media companies to test new creation tools, bring together developers and industrial users, and work with member states to develop regulatory sandboxes for Web 4.0 and virtual worlds (European Commission, 2023).

The third and fourth pillars focus on the actions that governments and the Commission can take to foster virtual public services and to shape global standards for open and interoperable virtual worlds. Concerning the third pillar, the Commission points out that the EU is already investing in major initiatives such as Destination Earth (DestinE; European Commission, 2024), Local Digital Twins for smart communities (European Commission, 2021), or the European Digital Twin of the Ocean (Directorate General for Research

and Innovation, 2024) to enable researchers to further scientific advancements, industries to create precision applications, and public authorities to make well-informed policy decisions. In addition, the Commission has launched two new flagship initiatives: CitiVerse, a digital twin of an immersive urban environment that allows for better city planning and management (European Commission, n.d.-a); and a European Virtual Human Twin (European Commission, n.d.-b), which replicates the human body to support medical decisions and personalized treatment. As regards the fourth pillar, the Commission states that it intends to shape global standards for Web 4.0 by engaging with internet governance stakeholders around the world, to ensure that such standards "will not be dominated by a few big players" (European Commission, 2023). The Commission then reiterates that it hopes to promote standards for the Metaverse that are in line with the EU's visions and values. In other words, the Commission sees the Metaverse as "an economic opportunity that necessitates both government support and oversight" (Gray & Tang, 2025, p. 4). Chances for European companies lie in creating more interoperability and in setting ethical and technical standards for the Metaverse.

However, as Martini (2025, p. 852) points out, the EU has positioned itself more "as an enabler than a critical challenger" of "massive corporate-owned datafication." Thus, currently, the EU is not making progress in promoting a decentralized, interoperable Metaverse based on blockchain technologies. And while the EU is traditionally good at influencing technical standard setting (Büthe & Mattli, 2011), there is not much movement towards technical standards for the Metaverse at the moment (Gilbert, 2022, p. 3). Therefore, the EU is acquiescing to a future where the Metaverse is controlled by US and Chinese Big Tech, with negative consequences for openness, digital rights, and market contestability.

## 5. Conclusion

The Metaverse is still an "emergent phenomenon" (Dolata & Schwabe, 2023, p. 239). Yet, China and the EU have already formulated distinct visions and policy strategies for the future of the "new internet." China has also implemented many of these policies and has made significant progress towards a domestic industrial Metaverse led by the country's Big Tech firms. Europe, on the other hand, has not yet been able to realize its vision of an open, interoperable Metaverse that respects digital rights and opens business opportunities for European companies. The US is "behind the curve" (Aaronson et al., 2023, p. 3) when it comes to specific visions or policies for the Metaverse. Nonetheless, it has implemented several policies that support the technology industry and have enabled its Big Tech firms to extend their dominance from the internet to the Metaverse. Thus, there are currently two competing visions for the future of the Metaverse articulated by China and the EU, and two actual instantiations of the Metaverse dominated by Chinese and American Big Tech firms, respectively. Neither the Chinese nor the American-dominated version of the Metaverse truly fosters openness, digital rights, or market contestability. Technical standard-setting processes (which have the potential to lead to a more open and interoperable Metaverse that provides businesses opportunities for many firms, not just for the largest digital platforms) are, moreover, largely dormant right now (Gilbert, 2022, p. 3).

However, a future in which the Metaverse is closed and dominated by Chinese and American Big Tech (in Chinese and Western markets, respectively) is not an inevitability. The Metaverse is still in its infancy and its "techno-political configuration" (Pohle & Voelsen, 2022, p. 13) can be contested, negotiated, and shaped by political and commercial choices, as was the case for the internet. If policymakers seize the moment and

take decisive action fostering interoperability, digital rights, and market competition, they can still "reorient [the Metaverse] towards humanist values rather than singular interests" (Dolata & Schwabe, 2023, p. 239).

In this article, I make three contributions. First, I examine and compare the Metaverse policies and strategies of the US, China, and the EU. Such a structured, systematic assessment of three different cases allows for more robust cross-country comparisons, which enables the insight that there are currently two different visions of the Metaverse, a European one and a Chinese one. Second, I explain how these divergent visions and policies shape the emergent Metaverse and either challenge or entrench the power of the companies that are currently building the "new internet." Third, I systematically analyze the Metaverse technology stack to figure out which companies dominate each layer of the stack. This analysis reveals that there is currently a Chinese industry-focused version of the Metaverse dominated by Chinese Big Tech and a consumer-focused Western version of the Metaverse dominated by American Big Tech. Overall, my analysis sheds light on the visions for, and contestation of, the Metaverse and contributes to a better understanding of this "hyper digital reality" (Tencent, 2021) and the emerging economic and political dynamics within it.

If visions of the Metaverse as a parallel, virtual plane of existence in which we spend much of our time—and significant chunks of our money—materialize, the firms dominating the Metaverse will not only make huge profits but also "become more powerful than any government" (Sweeney, 2015, as cited in Takahashi, 2016; Ball, 2022). Therefore, it is important to analyze the emergent Metaverse, critically examine its political, social, and economic implications, and understand how both companies and policymakers can steer it in a direction that is beneficial for society. One interesting direction for future research is to figure out how technical standard setting can contribute to an open and interoperable Metaverse, and how the EU can promote efforts to set standards in this realm. If shared technical standards are adopted through multi-stakeholder consultations in transnational standard-setting organizations, this could be a boon for digital rights and market competition in the Metaverse.

## Acknowledgments

I thank the reviewers, who through their constructive criticisms have pushed me to improve this article, and my colleagues on the University of Amsterdam's RegulAite project, with whom I have had many illuminating discussions about the power of Big Tech. I am also deeply grateful to Daniel Mügge and Harry Seip for their helpful feedback on the initial ideas for this article, and to the academic editors of this thematic issue, Chang Zhang, Zichen Hu, and Dennis Galligan, for their thoughtful comments, which allowed me to improve the article further.

## Funding

This work is part of the RegulAite project, hosted by the University of Amsterdam and funded by the Dutch Research Council (NWO, grant number VI.C.211.032). Publication of this article in open access was made possible through the institutional membership agreement between the University of Amsterdam and Cogitatio Press.

## Conflict of Interests

The author declares no conflict of interests.

## Supplementary Material

Supplementary material for this article is available online in the format provided by the author (unedited).

## References


Aaronson, S. A., Zable, A., O'Hara, J. V., & Lutz, M. (2023). *Reality check: Why the U.S. government should nurture XR development*. XR Association and Digital Trade & Data Governance Hub.

Ahn, S., Ellie Jin, B., & Seo, H. (2024). Why do people interact and buy in the Metaverse? Self-expansion perspectives and the impact of hedonic adaptation. *Journal of Business Research*, *175*, Article 114557. https://doi.org/10.1016/j.jbusres.2024.114557

Aïmeur, E., Amri, S., & Brassard, G. (2023). Fake news, disinformation and misinformation in social media: A review. *Social Network Analysis and Mining*, *13*(1), 1–36.

Allen, F., Cai, J., Gu, X., Qian, J., Zhao, L., & Zhu, W. (2022). *Centralization or decentralization? The evolution of state-ownership in China*. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4283197

Alphabet, Inc. (2024). *Form 10-K. Annual Report Pursuant to Section 13 or 15(D) of the Securities Exchange Act of 1934*. https://www.sec.gov/Archives/edgar/data/1652044/000165204425000014/goog-20241231.htm

Animal Crossing removed from sale in China amid Hong Kong protests. (2020, April 13). *BBC*. https://www.bbc.com/news/technology-52269671

Apple. (2021, January 27). *Data privacy day at Apple: Improving transparency and empowering users* [Press release]. https://www.apple.com/newsroom/2021/01/data-privacy-day-at-apple-improving-transparency-and-empowering-users

Ball, M. (2022). *The Metaverse: And how it will revolutionize everything*. Liveright Publishing.

Birch, K., & Cochrane, D. T. (2022). Big tech: Four emerging forms of digital rentiership. *Science as Culture*, *31*(1), 44–58. https://doi.org/10.1080/09505431.2021.1932794

Borak, M. (2020, June 4). Animal Crossing players organize virtual vigils for the Tiananmen Square crackdown. *South China Morning Post*. https://www.scmp.com/abacus/games/article/3087591/animal-crossing-players-organize-virtual-vigils-tiananmen-square

Bowles, E. (2022, December 2). Economic opportunities in the Metaverse: A policy approach. *Meta*. https://about.fb.com/news/2022/12/economic-opportunities-in-the-metaverse

Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press.

Buchholz, F., Oppermann, L., & Prinz, W. (2022). There's more than one metaverse. *I-Com*, *21*(3), 313–324. https://doi.org/10.1515/icom-2022-0034

Büthe, T., & Mattli, W. (2011). *The new global rulers: The privatization of regulation in the world economy*. Princeton University Press. https://doi.org/10.1515/9781400838790

Cerulus, L., Goujard, C., & Roussi, A. (2023, June 15). EU executive to block Huawei from its contracts. *Politico*. https://www.politico.eu/article/huawei-commission-eu-executive-to-block-from-its-contracts

Chen, Y., & Huang, J. (2024). Effective content recommendation in new media: Leveraging algorithmic approaches. *IEEE Access*, *12*, 90561–90570. https://doi.org/10.1109/ACCESS.2024.3421566

Cioffi, J. W., Kenney, M. F., & Zysman, J. (2022). Platform power and regulatory politics: Polanyi for the twenty-first century. *New Political Economy*, *27*(5), 820–836. https://doi.org/10.1080/13563467.2022.2027355

Copeland, C., Garris, G., Hall, M. L., Hagner, C., Shirk, J., & Whitehouse, M. (2022). *Federal technology vision 2022: Government enters the Metaverse*. Accenture. https://www.accenture.com/content/dam/accenture/final/industry/public-service/document/Accenture-Federal-Technology-Vision-2022-Government-Enters-the-MetaverseNew.pdf

Dalton, J. (2024, February 20). Seeing is believing: How AR and VR will transform business and the economy. *PwC*. https://www.pwc.com.au/digitalpulse/report-seeing-believing-ar-vr.html

Digital.gov. (2020). *Cloud and infrastructure*. https://digital.gov/topics/cloud-and-infrastructure

Directorate General for Research and Innovation. (2024, June 13). *European Commission unveils European digital twin of the ocean prototype* [News article]. European Commission. https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/european-commission-unveils-european-digital-twin-ocean-prototype-2024-06-13_en

Dolata, M., & Schwabe, G. (2023). What is the Metaverse and who seeks to define it? Mapping the site of social construction. *Journal of Information Technology*, *38*(3), 239–266. https://doi.org/10.1177/02683962231159927

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C. M. K., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D. P., Gustafsson, A., Hinsch, C., Jebabli, I., . . . Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *66*, Article 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542

Egliston, B., Carter, M., & Clark, K. E. (2024). Who will govern the metaverse? Examining governance initiatives for extended reality (XR) technologies. *New Media & Society*, *27*(6), 3361–3381. https://doi.org/10.1177/14614448231226172

Ericsson. (2025). *Ericsson and Nokia in call to secure Europe's tech future*. https://www.ericsson.com/en/news/2025/1/ericsson-and-nokia-in-call-to-secure-europes-tech-future

European Commission. (n.d.-a). *Citiverse*. https://digital-strategy.ec.europa.eu/en/factpages/citiverse#

European Commission. (n.d.-b). *European virtual human twins initiative for health and care*. https://digital-strategy.ec.europa.eu/en/policies/virtual-human-twins

European Commission. (2021, October 21). *Local digital twins: Forging the cities of tomorrow*. https://digital-strategy.ec.europa.eu/en/library/local-digital-twins-forging-cities-tomorrow

European Commission. (2023, July 11). *Towards the next technological transition: Commission presents EU strategy to lead on Web 4.0 and virtual worlds* [Press release]. https://digital-strategy.ec.europa.eu/en/news/towards-next-technological-transition-commission-presents-eu-strategy-lead-web-40-and-virtual

European Commission. (2024, June 3). *Destination earth factsheet*. https://digital-strategy.ec.europa.eu/en/library/destination-earth-factsheet

European Commission. (2025a, March 28). *Work program 2025-2027 of the digital Europe program (DIGITAL)*. https://digital-strategy.ec.europa.eu/en/library/work-programme-2025-2027-digital-europe-programme-digital

European Commission. (2025b, April 7). *Have your say: Shape the future of EU support for culture and creativity*. https://culture.ec.europa.eu/news/have-your-say-shape-the-future-of-eu-support-for-culture-and-creativity

Expert Market Research. (2024). *Europe cloud computing market growth analysis—Forecast trends and outlook (2025—2034)*. https://www.expertmarketresearch.com/articles/top-cloud-computing-it-companies-in-europe

Faggella, D. (2022, October 4). China's Metaverse advantages: How the West could lose its digital supremacy. *Emerj Artificial Intelligence Research*. https://emerj.com/chinas-metaverse-advantages

Fang, S. (2023, December 5). TikTok—Transform entertainment with AI. *Digital Innovation and Transformation*. https://d3.harvard.edu/platform-digit/submission/tiktok-transform-entertainment-with-ai

Fang, S. (2024, August 12). Fortnite crosses over with Star Wars, Marvel and more. *CBR*. https://www.cbr.com/fortnite-disney-marvel-star-wars-crossover

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, *44*(1), 42–79. https://doi.org/10.1162/isec_a_00351

Garcia, M. (2023, September 25). The forgotten "emerging" technology. *New America*. http://newamerica.org/future-security/reports/the-forgotten-emerging-technology

Ghosh, A., Lavanya, Hassija, V., Chamola, V., & El Saddik, A. (2024). A survey on decentralized Metaverse using blockchain and Web 3.0 technologies, applications, and more. *IEEE Access*, *12*, 146915–146948. https://doi.org/10.1109/ACCESS.2024.3469193

Gilbert, S. (2022, June 20). *The political economy of the Metaverse*. Ifri. https://www.ifri.org/en/memos/political-economy-metaverse

Global Times. (2021, March 31). *Streaming sites Bilibili and Douyu urged to remove vulgar content*. https://www.globaltimes.cn/page/202103/1219918.shtml

Google Ireland Limited. (2024). *Google Ireland Limited DSA audit implementation report 2024—Non-confidential version*. https://storage.googleapis.com/transparencyreport/report-downloads/dsa-audit-google-implementation_2023-8-28_2024-5-31_en_v1.pdf

Gray, J. E., & Tang, W. (2025). The Chinese metaverse: An analysis of China's policy agenda for extended reality (XR). *Policy & Internet*, *17*(1), Article e418. https://doi.org/10.1002/poi3.418

Greenstein, S. (2015). *How the Internet became commercial: Innovation, privatization, and the birth of a new network*. Princeton University Press. https://doi.org/10.1515/9781400874293

Grewal, D. S. (2008). *Network power: The social dynamics of globalization*. Yale University Press. https://www.jstor.org/stable/j.ctt1npvs2

Guluzade, A. (2019, May 7). Explained, the role of China's state-owned companies. *World Economic Forum: Geographies in Depth*. https://www.weforum.org/stories/2019/05/why-chinas-state-owned-companies-still-have-a-key-role-to-play

Haasch, P. (2020, April 24). Travis Scott's "Fortnite" concert was the game's most visually impressive event to date. *Business Insider*. https://www.businessinsider.com/travis-scott-fortnite-concert-video-photo-visually-stunning-the-scotts-2020-4

Hou, R., & Gafni, J. (2022, February 9). Game on? CFIUS clears Chinese video game acquisition. *ForeignInvestmentLinks*. https://www.linklaters.com/en/insights/blogs/foreigninvestmentlinks/2022/february/game-on-cfius-clears-chinese-video-game-acquisition

Huawei. (2024, March 5). *Huawei 5G core named "leader" for the sixth consecutive year by GlobalData, gets full scores in all dimensions for the first time*. https://www.huawei.com/en/news/2024/3/leader-5g-core

Huawei, Alibaba among companies seeking Chinese generative AI approvals. (2023, September 1). *The Economic Times*. https://economictimes.indiatimes.com/tech/technology/huawei-and-alibaba-among-companies-seeking-chinese-generative-ai-approvals/articleshow/103278986.cms?utm_source=chatgpt.com&from=mdr

Huld, A. (2022, September 22). The digital Yuan app—All you need to know about the new E-CNY tool. *China Briefing News*. https://www.china-briefing.com/news/china-launches-digital-yuan-app-what-you-need-to-know

Humphries, M. (2023, August 22). China proposes permanent, unique ID for everyone in the Metaverse. *PCMAG*. https://www.pcmag.com/news/china-proposes-everyone-should-have-a-permanent-unique-id-in-the-metaverse

Hurun Research Institute. (2024). *Hurun China Metaverse companies with the greatest potential 2024*. https://www.hurun.net/en-us/info/detail?num=3DP4671P9XCE

Interesse, G. (2023, September 25). China Metaverse action plan: Three-year national development strategy. *China Briefing News*. https://www.china-briefing.com/news/china-releases-three-year-action-plan-for-metaverse-industry-development

Jhala, K. (2021, June 7). Crypto-crazed Sotheby's launches first virtual gallery in digital metaverse Decentraland—Undefined. *The Art Newspaper*. https://www.theartnewspaper.com/2021/06/07/crypto-crazed-sothebys-launches-first-virtual-gallery-in-digital-metaverse-decentraland

Jonker, J. D. (2025). Is data labor? Two conceptions of work and the user-platform relationship. *Business Ethics Quarterly*, *35*(2), 153–186. https://doi.org/10.1017/beq.2024.25

Kadia, H. (2025, January 13). Ericsson's AI-powered NetCloud assistant transforms enterprise 5G operations. *TeckNexus*. https://tecknexus.com/5gnews-all/ericssons-ai-powered-netcloud-assistant-transforms-enterprise-5g-operations

Kai, P. Y. (2017, July 25). Chinese video site says content purge is "self-censorship." *Asia Times*. http://asiatimes.com/2017/07/chinese-video-site-says-content-purge-self-censorship

Kamath, B. (2022, November 8). TikTok parent bytedance reveals its SOTA recommendation engine. Analytics *India Magazine*. https://analyticsindiamag.com/ai-news-updates/tiktok-parent-bytedance-reveals-its-sota-recommendation-engine

Kaplan, A., & Haenlein, M. (2024). To be or not to be: Will virtual worlds and the Metaverse gain lasting traction? *California Management Review*, *66*(4), 5–22. https://doi.org/10.1177/00081256241259188

Kelton, M., Sullivan, M., Rogers, Z., Bienvenue, E., & Troath, S. (2022). Virtual sovereignty? Private internet capital, digital platforms and infrastructural power in the United States. *International Affairs*, *98*(6), 1977–1999. https://doi.org/10.1093/ia/iiac226

Kenney, M. F., & Zysman, J. (2016). The rise of the platform economy. *Issues in Science and Technology*, *32*(3). https://issues.org/rise-platform-economy-big-data-work

Khanal, S., Zhang, H., & Taeihagh, A. (2024). Why and how is the power of Big Tech increasing in the policy process? The case of generative AI. *Policy and Society*, *44*(1), 52–69. https://doi.org/10.1093/polsoc/puae012

Liao, R. (2017, November 7). How this Chinese video company is thriving on youth-generated content. *CFI*. https://chinafilminsider.com/bilibili-and-regulation-youth-generated-content

Lippit, V. D. (2007). *Capitalism*. Routledge. https://doi.org/10.4324/9780203965641

Mann, T. (2024, February 2). Untangling Meta's plan for its homegrown AI chips, set to actually roll out this year. Meta to deploy custom AI chips alongside AMD, Nvidia GPUs. *The Register*. https://www.theregister.com/2024/02/02/meta_ai_chips/

Martini, M. (2025). Materializing corporate futures: How the EU navigated the Metaverse hype. *Information, Communication & Society*, *28*(5), 852–869. https://doi.org/10.1080/1369118X.2024.2428331

Mayer-Schönberger, V., & Ramge, T. (2018). *Reinventing capitalism in the age of big data*. Basic Books.

McDowell, M. (2021, May 17). Inside Gucci and Roblox's new virtual world. *Vogue Business*. https://www.voguebusiness.com/technology/inside-gucci-and-robloxs-new-virtual-world

McKinsey. (n.d.). *Value creation in the metaverse*. https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/value-creation-in-the-metaverse

McKinsey. (2022a, June 15). *Meet the metaverse: Creating real value in a virtual world*. https://www.mckinsey.com/about-us/new-at-mckinsey-blog/meet-the-metaverse-creating-real-value-in-a-virtual-world

McKinsey. (2022b, August 17). What is the metaverse and where will it lead next? *McKinsey & Company*. https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-the-metaverse

Meta. (2021). *Introducing Meta: A social technology company*. https://about.fb.com/news/2021/10/facebook-company-is-now-meta

Metaverse Standards Forum. (n.d.). *The Metaverse Standards Forum*. https://metaverse-standards.org

Microsoft. (n.d.). *Discover the benefits of Azure OpenAI*. https://azure.microsoft.com/en-us/products/ai-services/openai-service

Ministry of Industry and Information Technology. (2023). *Three-year action plan for the innovative development of the metaverse industry (2023-2025) in China (translation by Virtual Dimension Center Fellbach)*. https://www.vdc-fellbach.de/en/knowledge-database/national-metaverse-strategies-worldwide/china-metaverse-strategy

Narang, N. K. (2023). Mentor's musings on role of standards, regulations & policies in navigating through Metaverse and its future avatars. *IEEE Internet of Things Magazine*, *6*(1), 4–11. https://doi.org/10.1109/MIOT.2023.10070410

Narayan, D. (2022). Platform capitalism and cloud infrastructure: Theorizing a hyper-scalable computing regime. *Environment and Planning A: Economy and Space*, *54*(5), 911–929. https://doi.org/10.1177/0308518X221094028

National Telecommunications and Information Administration. (n.d.). *Digital Infrastructure Resilience*. https://www.ntia.gov/programs-and-initiatives/digital-infrastructure-resilience

Nuccio, M., & Guerzoni, M. (2019). Big data: Hell or heaven? Digital platforms and market power in the data-driven economy. *Competition & Change*, *23*(3), 312–328. https://doi.org/10.1177/1024529418816525

Patel, S., Patel, R., Sharma, R., & Patel, D. (2023). Enhancing user engagement through AI-powered predictive content recommendations using collaborative filtering and deep learning algorithms. *International Journal of AI ML Innovations*, *12*(3), 1–24. https://ijoaimli.com/index.php/v1/article/view/11

Peng, G. (2023, February 1). Four core network capabilities that enable the Metaverse. *Huawei*. https://www.huawei.com/en/huaweitech/publication/202207/core-network-metaverse-capabilities

Plantin, J.-C., & Punathambekar, A. (2019). Digital media infrastructures: Pipes, platforms, and politics. *Media, Culture & Society*, *41*(2), 163–174. https://doi.org/10.1177/0163443718818376

Pohle, J., & Voelsen, D. (2022). Centrality and power. The struggle over the techno-political configuration of the Internet and the global digital order. *Policy & Internet*, *14*(1), 13–27. https://doi.org/10.1002/poi3.296

Radoff, J. (2024, January 18). Market map of the Metaverse. *Building the Metaverse*. https://medium.com/building-the-metaverse/market-map-of-the-metaverse-8ae0cde89696

Ray, P. P. (2023). Web3: A comprehensive review on background, technologies, applications, zero-trust architectures, challenges and future directions. *Internet of Things and Cyber-Physical Systems*, *3*, 213–248. https://doi.org/10.1016/j.iotcps.2023.05.003

Reid, J. (2022, October 15). Meta Quest Pro vs HoloLens 2—Consumer vs enterprise? *GoHere*. https://www.mixyourreality.com//insights/meta-quest-pro-enterprise-or-consumer

Sastry, G., Heim, L., Belfield, H., Anderljung, M., Brundage, M., Hazell, J., O'Keefe, C., Hadfield, G. K., Ngo, R., Pilz, K., Gor, G., Bluemke, E., Shoker, S., Egan, J., Trager, R. F., Avin, S., Weller, A., Bengio, Y., & Coyle, D. (2024). *Computing power and the governance of artificial intelligence*. Arxiv. https://arxiv.org/pdf/2402.08797

Saunders, T. (2025, January 9). UK's Darktrace turns 'more acquisitive' with Cado Security deal. *The Times*. https://www.thetimes.com/business-money/companies/article/uks-darktrace-turns-more-acquisitive-with-cado-security-deal-pbxs6hz8r

Schlegel, L., & Kowert, L. (2024). *Gaming and extremism: The radicalization of digital playgrounds*. Routledge; CRC Press. https://www.routledge.com/Gaming-and-Extremism-The-Radicalization-of-Digital-Playgrounds/Schlegel-Kowert/p/book/9781032482996

Siegel, J. (2023, November 15). With a systems approach to chips, Microsoft aims to tailor everything 'from silicon to service' to meet AI demand. *Microsoft*. https://news.microsoft.com/source/features/ai/in-house-chips-silicon-to-service-to-meet-ai-demand

Silver, J. (2019, August 27). Inside the UK unicorn that's about to become the Intel of AI. *Wired*. https://www.wired.com/story/graphcore-ai-intelligence-processing-unit

STMicroelectronics. (n.d.). *Product portfolio*. https://www.st.com/content/st_com/en/browse/product-portfolio.html

Sundaravadivazhagan, B., Balsubramaniam, S., Pethuru, R., & Shanta Kumari, S. (2025). *Applying Metaverse technologies to human-computer interaction for healthcare*. CRC Press.

Takahashi, D. (2016, December 9). The DeanBeat: Epic graphics guru Tim Sweeney foretells how we can create the open Metaverse. *VentureBeat*. https://venturebeat.com/games/the-deanbeat-epic-boss-tim-sweeney-makes-the-case-for-the-open-metaverse

Tan, M. (2023, November 28). China announces its 2025 actions for Metaverse. *TaylorWessing*. https://www.taylorwessing.com/en/insights-and-events/insights/2023/09/china-announces-its-2025-actions-for-metaverse

Tanner, B. (2023, October 23). Thales brings passwordless fingerprint authentication to the enterprise. *Intelligent CIO North America*. https://www.intelligentcio.com/north-america/2023/10/23/thales-brings-passwordless-fingerprint-authentication-to-the-enterprise

Tarasov, K. (2023, November 9). How Arm is gaining chip dominance with its architecture in Apple, Nvidia, AMD, Amazon, Qualcomm and more. *CNBC*. https://www.cnbc.com/2023/11/09/how-arm-gained-chip-dominance-with-apple-nvidia-amazon-and-qualcomm.html

Tencent. (2021). *The infinite possibilities of video games*. https://www.tencent.com/en-us/articles/2201154.html

The White House. (2012). *National strategy for global supply Chain security*.

The White House. (2020). Promoting the use of trustworthy artificial intelligence in the federal government. *Federal Register*. https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government

The White House. (2025). Executive order on removing barriers to American leadership in artificial intelligence. *Federal Register*. https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence

Thompson, B. (2022, April 12). DALL-E, the Metaverse, and Zero Marginal Content. *Stratechery*. https://stratechery.com/2022/dall-e-the-metaverse-and-zero-marginal-content

Thompson, B. (2025, May 5). Platform power is underrated. *Stratechery*. https://stratechery.com/2025/platform-power-is-underrated

Tiwari, A. (2025, February 27). Meta scores 73% market share but Apple Vision Pro is the trendsetter in VR/MR space. *Neowin*. https://www.neowin.net/news/meta-scores-73-market-share-but-apple-vision-pro-is-the-trendsetter-in-vrmr-space

Tombal, T. (2022). Ensuring contestability and fairness in digital markets through regulation: A comparative analysis of the EU, UK and US approaches. *European Competition Journal*, *18*(3), 468–500. https://doi.org/10.1080/17441056.2022.2034331

Uitto, T. (2024, September 18). Nokia and partners are driving the fusion of AI, Cloud and RAN. *Nokia*. https://www.nokia.com/blog/nokia-and-partners-are-driving-the-fusion-of-ai-cloud-and-ran

US official says Chinese cloud companies like Huawei and Alibaba Cloud could pose security threat. (2023, April 27). *The Straits Times*. https://www.straitstimes.com/world/united-states/us-official-says-chinese-cloud-companies-like-huawei-and-alibaba-cloud-could-pose-security-threat

van der Vlist, F., Helmond, A., & Ferrari, F. (2024). Big AI: Cloud infrastructure dependence and the industrialisation of artificial intelligence. *Big Data & Society*, *11*(1). https://doi.org/10.1177/20539517241232630

van Dijck, J., Poell, T., & de Waal, M. (2018). *The platform society*. Oxford University Press.

Vigkos, A., Bevacqua, D., Turturro, L., Kuehl, S., Fox, T., Diestre, P., & Sørensen, S. Y. (2022). *VR/AR industrial coalition: Strategic paper*. Publications Office of the European Union. https://data.europa.eu/doi/10.2759/197536

Virtual Dimension Center. (2025). *National Metaverse strategies worldwide comparison* [Data set]. https://www.vdc-fellbach.de/en/knowledge-database/national-metaverse-strategies-worldwide

von Ingersleben-Seip, N., & Georgieva, Z. (2024). Old tools for the new economy? Counterfactual causation in foreclosure assessment and choice of remedies on data-driven markets. *Journal of Antitrust Enforcement*, *13*(2), 328–352. https://doi.org/10.1093/jaenfo/jnae042

Wei, H. (2019, May 20). Tencent, Roblox in strategic partnership. *China Daily*. https://global.chinadaily.com.cn/a/201905/30/WS5cef31b5a3104842260be9d2.html

Weinberger, M. (2022). What is Metaverse?—A definition based on qualitative meta-synthesis. *Future Internet*, *14*(11), Article 310. https://doi.org/10.3390/fi14110310

Wen, Y. (2023). Rightful resistance: How do digital platforms achieve policy change? *Technology in Society*, *74*, Article 102266. https://doi.org/10.1016/j.techsoc.2023.102266

Wheeler, K. (2024, November 28). *US invests billions in Intel for domestic chip production*. https://technologymagazine.com/articles/us-invests-billions-in-intel-for-domestic-chip-production

Woolley, S. C., & Howard, P. N. (2018). *Computational propaganda: Political parties, politicians, and political manipulation on social media*. Oxford University Press.

Ye, J. (2022, November 1). China aims to ship 25 million virtual reality devices by 2026. *Reuters*. https://www.reuters.com/technology/china-aims-ship-25-million-virtual-reality-devices-by-2026-2022-11-01

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

## About the Author

Nora von Ingersleben-Seip is a postdoctoral researcher at the University of Amsterdam, working on the RegulAite Project. She studies how emerging digital technologies are governed at national, European, and international levels, and how governance frameworks interact with broader geopolitical dynamics.

Politics and Governance
2025 • Volume 13 • Article 10239
https://doi.org/10.17645/pag.10239

cogitatio

ARTICLE

Open Access Journal

# Virtual Worlds, Real Politics: A Cross-National Comparative Study of Metaverse Policy Approaches

Chang Zhang and Lexuan Wang

School of Government and Public Affairs, Communication University of China, China

**Correspondence:** Chang Zhang (changzhang@cuc.edu.cn)

**Submitted:** 28 February 2025 **Accepted:** 4 September 2025 **Published:** 20 November 2025

**Issue:** This article is part of the issue "Technology and Governance in the Age of Web 3.0" edited by Chang Zhang (Communication University of China), Zichen Hu (London School of Economics and Political Science), and Denis Galligan (University of Oxford), fully open access at https://doi.org/10.17645/pag.i443

## Abstract

While market sentiment toward the metaverse has cooled, states continue to promulgate metaverse policies with notable urgency—a paradox that signals the technology's ascendance as a critical theater of geo-technological rivalry in the emergent Web 3.0 landscape. Drawing upon a systematic content analysis of 34 policy documents issued across major economies and regions between 2021 and 2024, this study interrogates the strategic orientations underpinning these initiatives and traces the structural determinants shaping divergent national trajectories. Our analysis reveals that while metaverse policies across jurisdictions converge on three core imperatives (advancing foundational technologies, catalyzing sectoral applications, and establishing regulatory guardrails), national priorities diverge markedly in emphasis and strategic intent. To fully capture these distinctions, we developed a four-fold typology: techno-economic vanguards, industrial innovators, transformative opportunists, and regulatory vigilants. This study reveals that metaverse policy architectures are fundamentally conditioned by strategic positioning, technological endowments, and industrial composition. While leading powers such as China and the United States primarily wield the metaverse to consolidate technological hegemony and economic preeminence, middle powers with vibrant cultural industries, particularly Japan, South Korea, and France, tend to seize upon the metaverse as an instrument for amplifying cultural influence and sustaining competitive advantage in the global attention economy. Resource-rich economies perceive it as a transformative engine for economic diversification, embracing expansive, forward-leaning strategies that anticipate structural shifts in global production. The European Union, by contrast, maintains its characteristic regulatory posture, extending its precautionary governance framework to this novel domain with deliberate circumspection. This inquiry contributes to the emerging scholarship on metaverse governance while enriching comparative analyses of techno-political regimes, demonstrating how political-economic structures and geopolitical imperatives fundamentally configure state responses to transformative technologies.

**Keywords**
artificial intelligence; comparative policy analysis; metaverse; technology governance

## 1. Introduction

In October 2021, Facebook's rebranding as Meta did more than signal a corporate pivot—it epitomized the tech industry's tendency to mythologize the metaverse as the next frontier of digital life. Mark Zuckerberg's vision of "an embodied internet" (Meta, 2021) served less as a concrete roadmap and more as a grand narrative that fuelled investor and public hype. Giants such as Nvidia, Microsoft, and Roblox rushed to claim their stake in this nebulous virtual realm, projecting an image of seamless convergence between physical and virtual worlds. Yet, this speculative bubble quickly revealed cracks and, by early 2022, Google Trends already indicated waning public interest, exposing a stark disjunction between utopian promises and the harsh realities of immature technology and underdeveloped infrastructure. As Vidal-Tomás (2023) critically observes, the metaverse is trapped in a recurring "hype-disillusion cycle" that threatens its purported economic and social viability.

Despite its frequent portrayal as a cohesive digital future, the metaverse remains an unstable and contested signifier. Rather than treating it as a unified or coherent technological object, this study understands the metaverse as a discursive placeholder—a floating signifier that aggregates diverse aspirations and anxieties across virtual reality, Web 3.0 infrastructures, AI-driven simulations, and digital twin technologies. In this view, the metaverse is not a fixed endpoint but a techno-political imaginary shaped by narratives of innovation, crisis, and control (Mosco, 2023). This ambiguity is particularly visible amid market contraction and strategic rebranding, as illustrated by Meta's pivot toward AI and the decline of major metaverse ventures. It is further reinforced by decentralized Web 3.0 developments (Calzada, 2024), which significantly shape digital governance and raise unresolved questions for national frameworks regarding asset ownership, interoperability, and digital sovereignty.

More troubling are the ethical and security dilemmas embedded in the metaverse's design—its immersive, anonymous, and often unregulated spaces have become fertile ground for fraud, cyberbullying, surveillance, and data manipulation. These phenomena intensify pressing questions about digital sovereignty and governance, yet remain insufficiently addressed by both corporations and states (Chen et al., 2025; Shin & Park, 2025). In this context, the persistent push by states to develop metaverse strategies cannot be reduced to naive economic optimism. Instead, it must be understood as a calculated geopolitical maneuver, wherein the metaverse becomes a new arena for techno-political control and strategic rivalry.

Why do states keep issuing metaverse policies despite market decline? This persistence reflects the institutional logic of anticipatory governance and symbolic policymaking. Rather than focusing on immediate implementation, many national strategies function as tools for shaping long-term industrial positioning, preserving technological credibility, and securing bureaucratic legitimacy. Even amid commercial stagnation or technological setbacks, digital policy agendas endure, sustained by sunk costs, policy path dependencies, and the imperative to signal future readiness. This durability is further reinforced by consultancies, think tanks, and long-established digital ministries that benefit from keeping the metaverse on the policy agenda. For example, jurisdictions such as South Korea, China, and Dubai have unveiled ambitious national or regional metaverse strategies, signaling a desire to shape—and potentially dominate—emergent digital

ecosystems. As Gong (2024) notes, such efforts are often driven by dual objectives: promoting digital economic growth and aligning next-generation technologies with national power projections. In contrast, the United States and the European Union have adopted a more cautious stance—focusing less on industrial promotion and more on regulating extended reality technologies to manage emerging risks. These divergent approaches illustrate how the metaverse has become a contested arena where techno-industrial ambitions, geopolitical interests, and symbolic power converge, often masking deeper structural asymmetries and ideological alignments with digital market structures.

This study responds to these tensions by systematically analyzing 34 metaverse policy documents issued by 13 national and regional jurisdictions between 2021 and 2024. Through content analysis, it poses two questions: (a) What political, economic, and strategic factors drive the formulation of national metaverse policies? (b) How does the metaverse, as a nascent digital ecosystem, reconfigure geopolitical power dynamics? To answer these questions, this article proposes a typology of four national approaches: Techno-economic vanguards, industrial innovators, transformative opportunists, and regulatory vigilants, which link policy variations to underlying political-economic and geopolitical structures. By doing so, it challenges the prevailing techno-optimism and contributes to a more critical understanding of how states engage with immersive digital technologies amid broader struggles over global digital governance.

## 2. Literature Review

### *2.1. Mapping the Terrain of Digital Governance*

Digital governance comprises the frameworks, policies, and institutional mechanisms that guide the development, deployment, and societal integration of digital technologies, including algorithms, blockchain, extended reality, virtual reality, AI, and broader Web 3.0 ecosystem (Erkut, 2020). It spans a spectrum of policy tools, from innovation incentives to ethical and legal regulations, requiring multi-stakeholder coordination to align technologies with societal values (Van Dijck, 2021). Meanwhile, the concept of digital sovereignty—focusing on state control over digital infrastructures and data—has become central to governance debates (Moerel & Timmers, 2021). These dynamics highlight the intersection of innovation, rights protection, and geopolitical considerations in rapidly evolving technological landscapes. To explore their practical application, this study focuses on three key domains: steering technological innovation, promoting industrial diffusion, and establishing ethical and legal safeguards.

- *Steering Innovation to advance cutting-edge technologies*: Governments play a crucial role in fostering technological advancement by implementing national research agendas, funding programs, and creating institutional frameworks that align with national priorities such as economic competitiveness and societal resilience. In China, digital governance has significantly enhanced government capabilities, particularly in areas like dispute resolution and stability maintenance in the digital era (Hu & Zhang, 2023). Simultaneously, emerging technologies are reshaping governance by enhancing service delivery and decision-making processes. Algorithmic technologies, for instance, enable automated systems that improve control and coordination while fostering trust (Hanisch et al., 2023), while blockchain supports decentralized decision-making, promoting greater transparency and efficiency (Kassen, 2025). Ultimately, as Milakovich (2021) highlights, these innovations aim to enhance both governmental operations and public service delivery.

- *Industrial and economic policies to promote the diffusion and adoption of digital technologies*: These policies include infrastructure investments, startup ecosystem development, and workforce training to achieve platform sovereignty and strategic autonomy in digital markets (Pohle & Santaniello, 2024). In the Web 3.0 era, nations—particularly latecomer economies—prioritize the creation of interoperable platforms and virtual economies to secure leadership in the global digital economy (Foster & Azmeh, 2020). In contrast, the European Union focuses on regulatory measures to counteract the market dominance of global tech giants (Martini, 2025), while the United States emphasizes market-driven approaches. Bradford (2023) categorizes digital governance into three regulatory models—market-driven, state-driven, and rights-driven—highlighting the interplay between economic ambitions and geopolitical strategies in shaping governance systems.
- *Legal and ethical frameworks that manage the societal impacts of digital technologies*: These frameworks address various risks, including power imbalances, privacy and security concerns, the digital divide, disinformation, and cybersecurity threats (Erkut, 2020; Hanisch et al., 2023). Legal and regulatory instruments, such as the EU's GDPR or sector-specific extended reality standards, aim to ensure accountability and build trust in digital ecosystems, especially as data flows and user interactions become increasingly pervasive (Hine et al., 2024). At the same time, ethical governance emphasizes key principles, including autonomy and consent, fairness and non-discrimination, transparency and trust, as well as sustainability and security (Eke & Stahl, 2024), as advocated by the Council of Europe's guidelines on digital human rights (Yeung, 2018). These legal and ethical mechanisms are essential for aligning with democratic values and sustaining public trust in governance.

### *2.2. Approaching Metaverse Governance: "Metaverse as Industry" vs. "Metaverse+"*

The metaverse, a fusion of virtual and physical realms, is a key driving force behind Web 3.0. It fundamentally reshapes digital interactions and labor dynamics (Wang et al., 2025), while also raising concerns about privacy, security, and data governance (Eltanbouly et al., 2025). As the metaverse continues to expand, governance frameworks have evolved through the joint efforts of governments, civil society, and industry stakeholders, with particular emphasis on four central issues: privacy protection, safety and inclusion, fair competition, and the regulation of commercialization (Egliston et al., 2025). In this rapidly changing landscape, states are at the forefront of metaverse governance, focusing on the technological infrastructure, platform functions, and governance models (Mosco, 2023). To bridge the gap between visionary goals and real-world implementation, states have introduced precautionary regulations (Martini, 2025), reinforced oversight mechanisms (Kshetri et al., 2024), and are actively competing to set global standards (Yang, 2023).

The governance of the metaverse requires analytical clarity regarding its ontological status. The first perspective views the metaverse as a self-contained industry, emerging within the digital economy as a distinct sector characterized by new forms of economic activity and market competition. As a newly emerging sector within the digital economy, the metaverse serves as a hub for financial innovation that attracts international investment and drives competitive development (Vidal-Tomás, 2023). Major technology companies such as Meta, Microsoft, and NVIDIA have made significant investments in this domain, exploring novel business models and immersive virtual experiences (Dolata & Schwabe, 2023).

However, with the initial hype surrounding the metaverse subsiding, its significance as a standalone industry has notably declined (Martini, 2025). A more enduring and policy-relevant interpretation conceptualizes the

metaverse as an intermediary infrastructure—what may be termed "Metaverse+"—that connects users, services, data, and devices across both virtual and physical spaces, thereby activating and empowering the development of other sectors through technological innovation (Parcu et al., 2023). The Metaverse+ perspective not only links immersive technologies to traditional sectors but also intersects with Web 3.0 governance issues, including decentralized identity, tokenized assets, cross-platform interoperability, and data flows. By situating the metaverse within a Web 3.0 ecosystem, this approach explores how decentralized protocols, smart contracts, and DAO-based governance shape the management of digital assets, user identities, and platform rules across virtual environments (Hanneke et al., 2025). This shift in perspective helps explain why many governments continue to invest in metaverse-related initiatives: not for its industrial value alone, but for its potential to catalyze innovation, connectivity, and transformation across other strategic domains. In this framework, governance practices can be categorized into several domains:

- *Commercial applications*: Technologies such as non-fungible tokens (NFTs) and blockchain underpin secure virtual transactions and asset tokenization. Luxury brands such as Gucci and Louis Vuitton have embraced immersive virtual stores and NFT experiences (Sayem, 2022), enriching consumer engagement and transforming retail dynamics. These innovations are reshaping consumer experience and driving transformation across retail value chains (Russo et al., 2023).
- *Urban governance and public services*: Smart city initiatives utilize metaverse environments for urban planning, data simulation, and participatory governance. Digitizing cultural heritage and developing virtual government platforms further expand public service accessibility and enhance civic participation (Buragohain et al., 2024). Importantly, the metaverse offers a new channel to engage younger generations in public affairs and foster greater democratic transparency (Kshetri et al., 2024).
- *Diplomacy and military innovation*: The metaverse's geopolitical implications are evident, as Barbados became the first country to establish a diplomatic embassy within this virtual space (Grincheva, 2023). On the military front, applications include cognitive warfare simulations and AI-integrated training systems, exemplified by the US Department of Defense's adoption of the Project Maven Smart System (Vold, 2024).

To compare these two models, the Metaverse as Industry model focuses on its economic potential, with governments viewing it as a new sector for investment and competition. In contrast, the Metaverse+ model treats the metaverse as an intermediary infrastructure that facilitates and enhances the development of other sectors through technological innovation. Following the Metaverse+ framework, China integrates the metaverse in a way comparable to the "Internet+" national strategy (Jing & Li, 2019). This integration aligns the metaverse with China's technological ambitions, cultural policies, and governance strategies (Negro & Savina, 2025). Similarly, South Korea—with its capital Seoul—strives to become the world's first fully metaverse city, leveraging the metaverse to enhance its global presence (De Almeida, 2023). As Gray and Tang (2025) highlight, the metaverse is not only a technological system but also a geopolitical arena, driving nations to invest in it for both economic development and geopolitical influence.

### *2.3. Why States Invest in Metaverse Governance?*

Traditional international relations theories provide ample explanations for why states invest in technological governance. These theories attribute the motivations behind states' investments in emerging technologies to factors across political, economic, and cultural dimensions. The motivations behind states' investments

in emerging technologies, as well as the formulation of industrial policies and regulatory measures, can be summarized into three key factors: hegemonic maintenance or aspiration, economic-industrial advantage, and cultural-institutional factors.

For great powers, investing in the governance of the metaverse is primarily aimed at securing a strategic advantage, driven by geopolitical interests and the pursuit of dominance in the emerging digital economy. Classical realists, such as Morgenthau (1985, pp. 124–141), assert that technology constitutes the material foundation of national power, influencing both defense capabilities and global posture through technological superiority. Building on this, Gilpin (1981, p. 175) contends that hegemonic states must maintain technological leadership to sustain dominance, while rising powers use innovation and diffusion to challenge the existing order. This theoretical framework informs the ongoing US–China rivalry, where the competition for control over foundational digital technologies—such as those enabling the metaverse—has become central to shaping the future of global production and embedding strategic interests within digital infrastructure frameworks. By controlling standard-setting, cybersecurity regimes, and data sovereignty frameworks, the US and China are institutionalizing their visions of digital governance through a technologically designated metaverse (Gong, 2024), ensuring long-term influence and reinforcing their geopolitical dominance.

For middle powers, investment in metaverse governance centers on boosting economic competitiveness and promoting sustainable growth. Rather than pursuing global dominance, middle powers aim to secure regional leadership and reinforce sectoral competitive advantages through governance frameworks (Porter, 1990, p. 172). This is because middle powers often concentrate their governance resources in areas of historical strength—such as petroleum, pharmaceuticals, and precision engineering—where they possess regulatory capacity and credibility (Samuels, 1994, p. 58). Countries like Germany and Japan, through their automotive, electronics, and telecommunications sectors, establish de facto standards and extend industrial influence across borders (Kahler, 2017). In the metaverse, Germany leverages its traditional manufacturing strength, while Japan focuses on cultural industries. In cases where economies rely heavily on a single industry—such as oil-dependent ones like Saudi Arabia—the metaverse acts as a catalyst for transformation, facilitating a shift from traditional sectors, such as petroleum, towards diversified technology-driven industries and promoting sustainable economic growth.

States also invest in digital governance to institutionalize normative values that reflect their domestic cultural contexts. Grounded in historical, legal, and societal frameworks, this approach prioritizes governance preferences rooted in national identity rather than power or market forces. As Keohane and Nye (1977) argue, governance in the modern world increasingly occurs through institutional networks. This aligns with Jasanoff's (2015) notion of "sociotechnical imaginaries," where governance is shaped by cultural contexts. The EU exemplifies this with its "normative power Europe" thesis, promoting values like human rights and privacy through standards (Manners, 2002). The GDPR, described as "a key element of European identity" (Schimmelfennig, 2001), demonstrates how privacy is used to project normative power globally. This global phenomenon is termed the "Brussels Effect" (Bradford, 2020), where EU regulatory frameworks gain traction via market access rather than force. Countries like Finland and Norway, though not tech leaders, exert significant normative influence through privacy laws and telecom regulations, extending their governance reach. Based on this governance culture, the EU adopts a precautionary approach to technological governance (Newman & Posner, 2015), with the metaverse being no exception (Martini, 2025).

## 3. Analytical Framework: Towards a Typology of Metaverse Governance

### *3.1. The Analytical Dimensions of Metaverse Governance*

To conceptualize state approaches to metaverse governance, this study employs an analytical framework derived from an inductive content analysis of national policy documents, informed by the principles of grounded theory (Sebeelo, 2022). As shown in Table 1, this framework categorizes governance strategies across five dimensions—policy scale, policy issue, strategic orientation, platform dependency and governance approach—thereby offering insights into the diverse priorities and strategies states adopt to navigate the complexities of the metaverse.

**Table 1.** Dimensions of state approaches to metaverse governance.

| Dimension | Description |
|---|---|
| Policy scale | The scope of policy adoption: comprehensive, sectoral, and vision-centric. |
| Policy issue | The dominant thematic focus: economic, political, cultural, security, and R&D. |
| Strategic orientation | The aims of strategy: consolidate capacities, enforce existing strengths, drive economic transformation, and prevent potential risks. |
| Platform dependency | The degree of reliance on global technology infrastructure, supply chains, and standards: high, medium, and low. |
| Governance approach | The preferred governance logic: centralized, collaborative, innovation-driven, and ethics-based. |

First, the policy scale dimension evaluates the scope of national metaverse policies, distinguishing among comprehensive, sectoral, and vision-centric strategies. Drawing on Candel and Biesbroek's (2016) analysis of policy integration, this dimension contrasts cross-sectoral and sector-specific approaches, helping to assess whether states pursue broad, overarching strategies or focus on specific sectors. Given the metaverse's future-oriented nature (Floridi, 2022), vision-centric policies are particularly relevant as they reflect long-term aspirations, aiming to position the state as a global leader in metaverse technology and shape the future trajectory of digital governance.

Second, the policy issue dimension examines the thematic focus of national metaverse policies, covering economic, political, cultural, security, and R&D domains. This framework is informed by Kurbalija's (2016) internet governance taxonomy, which categorizes policy themes into economic, security, and socio-cultural domains, thereby aligning closely with the priorities of metaverse governance. Furthermore, the inclusion of R&D highlights the critical role of developing responsible standards in the metaverse (Hemphill, 2023), which are essential for addressing the evolving challenges and opportunities it presents.

Third, the strategic orientation dimension categorizes metaverse policies into five key objectives: capacity consolidation, regulatory enforcement, economic transformation, platform dependency, and risk prevention. This framework is grounded in Peters' (2018) work on strategic governance, which explores capacity building and regulatory adaptation. It also draws on Borrás and Edquist's (2013) analysis of innovation policy instruments aimed at economic transformation. Additionally, Hood and Margetts (2007) offer a framework for risk management in digital policy, reinforcing the importance of risk prevention within the metaverse.

Fourth, the platform dependency dimension analyzes the reliance of the state on global technology infrastructure, supply chains, and standards. States with low platform dependency possess robust domestic infrastructure and standard-setting authority. Those with medium dependency balance domestic and foreign platforms, achieving partial autonomy within external constraints. States with high dependency heavily rely on foreign platforms, exhibiting a structural tension between nominal sovereignty and material reliance in governance. Analysis of platform dependencies thus reveals how states assert discursive governance autonomy (Gorwa, 2019), yet remain materially constrained by asymmetric global technological infrastructures.

Fifth, the governance approach dimension analyzes the underlying logic of metaverse policies, distinguishing between centralized, collaborative, innovation-driven, and ethics-based models. Rhodes' (1997) distinction between hierarchical and network-based governance informs the centralized and collaborative models, while Ansell and Gash (2008) further develop the concept of collaborative governance through multi-stakeholder partnerships. Hartley et al. (2013) offer insights into innovation-driven governance, and Jasanoff's (2015) concept of sociotechnical imaginaries supports ethics-based approaches by emphasizing the role of cultural and ethical influences on technology policy.

These five dimensions—policy scale, policy issue, strategic orientation, platform dependency, and governance approach—form a comprehensive framework for analyzing state responses to the metaverse. By integrating discursive elements (policy priorities and strategic narratives) with material factors (technological capacities and infrastructure dependencies), the framework clarifies what states are doing and why they adopt particular approaches. This approach not only categorizes state actions but also illuminates the interaction between autonomous governance ambitions and structural constraints within the asymmetric global digital order, thereby strengthening the framework's explanatory power for understanding Web 3.0 governance.

### *3.2. Data Collection and Analysis*

This study analyzes state approaches to metaverse governance through a qualitative content analysis of 34 metaverse policy documents issued between 2021 and 2024 by 13 jurisdictions, as summarized in Table 2. The selection of these countries reflects a range of distinct roles within the global digital governance framework, encompassing dominant technological and economic powers (e.g., the United States and China), influential regional and cultural hubs (e.g., Japan, South Korea, and France), key regulatory actors (e.g., the European Union), and resource-driven economies (e.g., Saudi Arabia and the UAE), which offers a diversity basis for cross-national and cross-regional comparison.

These policy documents comprise three main categories: (a) dedicated national or local metaverse strategies (e.g., China's strategic development plans; Dubai's Metaverse Strategy); (b) broader digital and AI policies that explicitly reference the metaverse (e.g., the US Executive Order on AI; EU Digital Services Act); and (c) government-commissioned research reports (e.g., France's Exploratory Mission on the Metaverse). Notably, governance documents authored solely by private platform companies (e.g., Roblox and Meta) were excluded due to their commercial nature and lack of direct reflection of state policy intentions. This study focuses on finalized government strategies, national plans, and research reports that explicitly express political intentions (Colebatch, 2018)—features that make them suitable for qualitative content analysis.

**Table 2.** Number of metaverse-related policy documents issued by country/region.

| Types | Policy actor | Number of strategies |
|---|---|---|
| Supranational entity | European Union | 6 |
| Great power | China | 4 |
| | United States | 3 |
| Major power | United Kingdom | 4 |
| | France | 1 |
| | Germany | 1 |
| Middle power | Japan | 5 |
| | South Korea | 4 |
| | UAE | 2 |
| | Saudi Arabia | 1 |
| Small power | Norway | 1 |
| | Finland | 1 |
| | Switzerland | 1 |
| Total | | 34 |

We first identified and collected relevant documents through an initial keyword-based search, using terms such as strategy, interests, sovereignty, governance, policy, regulation, technology, innovation, economy, industry, investment, infrastructure, security, privacy, risk, and management. This approach, commonly used in policy analysis (Weiss & Jankauskas, 2019), helped locate key sections describing policy goals, governance mechanisms, and strategic narratives. Recognizing that relevant content is often dispersed across introductions, objectives, and implementation measures, we conducted full-text contextual readings to ensure comprehensive coverage, following best practices in qualitative policy research (Falleti & Lynch, 2009).

Drawing on grounded theory in comparative policy studies (Sebeelo, 2022), the analysis began with open coding to identify patterns and concepts within the data. This process revealed five analytical dimensions—policy scale, policy issue, strategic orientation, platform dependency, and governance approach. Through axial coding, these concepts were then developed into more coherent categories, drawing insights from established theoretical frameworks. The categorization process was informed by scholarly work on policy integration (Candel & Biesbroek, 2016), strategic governance (Peters, 2018), and innovation policy (Borrás & Edquist, 2013), while also incorporating perspectives from the emerging literature on platform governance (Gorwa, 2019; Mueller & Farhat, 2022) and broader governance models (Jasanoff, 2015; Rhodes, 1997). This approach allowed the analysis to remain grounded in the empirical material while engaging with relevant theoretical debates, ultimately capturing both the material and discursive dimensions of how metaverse governance is emerging.

Building on this foundation, we adopted a critical political economy lens to examine how metaverse policies operate within the broader structures of digital capitalism and geopolitical competition. This analytical approach revealed how policy discourse functions not merely as technical coordination but as a form of anticipatory governance that positions states within emerging technological hierarchies. By interrogating the institutional interests and ideological assumptions embedded in policy texts, we uncovered how metaverse strategies serve multiple functions: signaling technological sovereignty, attracting investment flows, and establishing regulatory precedents that may shape future digital governance architectures.

The coding process was conducted manually by two researchers. Inter-coder reliability was ensured through comparison and reconciliation of results. The codebook was revised as new patterns emerged—such as vision-centric strategies emphasizing soft power or global leadership—especially in countries like the UAE and South Korea. The final codebook covers the five dimensions mentioned previously, each with multiple specific codes (see Table B in the Supplementary File). By combining inductive content analysis with theoretical grounding and comparative document analysis, this method provides a systematic, transparent, and replicable examination of how states articulate their priorities, objectives, and governance logics for the metaverse.

### *3.3. Constructing a Typology of Metaverse Governance*

To analyze the diverse state responses to the metaverse, this study develops a typology grounded in the preceding qualitative content analysis. The typology emerged inductively from patterns observed across the coded policy materials. It offers an empirically grounded yet theoretically informed structure for capturing the diversity of national governance logics.

The countries selected represent a broad spectrum of global positions in digital governance, ranging from technological and economic powers to regulatory actors and resource-dependent economies. The analysis was guided by the five key dimensions, enabling a nuanced understanding of the various approaches states adopt in managing the metaverse. Informed by these dimensions, the typology categorizes states into four distinct governance archetypes presented in Table 3: techno-economic vanguards, industrial innovators, transformative opportunists, and regulatory vigilants. These types reflect the varying strategic priorities and governance rationalities that influence policy design and implementation, offering a comparative framework for understanding how different states address metaverse governance challenges.

**Table 3.** A typology of metaverse governance.

| Type | Techno-economic vanguards | Industrial innovators | Transformative opportunists | Regulatory vigilants |
|---|---|---|---|---|
| Policy scale | Comprehensive | Sectoral | Vision-centric | Comprehensive/ Vision-centric |
| Policy issue | Economic/R&D | Economic | Economic/Cultural | Security/Politics |
| Strategic orientation | Consolidating | Enforcing | Transformative | Preventative |
| Platform dependency | Low | Medium | High | Medium |
| Governance approach | Innovation-driven | Collaborative | Centralized | Ethics-based |

This study identifies four main types:

- *Techno-economic vanguards*: This archetype is defined by a comprehensive policy scope, focusing on economic and R&D priorities within a capacity-consolidating strategic orientation. With low platform dependency, these states can exercise greater autonomy in governance and standard-setting. They invest in infrastructure, international standards, and frameworks that align the metaverse with broader

geopolitical ambitions. They adopt an innovation-driven governance approach, positioning the metaverse as a key enabler of technological sovereignty and long-term competitiveness, thereby asserting structural power over emergent digital ecosystems.

- *Industrial innovators*: Characterized by a sectoral policy scope, these nations emphasize economic development within niche sectors such as manufacturing, telecommunications, electronics, and the entertainment industry. Their specialization in these industries drives a sustained enforcement-oriented strategic orientation. This also explains their medium platform dependency: while they hold advantages in specific industrial domains, they still need to coordinate with foreign technology providers to maintain partial autonomy. Consequently, governance follows a collaborative model in which public–private partnerships play a central role in shaping industrial metaverse applications and enhancing sectoral competitiveness.
- *Transformative opportunists*: Defined by a vision-centric policy scope, these nations show strong enthusiasm for emerging technologies—including the metaverse—and regard them as opportunities to diversify their economies, particularly in post-resource or tourism-driven contexts. To pursue these transformative goals, governance is highly centralized, with strong state coordination and top-down policy implementation. However, because these states often lack sufficient technological and industrial foundations, they exhibit high platform dependency, which in turn limits their autonomy. Consequently, compared to other archetypes, their engagement with the metaverse remains largely a symbolic performance—centered on soft power projection through cultural narratives and nation-branding—rather than being grounded in sector-specific development or actual policy execution.
- *Regulatory vigilants*: This archetype is defined by a comprehensive or vision-centric policy scope, with a strong emphasis on security, risk management, and democratic accountability. Although these states exhibit partial reliance on foreign platforms, their advantages in setting technological governance standards reduce their overall dependency to a medium level. This partial reliance contributes to their adoption of a preventative strategic orientation, which shapes an ethics-based governance approach that prioritizes digital rights, privacy, and normative safeguards. Consequently, regulatory frameworks aim to extend democratic values into immersive environments, asserting moral and normative influence in global digital governance.

These four archetypes and their cross-national distribution are mapped in Figure 1. This distribution, while capturing dominant patterns in metaverse governance, also reveals certain boundaries and blind spots. In certain cases, such as France or Japan, they may prioritize culturally oriented innovation over digital sovereignty, reflecting political-economic constraints or socio-technical legacies rather than purely strategic choices. Moreover, states are not static: they can display fluidity and hybridity, moving across categories or combining multiple governance logics. For example, South Korea demonstrates both technological leadership and cultural diplomacy, blurring the line between industrial innovators and transformative opportunists. These four archetypes thus serve as ideal types rather than fixed empirical categories, allowing for flexibility as policy objectives and technological capacities evolve. At the same time, this typology reveals how states adopt an adaptive posture within an asymmetric digital order, where autonomy is shaped by technological capacities and socio-economic conditions. Specifically, in Web 3.0 governance, state autonomy remains fundamentally constrained by the structural tension between discursive sovereignty and infrastructural control: states may assert independent leadership, yet their reliance on US (or Chinese) controlled infrastructure, cloud services, and standard-setting bodies reveals the limits of such claims (Mueller & Farhat, 2022).

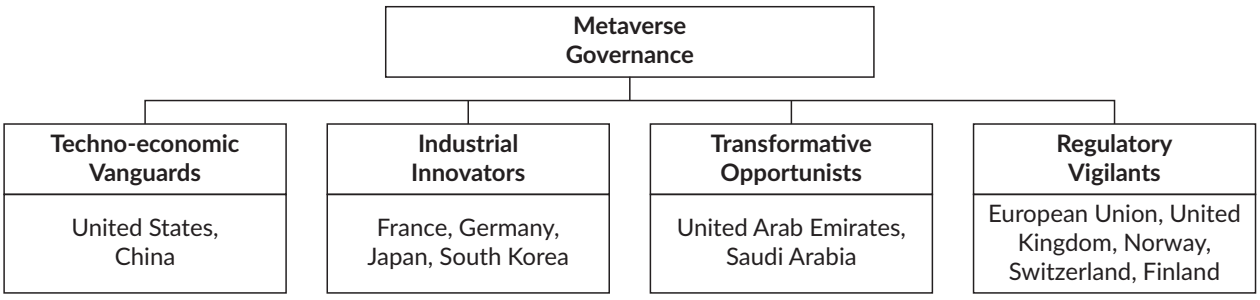



**Figure 1.** Cross-national distribution of metaverse governance dimensions.

This global asymmetry underscores the need to distinguish between governance execution and policy signaling. Governance execution emphasizes practical implementation, industrial development, and technological consolidation, whereas policy signaling highlights cultural narratives and expressions of international leadership. This distinction helps explain why, in the context of metaverse governance, some states continue to prioritize decentralization narratives or nation-branding in Web 3.0, even when their actual control over infrastructure remains limited. By framing the typology as a diagnostic tool, it integrates these structural constraints and hybrid strategies, providing a lens to understand how states navigate asymmetric dependencies, balance discursive sovereignty with material limitations, and design governance adaptive policies within the metaverse.

## 4. Comparative Metaverse Governance: National Strategies and Practices

To compare national approaches to metaverse governance, this study employs three interrelated criteria. First, it identifies each country's stated policy goals within broader strategies of digital governance and technological development, clarifying how states frame their ambitions in the metaverse. Second, it maps discursive sovereignty against material infrastructure control to expose structural contradictions, showing how narratives of decentralization or regulatory leadership often coexist with reliance on foreign-controlled chips, cloud services, and platforms. Third, it adopts a performance versus execution lens to distinguish symbolic signaling and nation-branding from the practical capacities of implementation, industrial consolidation, and technological integration. Together, these criteria provide a coherent framework for comparative analysis that links governance archetypes with the concrete strategies states adopt to manage asymmetric digital dependencies.

### *4.1. Techno-Economic Vanguards*

The United States and China, as leading techno-economic powers, pursue ambitious strategies to advance technology and Web 3.0 development, supported by strong technological foundations, talent, and national policy frameworks. However, comparative analysis of policy documents reveals distinct approaches: China adopts a state-centric strategy aimed at industrializing the metaverse and fostering domestic digital growth, whereas the United States emphasizes a market-oriented path, focusing on technological leadership and global standard-setting. These contrasts illustrate how states sharing underlying techno-economic strengths may adopt divergent strategies in metaverse governance.

#### 4.1.1. China: Metaverse Industrialization and Digital Economy Growth

China has been among the most proactive states in metaverse policymaking. Since 2022, more than 30 provinces and cities have issued over 50 policies, complemented by national strategies and local initiatives in major cities such as Beijing, Shanghai, and Guangzhou (Negro & Savina, 2025). Rooted in the Internet+ plan (Government of China, 2015), China's metaverse framework aligns with the *14th Five-Year Plan for Digital Economy Development*, which promotes digital transformation across industries (Government of China, 2022). In 2023, the *Three-Year Action Plan for the Innovative Development of the Metaverse Industry (2023–2025)* further codified national ambitions (Government of China, 2023), reflecting clear policy objectives within China's broader techno-economic consolidation strategy.

China's metaverse governance exemplifies a capacity-consolidating approach grounded in technological self-reliance and industrial coordination. National R&D programs prioritize breakthroughs in key enabling technologies—spatial computing, holographic displays, and 5G/6G infrastructure—aimed at reducing dependence on foreign platforms (Government of China, 2023). Beyond hardware, China actively cultivates domestic metaverse platforms and digital asset frameworks, seeking to establish alternative standards to those dominated by US tech giants. Implementation patterns at the municipal level illustrate this dual logic. Beijing's Tongzhou Sub-Center plan targets cultural tourism and enterprise clusters (Tongzhou District People's Government of Beijing Municipality, 2022), featuring digital twin applications and immersive experiences such as the Beijing City Library's metaverse center. While some initiatives remain experimental, they serve strategic functions—piloting regulatory frameworks, attracting investment, and signaling commitment to next-generation infrastructure. This sustained momentum is reinforced through China's strategic integration of industry, academia, and research, which functions as a coordinated mechanism to advance metaverse innovation (Government of China, 2023): over 8,500 academic publications addressing technological, commercial, and ethical dimensions have emerged (numbers consulted at the China National Knowledge Infrastructure at http://www.cnki.net when searching for the term "metaverse" in October 2025), supporting China's digital innovation ecosystem. Although recent policy shifts toward AI have reoriented resource allocation, institutional inertia ensures continued support for metaverse initiatives as part of China's diversified digital economy portfolio (Yao et al., 2021), reflecting adaptive rather than abandoned ambitions.

#### 4.1.2. United States: Market-Driven Metaverse Innovation and Technological Leadership

Unlike China's state-led approach, the United States's metaverse development is driven primarily by market forces and private-sector innovation. Yet this market orientation coexists with, and is reinforced by, strategic state intervention in critical domains: standard-setting, export controls, and technological gatekeeping. The US's influence is embedded less in explicit metaverse policies than in its structural control over the global digital ecosystem.

This control manifests most clearly in standard-setting institutions. In September 2022, the IEEE Standards Association, a US-dominated body, formally adopted the term "Metaverse" at the committee level, signaling American leadership in defining technical parameters for emergent technologies. Although the IEEE engages international experts and coordinates with the International Telecommunication Union (ITU), the International Electrotechnical Commission (IEC), and the International Organization for Standardization (ISO),

decision-making authority remains concentrated within US-based networks, extending American priorities through ostensibly collaborative frameworks. This illustrates a fundamental asymmetry: standard-setting appears multilateral but functions hegemonically, marginalizing alternative visions of metaverse architecture.

While the United States has not issued a dedicated national metaverse strategy, its position is encoded in broader technology frameworks prioritizing technological primacy over geopolitical rivals. The 2022 National Security Strategy explicitly positions technology as "the core of today's geopolitical competition" (White House, 2022), framing digital leadership as existential to national security. This logic underpins aggressive export controls: in January 2025, the Bureau of Industry and Security released the Framework for Artificial Intelligence Diffusion, imposing stringent chip restrictions targeting China (Regulations.gov, 2025)—policies that extend the Trump administration's "America First" technology strategy. As a contested domain within US–China digital rivalry, the metaverse exemplifies how the US leverages standard-setting, export controls, and private-sector ecosystems to preserve technological hegemony while constraining competitors' infrastructural autonomy.

### *4.2. Industrial Innovators*

Our analysis of metaverse policy documents from South Korea, Japan, and France reveals a distinct governance pattern characterized by sectoral specialization rather than comprehensive technological competition. South Korea leverages the K-Metaverse to boost the fan economy and enhance smart city integration and digital governance. Japan cultivates an anime-driven metaverse ecosystem, using anime IPs as tools of cultural diplomacy to expand global influence and promote cultural exports. France mobilizes heritage digitization and luxury brand virtualization to assert cultural presence amid platform dependency. Rather than directly challenging the US–Chinese platform hegemony, these states convert sectoral strengths into strategic niches, demonstrating how cultural assets enable governance participation even when technological control remains structurally foreclosed.

#### 4.2.1. South Korea: K-Metaverse Fan Economy and Smart Governance Synergy

South Korea's *Pan-Governmental Strategy on Metaverse* (Ministry of Science and ICT, 2022) coined the term "K-Metaverse," branding immersive technologies as extensions of the country's globally influential entertainment industry. The strategy positions metaverse platforms as vehicles for monetizing cultural exports, exemplified by SK Telecom's K-pop Metaverse Project, which integrates AR and mixed reality technologies into fan engagement ecosystems. Beyond commercial applications, this approach reflects hybrid governance ambitions, sectoral innovation in entertainment coexists with efforts to establish Seoul as a global metaverse hub—balancing industrial consolidation with symbolic nation-branding (Proctor, 2021)

The metaverse also figures prominently in South Korea's urban governance agenda. *The Metaverse Seoul* is the first comprehensive plan by a local government to develop a new tech-based administration platform, which is designed to quickly adapt to changing administrative needs and provide innovative public services (Seoul Metropolitan Government, 2021). Aligned with South Korea's longstanding approach to *Smart City Korea* and *Digital Strategy of Korea*, the plan targets metaverse integration across government services and urban management. While implementation remains largely experimental, digital twin applications serve as proof-of-concept rather than fully functional infrastructure. This dual emphasis illustrates South

Korea's enforcement-oriented approach, leveraging existing advantages while piloting innovations within established competitive sectors.

#### 4.2.2. Japan: Game Empower Metaverse and Cultural Soft Power Expansion

Japan's competitive advantage in the gaming and anime industries provides foundational infrastructure for metaverse development, reflecting technological alignment in virtual reality, 3D modeling, and immersive social environments. Capitalizing on this strategic positioning, Japan constructed the Open Metaverse Infrastructure RYUGUKOKU, which adopts role-playing game architectures as outlined in the *Agreement on the Japan Metaverse Economic Zone* (Fujitsu, 2023). This initiative, inspired by Hajime Tabata's vision of "updating Japan through games," targets digital twin society applications.

The establishment of Japan's Web 3.0 Policy Office in 2022 positioned the metaverse as an emerging interface for Generation Z, emphasizing economic opportunities arising from digital space and asset proliferation (Ministry of Economy, Trade and Industry, 2022). Prime Minister Kishida (2022) subsequently prioritized the development of Web 3.0 service development leveraging metaverse technologies. Japan strategically mobilizes its influential anime and otaku culture to consolidate global cultural soft power through metaverse platforms. However, Roquet (2023) identifies dual motivations underlying Japan's engagement: strategic cultural initiatives coexist with societal escapism impulses, revealing drivers that extend beyond state-directed cultural diplomacy.

#### 4.2.3. France: Digital Heritage Metaverses and Luxury-Fashion Marketing

France, renowned for its rich cultural heritage and extensive museum collections, positions itself for the metaverse as an instrument reconciling technological sovereignty with cultural autonomy. President Macron articulated this imperative: "France, through its language, its heritage, its towns and villages, its monuments, must also exist in the metaverse" ("Innovation and risk taking," 2022). The report *Mission Exploratoire sur les Métavers* commissioned by the Ministry of Economy, Finance, and Industrial and Digital Sovereignty, underlines French technological-cultural collaboration through public procurement to reduce American technology dependency (François et al., 2022), extending the *exception culturelle* doctrine into digital domains (Richieri Hanania, 2019).

France's luxury sector actively promotes metaverse engagement, driving innovation and market experimentation. Prominent brands such as Louis Vuitton, Gucci, and Burberry are exploring virtual storefronts and NFT collaborations with gaming companies, leveraging digital art and technology to enhance global influence and consumer experience (Profumo et al., 2023). As luxury production increasingly incorporates computational design alongside traditional craftsmanship (Armitage, 2023), metaverse marketing offers consumers immersive brand experiences that enhance both hedonic and utilitarian value, thereby strengthening customer satisfaction and brand loyalty (Weinberger, 2022). These industry practices, combined with France's strategic policy initiatives, demonstrate how the nation balances cultural sovereignty, technological innovation, and market execution to advance its metaverse presence.

### *4.3. Transformative Opportunists*

Energy-dependent economies view the metaverse as a transformative technological catalyst for future growth. Their policies adopt bold and far-reaching measures to diversify economies, create new jobs, and establish global leadership in the digital age. Although these countries actively invest in metaverse-related projects, including AI, digital cities, quantum computing, and biotechnology, many initiatives remain largely symbolic, serving as performative signals rather than as a reflection of fully implemented technological capacities. Nevertheless, these efforts illustrate how the symbolic political signaling in national policies can foster innovation and enhance international visibility, even when practical execution is limited, integrating them into a broader strategy aimed at long-term competitiveness.

#### 4.3.1. UAE: Achieving Economic Diversification and Global Visibility with the Metaverse

As the pioneering emirate of the UAE, Dubai launched the *Dubai Metaverse Strategy* with the ambitious objective of becoming one of the world's top ten metaverse economies (Government of Dubai Media Office, 2022). This strategy incorporates a diversification approach, emphasizing technological innovation, talent development, industry applications, and regulatory governance. Notably, Dubai has already attracted over 1,000 companies specializing in blockchain and metaverse technologies and aims to support more than 40,000 virtual jobs by 2030. While the actual implementation of some initiatives remains difficult to assess, they serve as high-profile signals of Dubai's commitment to digital leadership and attract global attention. To advance its metaverse vision, Dubai hosts events such as the Dubai Metaverse Assembly in August 2022, bringing together global experts to explore potential applications (Dubai Future Foundation, 2022). However, with the subsequent decline of the metaverse, this forum was not held again. These activities demonstrate how Dubai leverages the metaverse to enhance international visibility, attract foreign investment, and ultimately advance its broader goal of economic transformation.

#### 4.3.2. Saudi Arabia: Energy Transformation and Sustainable Development in the Metaverse

Saudi Arabia's metaverse strategy reflects vision-centric governance driven by *Saudi Vision 2030*'s economic diversification mandate, positioning the metaverse as a transformative catalyst for reducing oil dependency (Saudi Arabian Government, 2024). At the heart of this strategy is the $500 billion NEOM project, which leverages digital twin technology to simulate human interactions and enhance living experiences. By analyzing data from sensors and Internet of Things systems, NEOM is designed to stimulate growth in the digital economy. Another key initiative, the Cultural Universe platform (Saudi Press Agency, 2024), was launched by Saudi Arabia's Ministry of Culture, which provides an immersive, interactive exploration of the kingdom's cultural heritage. These centralized initiatives signal state commitment to technological innovation and cultural preservation, yet they function primarily as symbolic instruments projecting global leadership despite nascent implementation.

In the global wave of digital transformation, Middle Eastern nations are actively investing in the metaverse, with Dubai aiming to become a leading metaverse economy and Saudi Arabia focusing on its NEOM smart city project. Despite distinct national strategies, these efforts share a performative dimension that prioritizes visibility over operational depth. In order to convert vision-centric policies into competitive advantages, these efforts entail leveraging unique cultural and resource strengths to develop region-specific metaverse

applications alongside establishing transparent and adaptable regulatory frameworks to attract international investment and talent.

### *4.4. Regulatory Vigilants*

Distinguished by its strategic prioritization of rights-based regulation, the European Union embodies the regulatory vigilant archetype in metaverse governance. Often characterized as lacking the "gene" for internet innovation due to weaker economic foundations and strong legal traditions emphasizing privacy protection (Mayer, 2000), the EU has nonetheless emerged as a global regulatory superpower. Through landmark frameworks such as GDPR, the Data Act, and the AI Act, it shapes the normative contours of emerging digital environments, including the metaverse (Young, 2015). This trajectory reflects strategic reliance on regulatory instruments to assert discursive sovereignty despite heavy dependency on foreign digital infrastructure and platform capital.

Although regulatory spheres sometimes overlap, the EU and its member states pursue different strategic priorities and should be treated as distinct actors. The EU, as a supranational bureaucratic body, has its own institutional interests and incentives. It seeks to exercise normative authority through anticipatory regulations rooted in ethical, privacy, and security concerns, signaling discursive leadership despite material constraints (Manners, 2002). By contrast, member states such as Germany and France—classified here as industrial innovators—leverage industrial and cultural assets to capitalize on the metaverse's economic and strategic potential. Germany applies digital twin technologies to smart manufacturing, while France uses immersive media to amplify cultural branding and luxury markets (Profumo et al., 2023). These approaches reflect national ambitions to enhance competitiveness, not simply to regulate.

This strategic divergence is shaped by structural differences. The EU, lacking major indigenous platforms and significant economic sovereignty, attempts to project power through regulatory activism, relieving a tension between its discursive authority and dependency on foreign technological infrastructure (Leonard et al., 2019). These compliance burdens may redirect resources away from R&D (Martini, 2025), limiting practical innovation. In addition, its bureaucratic logic prioritizes harmonization, standard-setting, and normative consistency. In contrast, member states have the flexibility to experiment with sectoral policies and pilot initiatives that align with national growth models—even as they must navigate EU-wide regulations. These national efforts are not merely subcomponents of EU policy, but expressions of distinct economic agendas.

Diverse national trajectories confirm this distinction. Finland was the first EU member state to launch a national metaverse strategy, warning of digital dependency on foreign tech giants (Digital Finland, 2023). Sweden and Norway have explored metaverse applications in music streaming and virtual tax offices, respectively. France's metaverse strategy emphasizes cultural sovereignty and cross-sector collaboration (François et al., 2022), while the EU focuses on cross-border data governance and regulatory integrity. These examples highlight the persistent tension between the EU's bureaucratic orientation and its member states' strategic objectives, which do not fully converge.

In sum, classifying the EU as a regulatory vigilant—separate from France and Germany—captures the institutional logics that underpin metaverse governance in Europe. While the EU promotes a coherent ethical regime through regulation, member states pursue more pragmatic innovation strategies aimed at

advancing national power and competitiveness. This analytical separation reflects not only formal legal distinctions but also the inherent tension between normative authority and material dependency in shaping Europe's digital future.

## 5. Conclusion and Discussion

Despite the cooling of global metaverse hype, examining its development, governance, and international implications remains highly relevant. As a convergence of digital technologies, cultural production, and regulatory frameworks, the metaverse—and Web 3.0 more broadly—provides a lens for analyzing how states navigate technological innovation and governance challenges. Understanding these dynamics provides insights into digital competition, policy experimentation, and the tension between discursive sovereignty and material infrastructure. Even if immediate enthusiasm has subsided, ongoing technological, cultural, and regulatory trajectories continue to reshape international digital landscapes.

This study analyzed 34 metaverse policy documents issued between 2021 and 2024 across 13 countries and regions, revealing variations shaped by strategic positioning, technological capacity, and industrial structure. To explain these differences, we propose a typology: techno-economic vanguards, industrial innovators, transformative opportunists, and regulatory vigilants. Techno-economic vanguards, such as China and the United States, leverage metaverse governance to maintain or challenge global hierarchies (Gilpin, 1981). Industrial innovators, including France, Japan, and South Korea, integrate metaverse technologies into industrial and cultural sectors. Transformative opportunists, such as UAE and Saudi Arabia, view the metaverse as a catalyst for economic diversification, while regulatory vigilants like the EU emphasize ethical governance and privacy protections (Bradford, 2020).

The typology advances understanding of metaverse and Web 3.0 governance within a structural context. First, it shows how governance styles reflect states' adaptive management of dependencies on US or China-controlled Web 3.0 platforms rather than fully autonomous choices (Mueller & Farhat, 2022). This typology thus functions as a diagnostic tool for assessing how states navigate reliance on foreign-controlled digital infrastructure while pursuing governance objectives. Second, a performance-versus-execution lens captures symbolic policymaking, where some states launch high-visibility Web 3.0 initiatives to signal intent but may lack substantive implementation. Third, contrasting discursive sovereignty with control over material infrastructure highlights structural contradictions, explaining why some states lead in Web 3.0 regulation while still relying on foreign chips, cloud services, or platform ecosystems, and why even ambitious governance strategies may encounter practical limits.

In addition, the typology also provides practical guidance for policymakers grappling with the uncertain and evolving nature of Web 3.0 technologies. By unpacking the governance logics embedded in national strategies, it offers a comparative lens for assessing not only where states stand, but also how their political economies, institutional capacities, and normative commitments shape feasible policy choices. Rather than promoting a one-size-fits-all model, the typology encourages reflexive governance—enabling states to align their metaverse and Web 3.0 ambitions with broader developmental priorities, avoid policy imitation, and critically evaluate the symbolic versus substantive functions of digital strategy in times of market volatility and technological hype. Importantly, the framework is not a static categorization but a dynamic one: as key factors such as infrastructure dependencies, regulatory priorities, and cultural strategies evolve, states may

move across categories or combine multiple logics. This emphasis on adaptability highlights the typology's role in capturing fluid governance trajectories rather than fixed policy types.

Despite these contributions, the study confronts inherent limitations rooted in the metaverse's fluid and contested nature. Deriving from formal policy documents rather than implementation outcomes, the typology cannot fully assess operational effectiveness or distinguish symbolic performance from substantive execution. The sample inevitably skews toward digitally proactive states, as many countries have yet to articulate formal metaverse strategies, raising questions about generalizability. Most critically, the 2021–2024 timeframe captures metaverse hype's rise and fall as a synchronic snapshot, flattening temporal dynamics and obscuring how states adapted—or failed to adapt—to market volatility and technological pivots. Without tracing these diachronic shifts, the analysis risks missing crucial discontinuities, policy reversals, and rhetorical adjustments that reveal how digital governance evolves under uncertainty.

Future research, therefore, should adopt complementary approaches to deepen understanding. Longitudinal studies tracking early adopters like China, South Korea, and the UAE would reveal whether ambitious strategies yield tangible transformation or merely symbolic gestures (Radu, 2021). Equally important is examining policy revisions, defunding, and discursive rebranding following industrial stagnation—dynamics that illuminate how states manage failure within digital policy cycles. Regional comparative analyses, particularly within the EU, could expose tensions between supranational coordination and national autonomy (Hine et al., 2024), while integrating science and technology studies perspectives would clarify how non-state actors, stakeholder contestation, and public deliberation shape more accountable metaverse governance (Goldberg & Schär, 2023).

This study advances digital governance scholarship by revealing how technological capacities, industrial endowments, and geopolitical positioning fundamentally shape metaverse policy formations. The typology exposes persistent gaps between discursive sovereignty and material infrastructure control, challenging policymakers to align ambitions with capabilities while acknowledging structural dependencies. As Web 3.0 governance evolves amid market volatility and technological uncertainty, sustained inquiry into these asymmetric dynamics remains essential—not only for understanding present challenges, but for exploring pathways toward more inclusive and equitable digital governance that accommodates diverse national strategies and development priorities.

## Acknowledgments

The author would like to thank the academic editors for their insightful comments and the anonymous reviewers for their constructive suggestions. Sincere thanks also go to Mai Tian for her assistance with data collection.

## Funding

This research receives financial support from the National Social Science Fund of China (Grant Number: 24BCJ002).

## Conflict of Interests

In this article, editorial decisions were undertaken by Zichen Hu (London School of Economics and Political Science) and Denis Galligan (University of Oxford).

## LLMs Disclosure

Large language models were employed exclusively for language editing and proofreading purposes.

## Supplementary Material

Supplementary material for this article is available online in the format provided by the authors (unedited).

## References

Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory*, *18*(4), 543–571.

Armitage, J. (2023). Rethinking haute couture: Julien Fournié in the virtual worlds of the metaverse. *French Cultural Studies*, *34*(2), 129–146.

Borrás, S., & Edquist, C. (2013). The choice of innovation policy instruments. *Technological Forecasting and Social Change*, *80*(8), 1513–1522.

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.

Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press.

Buragohain, D., Meng, Y., Deng, C., Li, Q., & Chaudhary, S. (2024). Digitalizing cultural heritage through metaverse applications: Challenges, opportunities, and strategies. *Heritage Science*, *12*(1), Article 295.

Calzada, I. (2024). Decentralized web3 reshaping internet governance: Towards the emergence of new forms of nation-statehood? *Future Internet*, *16*(10), Article 361.

Candel, J. J. L., & Biesbroek, R. (2016). Toward a processual understanding of policy integration. *Policy Sciences*, *49*(3), 211–231.

Chen, Y., Wu, C., & Zhang, R. (2025). Hotspots and prospects of metaverse: An international comparison. *Journal of Computer Information Systems*, *65*(5), 531–541.

Colebatch, H. (2018). The idea of policy design: Intention, process, outcome, meaning and validity. *Public Policy and Administration*, *33*(4), 365–383.

De Almeida, G. G. F. (2023). Cities and territorial brand in the metaverse: The metaverse SEOUL case. *Sustainability*, *15*(13), Article 10116.

Digital Finland. (2023). *Metaverse initiative by the finnish ecosystem: Virtual potential into real-world impact*.

Dolata, M., & Schwabe, G. (2023). What is the metaverse and who seeks to define it? Mapping the site of social construction. *Journal of Information Technology*, *38*(3), 239–266.

Dubai Future Foundation. (2022). *Dubai metaverse assembly*. https://www.dubaifuture.ae/wp-content/uploads/2022/12/TheMetaverseAssembly-OutcomesReport-WP-English.pdf

Egliston, B., Carter, M., & Clark, K. E. (2025). Who will govern the metaverse? Examining governance initiatives for extended reality (XR) technologies. *New Media & Society*, *27*(6), 3361–3381.

Eke, D., & Stahl, B. (2024). Ethics in the governance of data and digital technology: An analysis of European data regulations and policies. *Digital Society*, *3*, Article 11.

Eltanbouly, S., Halabi, O., & Qadir, J. (2025). Avatar privacy challenges in the metaverse: A comprehensive review and future directions. *International Journal of Human–Computer Interaction*, *41*(4), 1967–1984.

Erkut, B. (2020). From digital government to digital governance: Are we there yet? *Sustainability*, *12*(3), Article 860.

Falleti, T. G., & Lynch, J. F. (2009). Context and causal mechanisms in political analysis. *Comparative Political Studies*, *42*(9), 1143–1166.

Floridi, L. (2022). Metaverse: A matter of experience. *Philosophy & Technology*, *35*(3), Article 73.

Foster, C., & Azmeh, S. (2020). Latecomer economies and national digital policy: An industrial policy perspective. *The Journal of Development Studies*, *56*(7), 1247–1262.

François, C., Basdevant, A., & Ronfard, R. (2022, October 24). Mission exploratoire sur les métavers. *Vie-publique.fr*. https://www.vie-publique.fr/rapport/286878-mission-exploratoire-sur-les-metavers

Fujitsu. (2023, February 27). *Agreement on the creation of the "Japan Metaverse Economic Zone"* [Press release]. https://www.fujitsu.com/global/about/resources/news/press-releases/2023/0227-02.html

Gilpin, R. (1981). *War and change in world politics*. Cambridge University Press.

Goldberg, M., & Schär, F. (2023). Metaverse governance: An empirical analysis of voting within decentralized autonomous organizations. *Journal of Business Research*, *160*, Article 113764.

Gong, X. (2024). Turning the virtual into reality: China's role in the metaverse. *Asia Policy*, *19*(1), 8–20.

Gorwa, R. (2019). What is platform governance? *Information, Communication & Society*, *22*(6), 854–871.

Government of China. (2015). *Guowuyuan guanyu jiji tuijin "hulianwang+" xingdong de zhidao yijian*. https://www.gov.cn/zhengce/zhengceku/2015-07/04/content_10002.htm

Government of China. (2022). Guowuyuan guanyu yinfa "shisiwu" shuzi jingji fazhan guihua de tongzhi. https://www.gov.cn/zhengce/content/2022-01/12/content_5667817.htm

Government of China. (2023). *Yuanyuzhou chanye chuangxin fazhan sannian xingdong jihua (2023–2025 nian) de tongzhi*. https://www.gov.cn/zhengce/zhengceku/202309/content_6903023.htm

Government of Dubai Media Office. (2022). *Hamdan Bin Mohammed launches Dubai metaverse strategy*. https://www.mediaoffice.ae/en/news/2022/july/18-07/hamdan-bin-mohammed-launches-dubai-metaverse-strategy

Gray, J. E., & Tang, W. (2025). The Chinese metaverse: An analysis of China's policy agenda for extended reality (XR). *Policy & Internet*, *17*(1), Article e418.

Grincheva, N. (2023). The past and future of cultural diplomacy. *International Journal of Cultural Policy*, *30*(2), 172–191.

Hanisch, M., Goldsby, C. M., Fabian, N. E., & Oehmichen, J. (2023). Digital governance: A conceptual framework and research agenda. *Journal of Business Research*, *162*, Article 113777.

Hanneke, B., Heß, M., & Hinz, O. (2025). Foundations of decentralized metaverse economies: Converging physical and virtual realities. *Journal of Management Information Systems*, *42*(1), 238–272.

Hartley, J., Sørensen, E., & Torfing, J. (2013). Collaborative innovation: A viable alternative to market competition and organizational entrepreneurship. *Public Administration Review*, *73*(6), 821–830.

Hemphill, T. A. (2023). The 'Metaverse' and the challenge of responsible standards development. *Journal of Responsible Innovation*, *10*(1), Article 2243121.

Hine, E., Rezende, I. N., Roberts, H., Wong, D., Taddeo, M., & Floridi, L. (2024). Safety and privacy in immersive extended reality: An analysis and policy recommendations. *Digital Society*, *3*(2), Article 33.

Hood, C., & Margetts, H. (2007). *The tools of government in the digital age*. Bloomsbury Publishing.

Hu, J., & Zhang, X. (2023). Digital governance in China: Dispute settlement and stability maintenance in the digital age. *Journal of Contemporary China*, *33*(148), 561–577.

Innovation and risk taking echo our country's deep rooted history. (2022, April 21). *The Big Whale*. https://en.thebigwhale.io/article-en/innovation-and-risk-taking-echo-our-country-s-deep-rooted-history

Jasanoff, S. (2015). Future imperfect: Science, technology, and the imaginations of modernity. In S. Jasanoff & S. H. Kim (Eds.), *Dreamscapes of modernity: Sociotechnical imaginaries and the fabrication of power* (pp. 1–33). University of Chicago Press.

Jing, Y., & Li, D. (2019). Private roles in enhancing multi-Level governance: China's "Internet+" national strategy. *Public Policy and Administration*, *34*(2), 144–164.

Kahler, M. (2017). Regional challenges to global governance. *Global Policy*, *8*(1), 97–100.

Kassen, M. (2025). Blockchain and digital governance: Decentralization of decision making policy. *Review of Policy Research*, *42*(1), 95–121.

Keohane, R. O., & Nye, J. S. (1977). *Power and interdependence: World politics in transition*. Little, Brown and Company.

Kishida, F. (2022). *Policy speech by Prime Minister KISHIDA Fumio to the 210th session of the Diet* [Speech transcript]. https://japan.kantei.go.jp/101_kishida/statement/202210/_00003.html

Kshetri, N., Dwivedi Y. K., & Janssen M. (2024). Metaverse for advancing government: Prospects, challenges and a research agenda. *Government Information Quarterly*, *41*(2), Article 101931.

Kurbalija, J. (2016). *An introduction to internet governance*. Diplo Foundation.

Leonard, M., Pisani-Ferry, J., Ribakova, E., Shapiro, J., & Wolff, G. (2019). Securing Europe's economic sovereignty. *Survival*, *61*(5), 75–98.

Manners, I. (2002). Normative power Europe: A contradiction in terms? *Journal of Common Market Studies*, *40*(2), 235–258.

Martini, M. (2025). Materializing corporate futures: How the EU navigated the metaverse hype. *Information, Communication & Society*, *28*(5), 852–869.

Mayer, F. C. (2000). Europe and the internet: The old world and the new medium. *European Journal of International Law*, *11*(1), 149–169.

Meta. (2021). *Founder's letter, 2021*. https://about.fb.com/news/2021/10/founders-letter

Milakovich, M. E. (2021). *Digital governance: Applying advanced technologies to improve public service*. Routledge.

Ministry of Economy, Trade and Industry. (2022). *Web 3.0 policy office established in the Minister's Secretariat as a cross-departmental internal organization*. https://www.meti.go.jp/english/press/2022/0715_002.html

Ministry of Science and ICT. (2022, January 19). *Korea's pan-governmental strategy on metaverse* [Press release]. https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=621&searchOpt=ALL&searchTxt=

Moerel, L., & Timmers, P. (2021). *Reflections on digital sovereignty*. EU Cyber Direct.

Morgenthau, H. J. (1985). *Politics among nations: The struggle for power and peace* (6th ed.). Alfred Kopf.

Mosco, V. (2023). Into the metaverse: Technical challenges, social problems, utopian visions, and policy principles. *Javnost—The Public*, *30*(2), 161–173.

Mueller, M. L., & Farhat, K. (2022). Regulation of platform market access by the United States and China: Neo-mercantilism in digital services. *Policy & Internet*, *14*(2), 348–367.

Negro, G., & Savina, T. (2025). Yuanyuzhou: Yesterday, today, tomorrow. Historical roots, current visions, and future dynamics of real-world integration in the Chinese governmental narrative on the metaverse. *Information, Communication & Society*, *28*(5), 890–909.

Newman, A. L., & Posner, E. (2015). Putting the EU in its place: Policy strategies and the global regulatory context. *Journal of European Public Policy*, *22*(9), 1316–1335.

Parcu, P. L., Rossi, M. A., Innocenti, N., & Carrozza, C. (2023). How real will the metaverse be? Exploring the spatial impact of virtual worlds. *European Planning Studies*, *31*(7), 1466–1488.

Peters, B. G. (2018). *The politics of bureaucracy: An introduction to comparative public administration*. Routledge.

Pohle, J., & Santaniello, M. (2024). From multistakeholderism to digital sovereignty: Toward a new discursive order in internet governance? *Policy & Internet*, *16*(4), 672–691.

Porter, M. E. (1990). *The competitive advantage of nations*. Free Press.

Proctor, J. (2021). Labour of love: Fan labour, BTS, and South Korean soft power. *Asia Marketing Journal*, *22*(4), 79–101.

Profumo, G., Testa, G., Viassone, M., & Ben Youssef, K. (2023). Metaverse and the fashion industry: A systematic literature review. *Journal of Global Fashion Marketing*, *15*(1), 131–154.

Radu, R. (2021). Steering the governance of artificial intelligence: National strategies in perspective. *Policy and Society*, *40*(2), 178–193.

Regulations.gov. (2025). *Framework for artificial intelligence diffusion*. https://www.regulations.gov/document/BIS-2025-0001-0001

Rhodes, R. A. (1997). *Understanding governance: Policy networks, governance, reflexivity and accountability*. Open University Press.

Richieri Hanania, L. (2019). Trade, culture and the European Union cultural exception. *International Journal of Cultural Policy*, *25*(5), 568–581.

Roquet, P. (2023). Japan's retreat to the metaverse. *Media Culture & Society*, *45*(7), 1501–1510.

Russo, S. P., Mele, C., & Russo Spena, T. (2023). Innovative value propositions in the fashion metaverse. *Journal of Global Fashion Marketing*, *15*(1), 39–61.

Samuels, R. J. (1994). *"Rich nation, strong army": National security and the technological transformation of Japan*. Cornell University Press.

Saudi Arabian Government. (2024). *Vision 2030 annual report 2024*. https://www.vision2030.gov.sa/en/annual-reports

Saudi Press Agency. (2024). *Saudi Arabia launches cultural universe platform*. https://www.spa.gov.sa/en/N2066324

Sayem, A. S. M. (2022). Digital fashion innovations for the real world and metaverse. *International Journal of Fashion Design, Technology and Education*, *15*(2), 139–141.

Schimmelfennig, F. (2001). The community trap: Liberal norms, rhetorical action, and the Eastern enlargement of the European Union. *International Organization*, *55*(1), 47–80.

Sebeelo, T. B. (2022). The utility of constructivist grounded theory in critical policy analysis. *International Journal of Qualitative Methods*, *21*, Article 16094069221090057.

Seoul Metropolitan Government. (2021). *Seoul to provide public services through its own metaverse platform*. https://english.seoul.go.kr/seoul-to-provide-public-services-through-its-own-metaverse-platform

Shin, S., & Park, J. (2025). A study on metaverse risk factors and user risk perception in South Korea. *Telecommunications Policy*, *49*(3), Article 102911.

Tongzhou District People's Government of Beijing Municipality. (2022). *Beijingshi jingji he xinxihua ju guanyu yinfa "Beijing chengshi fuzhongxin yuanyuzhou chuangxin fazhan xingdong jihua (2022–2024 nian)" de tongzhi*. https://www.bjtzh.gov.cn/bjtz/xxfb/202208/1612371.shtml

Van Dijck, J. (2021). Seeing the forest for the trees: Visualizing platformization and its governance. *New Media & Society*, *23*(9), 2801–2819.

Vidal-Tomás, D. (2023). The illusion of the metaverse and meta-economy. *International Review of Financial Analysis*, *86*, Article 102560.

Vold, K. (2024). Human-AI cognitive teaming: Using AI to support state-level decision making on the resort to force. *Australian Journal of International Affairs*, *78*(2), 229–236.

Wang, G., Zhang, Z., Nandhakumar, J., & Manoharan, N. (2025). Everyday metaverse: The metaverse as an integral part of everyday life. *Journal of Management Information Systems*, *42*(1), 310–342.

Weinberger, M. (2022). What is metaverse?—A definition based on qualitative meta-synthesis. *Future Internet*, *14*(11), Article 310.

Weiss, M., & Jankauskas, V. (2019). Securing cyberspace: How states design governance arrangements. *Governance*, *32*(2), 259–275.

White House. (2022). *The Biden-Harris administration's national security strategy*. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/10/12/fact-sheet-the-biden-harris-administrations-national-security-strategy

Yang, L. (2023). Recommendations for metaverse governance based on technical standards. *Humanities and Social Sciences Communications*, *10*(1), 1–10.

Yao, D., Zhu, Y., & Yu, K. (2021). Institutional inertia, local leadership turnover, and changes in the structure of fiscal expenditure. *The Journal of Chinese Sociology*, *8*(1), Article 13.

Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, *12*(4), 505–523.

Young, A. R. (2015). The European Union as a global regulator? Context and comparison. *Journal of European Public Policy*, *22*(9), 1233–1252.

## About the Authors

Chang Zhang is an associate professor at the School of Government and Public Affairs, Communication University of China, and director of the Center for International Organization Studies. Her research focuses on international political communication, media and global governance, and Chinese and Russian foreign policy.

Lexuan Wang is a PhD candidate at the School of Government and Public Affairs, Communication University of China, and a research associate at the Institute for Political Communication. His research focuses on political communication, examining domestic party politics and political marketing, alongside international information geopolitics.

Politics and Governance
2025 • Volume 13 • Article 10245
https://doi.org/10.17645/pag.10245

cogitatio

ARTICLE

Open Access Journal

# Governing AI Decision-Making: Balancing Innovation and Accountability

David Mark and John Morison

School of Law, Queen's University Belfast, UK

**Correspondence:** David Mark (dmark02@qub.ac.uk)

**Submitted:** 28 February 2025 **Accepted:** 4 September 2025 **Published:** 19 November 2025

**Issue:** This article is part of the issue "Technology and Governance in the Age of Web 3.0" edited by Chang Zhang (Communication University of China), Zichen Hu (London School of Economics and Political Science), and Denis Galligan (University of Oxford), fully open access at https://doi.org/10.17645/pag.i443

## Abstract

This article explores the growing use of algorithmic models to make or inform decisions within the public sector. Amidst a climate of accelerating investment, expanding system applicability, and rapid technical progress, it concentrates on how key jurisdictions, most prominently the "digital empires" of the United States, European Union, and China, construct the problems associated with such algorithmic systems, and how these constructions impact governance. Drawing on an example from the legal sphere, it highlights both the potential efficiency gains and the increasing tensions concerning automation and fairness. This article then adopts aspects of Carol Bacchi's Foucauldian-inspired "What's the Problem Represented to Be?" framework to trace how divergent problem framings, ranging from the United States' emphasis on an "innovation gap," to the European Union's "trust deficit," and China's "stability risk," have produced distinct regulatory trajectories. Yet, despite these divergent framings and national strategies, this article argues that a common post-2024 trend emerges, revealing a general shift toward regulatory softening, one that privileges innovation over precautionary safeguards. This convergence raises critical questions about the future direction and resilience of "algorithmic decision-making" governance.

## Keywords

accountability; AI regulation; algorithmic decision making; judicial AI; problematization; public sector innovation; techlash

## 1. Introduction

As governments worldwide seek to harness increasingly sophisticated algorithmic systems to complement decision-making processes, several strategic objectives are being pursued. These include ambitions for public

service transformation, the pursuit of economic growth, and efforts to secure national security and geopolitical advantage. This article investigates how key jurisdictions, specifically the US, the EU, and China, frame the risks and opportunities associated with such technologies, and how these divergent framings shape the regulation of the arena.

This article begins by explaining its choice of "algorithmic decision making" (ADM) as the central analytical terminology, before exploring the surrounding techno-economic landscape, highlighting a resurgence in algorithmic deployment, investment, and technical progress. It then examines the context in which ADM is being implemented in the public sector, using the judicial sphere to provide an illustrative example. Finally, it draws upon Carol Bacchi's "What's the Problem Represented to Be?" (WPR) framework (Bacchi, 2009) to ask how algorithmic technologies are problematized within current governance strategies and policy discourse advanced by the three key global actors, how these problem representations materialise, and what rationalities underpin them. In doing so, this article foregrounds how problem representations, ranging from an "innovation gap" in the US, a "trust deficit" in the EU, and a "stability risk" in China, operate to shape regulations. The analysis argues that these framings reflect underlying political rationalities such as market freedom, rights protection, or state control; usher in institutional logics such as precautionary legal principles or permissionless innovation; and signal techno-economic framings, such as market competitiveness or ideological stability. At the same time, somewhat paradoxically, this article identifies a recent convergence toward regulatory softening: despite divergent framings, deregulatory pressures across all three jurisdictions increasingly privilege innovation over precautionary safeguards.

The analysis draws on qualitative document analysis, centring on public policy documents, white papers, regulatory proposals, and government statements produced between 2020 and early 2025 within the three jurisdictions under study. These were selected using purposive sampling, based on their prominence in public discourse and their significance in shaping regulatory trajectories.

## 2. The Centrality of Decision Making

As noted, this article focuses on ADM. There are two principal reasons for this. First, operational decision-making constitutes the "most common purpose of deployed AI across government bodies" (House of Lords, 2024), making it analytically indispensable. Second, and more critically, the ADM nomenclature provides conceptual inclusivity, encompassing any system in which decision-making authority is partially or fully delegated to algorithms. Such terminology deliberately shifts attention from the technical architecture of systems to their endpoint: the juncture where data aggregation, algorithmic processing, and interpretive analysis converge to produce actionable outcomes (Yeung, 2017). The computational processes underpinning these models range from simple rule-based systems—like the British Home Office's rules-based ADM for immigration decisions (Booth, 2024a) or US federal agencies' Risk Classification Assessment systems (Department of Homeland Security, 2024)—to more complex machine learning algorithms, such as the UK Department for Work and Pensions' ML model for universal credit risk assessment (Department for Work and Pensions, 2024) and the Netherlands Tax and Customs administration's adaptive ML systems (Heikkilä, 2022). Rather than dissecting technical specificities, this analysis prioritises their unifying decision-making capacity. This approach also aligns with real-world policy and governance considerations. Many national regulatory policies tend to focus on the consequences of AI-driven decisions, rather than the particularities of the underlying technology. For example, the

classification rules in Article 6(3) and Recital 53 of Europe's seminal AI Act (Regulation (EU) 2024/1689, 2024) point to the importance of the decision-making function in assessing whether a system qualifies as high-risk. Similarly, within the US, ADM has become an "early target of state AI regulation," giving regulators an overarching concept to hang their policies on (Anderson et al., 2025).

This framing is particularly valuable in addressing challenges stemming from ambiguous definitions and rapid technological evolution. Take the term "artificial intelligence" (AI) as an example. Widely used as an umbrella term, it encompasses a diverse range of technologies (Wang, 2019). The difficulty of pinning down a precise definition is exemplified by the UK government: in its response to a white paper consultation on AI regulation, it explicitly avoided providing a formal definition (Department for Science, Innovation and Technology, 2023; Gallo & Nair, 2023), arguing that the fast-moving nature of the technology makes such a task impractical.

ADM thus provides a flexible and policy-relevant lens for examining the governance of algorithmic systems within the public sector. To contextualise this analysis, the following section outlines the evolving techno-economic landscape that is reshaping regulatory assumptions and priorities.

## 3. The Dynamic Context for Governance: Techno-Optimism Emerging from Stagnation and Fear

After a half-decade characterised by concern and critique, this research suggests there is a renewed (if still somewhat ambivalent) aura of excitement and techno-optimism surrounding algorithmic technologies. Fuelled by rapid technical advancements, increased investment, and growing deployment, this discourse has disrupted the relatively stable regulatory assumptions of the early 2020s and ushered in a decidedly more innovation-friendly policy climate.

### *3.1. The AI Backlash (Late 2010s–Early 2020s)*

This period, described as "the AI Backlash" (Oremus, 2023), extended the 2010s "techlash" against major technology companies (Atkinson, 2019; Neidig, 2018; Viljoen, 2021) into the realm of algorithmic technologies. Media narratives amplified an "AI technopanic" (Weiss-Blatt et al., 2024), fuelled by open letters emerging from leading scientists calling for pauses on AI production (Future of Life Institute, 2023), and warnings of "extinction level" risks (Roose, 2023). With rising public concern (Pew Research Center, 2023) prompting ambitious regulatory proposals from key global regulators (Biden, 2023; Regulation (EU) 2024/1689, 2024).

Economic indicators mirrored this mood. This period saw the first year-on-year decline in AI funding as global private investing fell 26% from 2021 to 2022 (Stanford Institute for Human-Centered Artificial Intelligence, 2023), with venture funding falling 43% in Q1 2023 (CB Insights, 2023). Uptake and development also encountered issues. AI adoption amongst organisations plateaued in the 50th percentile between 2017 and 2023 (McKinsey & Company, 2022), and developers worried about how a "data wall" would curtail technical evolution ("A.I. companies face," 2024). Moreover, there was a substantial deceleration in the number of AI patent applications (Williams & Sibley, 2022).

### 3.2. A Recent Resurgence

However, that consensus now looks outdated. Indeed, this article argues that we are at the beginning of a turnaround regarding deployment, funding, technological progress, and, as explored later, regulatory policymaking. According to McKinsey & Company's (2025) global report on the "state of AI" there has been a sharp jump in business deployment of AI, with 78% of surveyed organisations saying they now use AI in at least one business function in 2024, up from 55% on the previous year, marking a major acceleration after the period of prolonged stagnation between 2017 and 2023 (McKinsey & Company, 2025). Accompanying this are extraordinary levels of financial investment: the 2025 *Stanford AI Index* documents that 2024 saw the highest-ever global private investment in AI technologies of over $252 billion (Stanford Institute for Human-Centered Artificial Intelligence, 2025). Such implementation of algorithmic technologies is beginning to result in a notable economic impact, with recent PwC research indicating that AI adoption could boost global GDP by an additional 15 percentage points by 2035, rivalling the growth increment the world began to enjoy during the 19th-century industrialisation (PwC, 2025).

A renewed surge in AI investment and operational adoption is driven by a critical technological evolution—the rise of frontier models capable of methodically "thinking through" problems before solving them (OpenAI, 2024; Pinchai et al., 2025; xAI, 2025). These systems offer significant advantages over earlier generations (Besta et al., 2025), promising greater reliability and interpretability in real-world applications by supposedly emulating nuanced human-like reasoning. Crucially, their rapid emergence is proving disruptive to policy timelines. As European Commission President Ursula von der Leyen acknowledged at the 2025 annual EU budget conference: "[W]hen the current budget was negotiated, we thought AI would only approach human reasoning around 2050. Now we expect this to happen already next year" (Von der Leyen, 2025, para. 3).

### 3.3. Public Sector Adoption

Importantly, this intensification of AI activity is not confined to the private sector. According to *the G7 Toolkit for Artificial Intelligence in the Public Sector*: "[a]rtificial intelligence is revolutionising how governments work, offering unprecedented opportunities to deliver better public services, improve policy outcomes, enhance public sector productivity, and foster accountability" (OECD & UNESCO, 2024, p.3). Moreover, the Boston Consulting Group estimate "productivity gains of generative AI for the public sector will be valued at $1.75 trillion per year by 2033" (Carrasco et al., 2023, para. 1). These potential advantages have resulted in a substantial increase in algorithmic implementation, strategic policies, and public–private investment initiatives from key global actors, as jurisdictions compete for leadership in AI infrastructure and capabilities (Oxford Insights, 2024).

Nowhere is this adoption more evident than in the US, where the involvement of tech entrepreneurs within the government itself suggests that AI will be a dominant force in both the private and public sectors as the year progresses. Consider, for example, the US Stargate Project (OpenAI, 2025)—a $500 billion AI infrastructure initiative launched in early 2025, described by President Trump as "the largest AI infrastructure project by far in history" (Trump, 2025, para. 7). Accompanying this investment are policy instruments strongly promoting federal adoption of AI technologies. Explored later, these include the Trump Administration's Executive Orders on AI (White House, 2025a) and the accompanying guidance from the Office of Management and Budget (OMB) on AI procurement and use by federal agencies (White House, 2025b).

The US is not alone in this push. Just one month after the Stargate announcement, the EU unveiled its own public–private partnership entitled InvestAI, aiming to mobilise €200 billion to advance AI development and infrastructure across the Union. Commission President Ursula von der Leyen likened it to a "CERN for AI" (European Commission, 2025). Such effort aligns with longstanding EU ambitions to "make the public sector a trailblazer for using AI" (European Commission, 2021, p. 46), a goal that was reaffirmed in the Commission's 2024 study, which "calls for strategic AI adoptions to transform public sector services" (European Commission, 2024a).

The UK government's 2024 *Algorithmic Transparency Report* similarly exemplifies this shift. It frames AI deployment as essential for achieving "technological improvements in critical government services" (Department for Science, Innovation and Technology, 2024, para. 1). Building on this, in January 2025, the government published a plan to drive economic growth and transform the state by scaling up AI across the public sector and acting as a catalyst for private sector AI development (Department for Science, Innovation and Technology, 2025a).

A similar trajectory is also evident in China, where policymakers have long viewed AI as "critical for the future development of innovation, smart industrial systems, and digital life." (Gong & Dorwart, 2024, para. 6). This focus is particularly obvious in the "New Generation Artificial Intelligence Development Plan" (Webster et al., 2017), which emphasises AI's role in boosting economic growth, improving social services, and strengthening national security.

Governments across leading economies are realigning strategically around AI, increasingly framing it as a strategic core asset that can underpin national security and drive economic competitiveness and public sector transformation. The early 2020s "AI Backlash," characterised by declining investment, adoption plateaus, and mounting concerns over limitations and risks, now appears to have been a temporary contraction rather than a structural slowdown.

### *3.4. Some Concerns Remain*

This is not to suggest that recent public sector AI adoption has proceeded without hesitancy. Despite increased deployment and investment as governments position themselves to leverage these technologies, scepticism persists amid increasing acknowledgement of inherent safety and ethical concerns.

Some of the clearest manifestations of this balancing act—between innovation, investment, and safety concerns—emerge in foundational documents for the EU's seminal AI Act. The Commission's original white paper on AI frames the technology as a double-edged sword, noting it "brings both opportunities and risks" and stressing that "while AI can do much good…it can also do harm" (European Commission, 2020a, pp. 9, 11). Similarly, the EU's High-Level Expert Group on AI echoes these concerns, emphasising that AI systems "while bringing substantial benefits to individuals and society…also pose certain risks and may have a negative impact" (European Commission, 2019, p. 2). Such institutional caution is reinforced by non-governmental critics who challenge government AI deployment and harm-mitigation policies (Arda, 2024; Hacker, 2023; Kretschmer et al., 2023).

A broader international perspective emerged in 2025 with the *International AI Safety Report*, prepared by 96 international experts from 30 countries following the Bletchley Park AI Safety Summit (Department for

Science, Innovation and Technology & AI Safety Institute, 2025). It is essentially a cautionary account of AI's capabilities, the associated risks, and possible ways to mitigate them. The concerns raised by these reports have also resonated within academia and the wider AI research community. In February 2025, an open letter signed by AI practitioners and public figures (Milmo, 2025) endorsed an accompanying academic article setting out principles for developing responsible AI (Butlin & Lappas, 2025). Reinforcing these concerns, the *Final Report of the Pissarides Review on the Future of Work and Wellbeing*, published in early 2025 (Institute for the Future of Work, 2025), the latest in a series of cautionary accounts, underscores AI's transformative impact on employment, echoing earlier reports (Department of Education, 2023; Jung & Desikan, 2024).

Against this backdrop of increasing public-sector interest in algorithmic systems, growing institutional caution, and academic concern, mapping the actual state of ADM integration within government also faces notable blind spots. The following section explores these issues.

## 4. Public Sector Uptake Difficulties

As scholarly assessments remain divided on ADM impacts (Alhosani & Alhashmi, 2024; Contreras & Gil-García, 2024; Mergel et al., 2023), there is a growing number of widely cited instances of ADM failure in the public sector: the UK's A-level exam algorithm (Kippin & Cairney, 2022) and spousal visa AI (Stacey, 2023); US COMPAS sentencing tools (Engel et al., 2024); the Dutch childcare benefit scandal (Hadwick & Lan, 2021); and Australia's "Robodebt" (Chowdhury, 2024), are examples of recurring public-sector risks. However, despite these examples and the mounting interest and investment within public administration, the actual state of ADM deployment in government remains somewhat opaque and difficult to assess comprehensively. Some high-level inter-governmental papers and surveys concentrate upon government AI readiness, such as the OECD's (2024) *Governing with Artificial Intelligence: Are Governments Ready*? and Oxford Insights' (2024) *Government AI Readiness Index*. Certain jurisdictions, such as the EU, have released limited overviews and studies of government use of algorithmic systems (European Commission, 2023, 2024b). However, getting granular detail on system implementation, functionality, or oversight of specific ADM uses within national governments is more difficult. The OECD's November 2024 report on *Algorithmic Transparency in the Public Sector* highlights information gaps globally. Its mapping of public algorithms repositories found that most public bodies fail to provide "meaningful transparency," or "disclose pertinent and sufficient information to evaluate AI systems" (Gutiérrez & Muñoz-Cadena, 2024, p. 20). Compounding this, systematic under-reporting persists; for example, in the Netherlands, only 5% of reported AI systems are listed in the public registry (Rekenkamer, 2024), and the UK's central algorithmic registry remains sparsely populated years after launch (Booth, 2024b).

The noted OECD report attributes disclosure gaps to institutional incapacity or political reluctance, cybersecurity fears, and IP constraints. There are several cases that would support these assertions, for example, in France, the social security agency Caisse Nationale d'Allocations Familiales initially rejected freedom-of-information requests for its welfare-scoring code, arguing that disclosure would "give fraudsters the keys" (Sénécat, 2023, para. 3). In the Netherlands, indicators used by the SyRI welfare fraud detection algorithm were kept secret until a 2020 court struck down the system, noting its excessive opacity (Zuiderveen Borgesius & van Bekkum, 2021). Across the Atlantic, the US Internal Revenue Service will not release the training or methodology behind its AI-driven audit-selection model (Loricchio & Wallace, 2024).

### *4.1. UK Case Study*

In this context, the UK offers a useful exemplary case study, not least due to its 2025 blueprint "to turbocharge AI," boost public sector adoption, and "make Britain the world leader" in these technologies (Department for Science, Innovation and Technology, 2025e). Yet this ambition sits in tension with the limited public data on public ADM and the recurring challenges associated with implementation.

Historically, the UK has been a leader in governmental use of digital technologies, ranking first in the UN's (2016) e-government development index and third in the OECD's (2023) *Digital Government Index*. However, an up-to-date picture, including the range of deployment of algorithmic technologies, is more difficult to find. Following a consultation on the last *Government's National Data Strategy* (Department for Science, Innovation and Technology, 2024), a mandatory Algorithmic Transparency Recording Standard now exists. However, so far, there is only a small repository of fairly basic information (Cabinet Office, 2025). There is a clear desire to develop such technologies: the Blueprint for Modern Digital Government (Department for Science, Innovation and Technology, 2025c, p. 4) which accompanies the State of Digital Government Review (Department for Science, Innovation and Technology, 2025b), recognises the potential to "catalyse a wholesale reshaping of the public sector." However, there is also a clear recognition of the scale of the challenges that face the newly established Government Digital Service (Department for Science, Innovation and Technology, 2025c, p. 1). Perhaps as a result, a National Audit Office report from 2024 suggests a relatively small and slow uptake of AI across government, with only 37% of the 87 government bodies responding to the National Audit Office survey reporting that they deploy AI, although it is acknowledged that some 70% are piloting or planning AI systems (National Audit Office, 2024).

Financial and logistical issues impact this slow uptake. But there are also regulatory concerns. As the National Audit Report acknowledges: "Government standards and guidance to support responsible and safe adoption of AI are still under development" (National Audit Office, 2024, p. 10). Those that do exist tend to be rather general in their advice; for example, the current action plan (Department for Science, Innovation and Technology, 2025a) is largely focused upon development, with a desire for "pro-innovation" regulation. Meanwhile, the *Generative AI Framework for HM Government* (Cabinet Office, 2024) can offer only 10 principles in line with very general ideas of lawfulness and ethics, while the AI Safety Institute offers a five-step process-driven approach (AI Safety Institute, 2025). More specific policies, such as Lord Clement-Jones' private members bill on Public Authority Algorithmic and Automated Decision-Making Systems Bill (House of Lords, 2024), advance slowly.

The UK is an illustrative example of the wider international challenges posed by the current regulatory landscape and underutilisation of data repositories. Effectively, it remains difficult to determine exactly where and how algorithmic technologies are being deployed within the public sector, and, as a result, what the most pressing risks are. Amid this ambiguity, this article analyses one area of the public sector where ADM has gained major global traction: the court system. This setting offers a valuable lens through which to examine the benefits, challenges, and risks that government agencies must navigate when implementing ADM systems. Serving as a microcosm of the broader challenges surrounding ADM adoption in the public sector, particularly in the noted absence of comprehensive information on other cases of use.

### *4.2. AI in the Courts: An Exemplar*

Courts have historically been early adopters of new technologies, in part because the legal system (especially judging) has long attracted the interest of technology specialists. This may arise from a common, though reductive, perspective among computer scientists, who often view law as a more sophisticated version of games like chess or Go, where computational power is presumed to surpass human judgment. However, as Morison and Harkens (2019) point out, law is not merely about applying the "correct" rule to a given set of "facts"; it is a far more complex and socially embedded process.

Nonetheless, there is often considered to be potential for the development of AI in the court context, particularly given the promise of increased efficiency. In England and Wales alone, some 3.1 million cases pass through the courts annually. An AI system working continuously at speed might be seen to improve access to justice and reduce costs—arguments that perhaps underpin much of the UK government's support for such algorithmic systems in the judicial context (Mark et al., 2024). This trend is not unique to the UK. In the US, ADM tools such as COMPAS (Brennan & Dieterich, 2017) and Advancing Pretrial Policy & Research (APPR, 2025) have already been incorporated into judicial processes. Similarly, in Europe, models like OxRec have been trialled, with the European Commission's communication *Digitisation of Justice in the European Union: A Toolbox of Opportunities* stating: "AI applications can bring a lot of benefits" (European Commission, 2020c, p. 10). Perhaps the most ambitious initiative can be found in China, where the Supreme People's Court has issued guidance requiring courts to develop competent AI systems by 2025 (Sourdin, 2021; Supreme People's Court, 2022; Xia, 2024).

Within the judiciary itself, despite warnings that ADM systems may entrench existing data biases, undermine accountability, and erode meaningful oversight (Big Brother Watch, 2023; Public Law Project, 2023), it is perhaps relatively uncontroversial to suggest that some judicial processes are amenable to a degree of automation or assistance, with some judicial actors appearing open to such assistance. For example, Lord Justice Birss famously commented that he has used ChatGPT and found that it can be "jolly useful" in giving a summary of an area of law which he knew already (Corfield, 2023). Others go even further, using LLMs more directly in producing judgments (Digital Watch Observatory, 2023; Gutiérrez, 2024; Taylor, 2023). More ambitiously, some proponents argue that ADM tools may even be an improvement on human judging, minimising bias and operating more objectively, particularly in routine administrative decisions that follow procedural steps, such as parking fines or license applications (Alessa, 2022; Katsh & Rabinovich-Einy, 2017). However, matters involving criminal sentencing or child custody may be thought to require a more personalised, human approach. Clearly, there is a spectrum of legal decisions, from what might be seen as purely "administrative" decisions (where automation may be unproblematic) to the more obviously "judicial" (which may seem to require the input of a human; Morison & McInerney, 2025). As such, despite the promises of reduced cost and potential efficiency gains, the wholesale replacement of judges by ADM remains unlikely, but clearly, there is room and appetite for some algorithmic tools (Ministry of Justice, 2025).

Regulatory activity around ADM in the judiciary remains relatively limited, reflecting broader trends in public sector adoption of algorithmic technologies. In the EU, the 2018 European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment outlines five general principles, but it predates recent advances in generative AI. The UK has issued only brief guidance, offering high-level risk categories and

placing responsibilities on judges for all material produced (Courts and Tribunals Judiciary, 2023). In the US, judicial engagement is emerging through case law, for example, Ross v United States (2025) acknowledges AI's utility but warns against delegating decision-making. China, despite its rapid deployment of AI in courts, has given comparatively little attention to regulatory safeguards. By contrast, Australia offers a more proactive model, with a collaborative initiative between judges and academics aimed at monitoring AI developments and creating practical judicial guidance (Australian Institute of Judicial Administration, 2023).

Intriguingly, there appears to be a clear desire amongst practitioners for further guidance. The UNESCO Global Judges' Initiative (UNESCO, 2024) surveyed judicial understanding and use of AI, with 72% of respondents believing there should be mandatory rules for judges in this area (UNESCO, 2024, p. 11).

This snapshot of how ADM has been approached in the judicial context exposes the core tensions shaping its use across the public sector. It puts a focus on decision-making and stresses the values of publicness. The main issues—balancing efficiency with fairness, and technological progress with meaningful human judgment—are mirrored across other government contexts and highlight a central balancing act in the use of ADM. States increasingly prioritise algorithmic-driven modernisation, yet must reconcile these ambitions with accountability gaps where transparency and human oversight are missing. Crucially, how these tensions are understood as "problems" directly shapes governance. Therefore, the following sections analyse how key jurisdictions problematise such tensions, examining emerging policies and regulatory discourse.

## 5. Problematization

While documenting the resurgent techno-optimism, fuelled by private-sector innovation, public-sector AI adoption (e.g., judicial systems), and state ambitions, this analysis reveals fundamental tensions in governing priorities. Despite apparent enthusiasm for the transformative potential of algorithmic technologies, each jurisdiction constructs the associated risks and responsibilities in distinct ways. Crucially, jurisdictions diverge radically in framing algorithmic "problems": the US embraces light-touch governance versus the EU's precautionary paradigm, for example. To interrogate this divergence, we apply aspects of Bacchi's (2009) WPR framework. This approach examines how phenomena become constituted as governance "problems" (Foucault, 1985, p. 115) and why solutions reflect specific ideological and institutional positionalities (Miller & Rose, 2008).

While the following sections do not apply Bacchi's WPR framework in a step-by-step manner, its core analytical questions serve to guide the comparative discussion that follows. In particular, attention is paid to how ADM is problematized in each jurisdiction, what assumptions and rationalities underpin these framings, and what silences are produced. By doing so, the analysis moves beyond descriptive comparison to interrogate the underlying political rationalities, institutional logics, and techno-economic imperatives shaping governance strategies in the US, EU, and China. This approach allows for a deeper reflection on how problem representations influence governance and the broader dynamics of power and responsibility, particularly when algorithmic systems take on tasks, such as judicial or administrative decision-making, once performed exclusively by human experts.

As noted, this analysis focuses on recent domestic regulation and national policy discourse. In the context of AI regulation, Veale et al. (2023) identify six regulatory modalities, including ethical codes, industry

governance, licensing, standards, and international agreements, but highlight converging and extraterritorial domestic legislation as the most concrete. Whilst acknowledging the relevance of other approaches, this research centres on that last modality, focusing on how jurisdictions assert authority and shape norms through national domestic regulatory frameworks. This focus offers a grounded lens through which to analyse the problematization and governance of ADM systems.

## 6. Key Players

Focusing on the EU, US, and China, described by Bradford (2023) as competing "digital empires," this account sketches out their contest to shape global AI governance. Bradford maintains that because of the global nature of the digital economy, these leading regulatory models extend across jurisdictions, impacting foreign societies. Other nations are almost forced to align with one of the three models expounded by the US, EU, and China. This triadic dynamic is further illuminated by Schneider's (2025) work on digital sovereignty, which positions the EU's rights-based framework as a "third way" between the US market-driven approach and China's state-centric techno-authoritarianism. Given the noted absence of comprehensive sector-specific legislation governing ADM itself, this article concentrates upon emerging regulatory policies and related discourse, developed under the broader frameworks of AI or digital governance in general, which function as proxies through which the governance of ADM can be analysed.

### *6.1. United States*

In the US, regulation of algorithmic technologies is notably fragmented, relying on a combination of existing federal laws, non-binding guidance, and state-level initiatives rather than a single comprehensive framework. Moreover, the overarching direction set by the executive branch tends to fluctuate with the political orientation of the incumbent administration, producing distinct shifts between Republican and Democratic leadership. Yet, across these shifts, certain commonalities remain that speak to a uniquely American way of framing algorithmic problems.

For instance, recent executive initiatives, most notably the Removing Barriers to American Leadership in Artificial Intelligence Executive Order (EO 14179) and the July 2025 AI Action plan (White House, 2025c), represent a longstanding commitment to fostering an innovation-friendly environment and reflect a deep-seated political rationality of permissionless innovation (Thierer, 2016), in which regulation itself is often portrayed as a problem. This orientation draws on longstanding US traditions of free-market liberalism and deregulation, particularly in the governance of emerging technologies. A formative example is the Clinton Administration's 1997 Framework for Global Electronic Commerce. This laid the foundations for internet governance. Its first two principles, "the private sector should lead" and "governments should avoid undue restrictions on electronic commerce," rejected prior regulatory models, embracing self-regulation, enforced through market competition and tort law (White House, 1997, p. 3). Technology was constructed as a domain of market freedom rather than state control, an understanding that continues in contemporary algorithmic regulation today.

Consider, for example, the recent AI Action plan, which requires the removal of any policy "that unnecessarily hinder[s] AI development or deployment" (White House, 2025e, p. 3), a clear extension of the earlier executive order 14179 and its revocation of any "existing AI policies and directives that act as barriers to American AI

innovation" (White House, 2025d, s. 1). This deregulatory framing was further evident in the specific repeal of President Biden's expansive executive order 14110 on "safe, secure, and trustworthy development and use of artificial intelligence" (Biden, 2023). Executive order 14110 had imposed substantive obligations on federal agencies to ensure transparency, safeguard against algorithmic discrimination in public services, and manage risks in government use of AI. It was arguably the most far-reaching executive action on algorithmic governance to date. Its revocation also raises uncertainty over the future of the underlying Blueprint for an AI Bill of Rights. This was an earlier Biden-era document that acted as a "national values statement," laying out principles for safe and effective algorithmic systems, stating that citizens "should not face discrimination by algorithms" and could seek review of consequential automated decisions (Office of Science and Technology Policy, 2022, para. 6).

Further insight can be garnered from memoranda emerging from the OMB. Mandated by the AI in Government Act of 2020, these documents now constitute the de facto regulatory framework for AI systems across the US federal government. Executive Order 14179 specifically revised OMB's guidance, eliminating all references to the Blueprint for an AI Bill of Rights previously embedded in the Biden-era M-24-10/M-24-18. This revision signals a reprioritisation of objectives, with the opening directives of OMB Memorandum 25-21 stating: "Agencies must remove barriers to innovation and provide the best value for the taxpayer," "Agencies must empower AI leaders to accelerate responsible AI adoption," and "Agencies must ensure their use of AI works for the American people" (Office of Management and Budget, 2025, p2). Innovation now explicitly precedes safeguards in the regulatory hierarchy.

Effectively, the problem is currently framed as "burdensome requirements" stifling innovation (White House, 2025a), with the current administration responding with deregulatory guidance. However, it should be noted that whilst this deregulatory attitude has perhaps accelerated under the new presidency, it is reflective of historical US policymaking and the underlying political rationality of permissionless innovation. Even under the more guardrail friendly Biden administration, commitments to algorithmic safety and security were largely realised through soft law instruments, revealing a persistent reluctance to impose binding regulatory constraints on algorithmic innovation.

Indeed, there is a notable institutional logic commonality across administrations, an apparent desire to avoid new binding regulation. President Trump's first term set the tone with executive order 13859 (Trump, 2019) and the American AI Initiative, which instructed agencies to "avoid regulatory over-reach" (Office of Science and Technology Policy, 2020, p. 15) and to promote innovation within existing statutory mandates. Later, OMB Memorandum M-21-06 crystallised that approach, advising agencies that they should "consider either not taking any action" or adopt "non-regulatory approaches" when regulating these technologies (OMB, 2020). President Biden arguably preserved this preference with the Blueprint for an AI Bill of Rights (Office of Science and Technology Policy, 2022), the voluntary NIST AI-RMF (National Institute of Standards and Technology, 2023), and a range of federal agencies' voluntary guidelines and frameworks, all resting on self-assessment and voluntary commitments rather than enforceable mandates.

Consequently, individuals seeking redress for algorithmic decisions causing harm must generally rely upon existing legal frameworks and established federal agencies. For instance, the Fair Credit Reporting Act, the Civil Rights Act, and the Equal Protection Clause of the Fourteenth Amendment have been invoked in the past to challenge discriminatory outcomes produced by automated systems. Meanwhile, a joint statement from

four federal agencies, the Consumer Financial Protection Bureau, Department of Justice, Equal Employment Opportunity Commission, and Federal Trade Commission (2023) makes it clear that they will apply current sector specific legal policies to algorithmic harms, stating that "existing legal authorities apply to the use of automated systems and innovative new technologies just as they apply to other practices." However, emerging from this logic is a relative silence about rights or issues that fall outside the traditional US legal framework. For example, the right to an explanation of algorithmic decisions, a topic of discussion in the EU, is not explicitly recognised in most US regulatory policies; the Blueprint for an AI Bill of Rights hints at it but doesn't actively enforce it. Similarly, protections against more diffuse harms are not developed in US discourse.

Intriguingly, reflective of this constitutional minimalism logic, regulatory attempts to provide broader and more direct governance often do not prosper. For instance, the Algorithmic Accountability Act of 2022 (H.R. 6580), introduced in the US House of Representatives, sought to mandate impact assessments for ADM systems to mitigate potential biases. Yet, the bill stalled after being referred to the Subcommittee on Consumer Protection and Commerce and ultimately failed to pass before the 117th Congress adjourned. Such actions reveal a further representation within US policy that existing legal norms and established regulators are presumed to provide adequate cover for algorithmic harms.

It should be noted that there is perhaps more of a push for regulation at the state level, with various narrow legislative policies on AI emerging in recent years (California State Legislature, 2024; Colorado General Assembly, 2024; New York State Legislature, 2024; Virginia General Assembly, 2025). However, these state-level initiatives often face similar obstacles to those encountered at the federal level. Consider, for example, California's SB1047, which would have implemented some algorithmic safeguards on frontier models. Despite some support for this bill (Lovely, 2024; Nazzaro, 2024), opponents pushed back (Abbott, 2024; Bensinger, 2024), arguing that strict regulatory thresholds would hinder competitiveness and fail to capture the full scope of risks. As a result, the bill was vetoed by Governor Gavin Newsom in September 2024, arguably reflecting a broader, recurring pattern in US policymaking, where concerns surrounding technological leadership and stifling innovation often outweigh a call for precautionary safeguards.

Moreover, it should also be acknowledged that there is a reluctance at the executive level to allow a fragmented regulatory approach across states, with OMB guidance encouraging federal agencies to consider pre-empting state laws. More recently, a failed provision placed into a draft federal budget bill attempted to ban all state regulation of "artificial intelligence models, artificial intelligence systems, or automated decision systems' for the next ten years" (US House of Representatives, 2025). Whilst absent in the final bill, such a provision perhaps reveals a determination by some policymakers in the US to ensure that state regulation does not become a barrier to innovation and investment.

In sum, ADM governance in the US is structured in part by administration cycles, but underlying this is a durable understanding of pro-innovation political rationalities, soft-law institutional logics, and techno-economic imperatives prioritising growth dynamics that arguably also create certain blind-spots around unique algorithmic harms. In this context, innovation often outweighs other concerns for this key actor, with regulatory policy and discourse framing an "innovation gap" as a central problem. Moreover, the recent increase of deregulatory action under the current administration is perhaps the clearest illustration of the broader trend mentioned in Section 3 of this article, where regulatory design is progressively facilitating technological leadership and the pursuit of innovation over a desire for protective guardrails.

### *6.2. European Union*

The EU's approach to ADM presents a near antithesis to the innovation-led US model. Fundamentally precautionary in nature, it reflects a conviction that emerging technologies risk harming foundational concepts such as fairness, privacy, and fundamental rights, necessitating new and comprehensive regulatory architecture. This stance embodies Europe's longstanding "regulatory state" tradition (Majone, 1994) and implicitly acknowledges the inadequacy of existing legal safeguards.

This framing reflects a deeper political rationality rooted in the EU's long-standing commitment to the precautionary principle. This is a key governing approach in European regulation, originating in international environmental law and incorporated into European governance through the Maastricht Treaty 1992 and Article 191 of the Treaty on the Functioning of the European Union. It mandates that policymakers "err on the side of caution by adopting relatively stringent regulations even in cases where the scientific evidence…is unclear, inconclusive, ambiguous or uncertain" (Vogel, 2012). Although traditionally applied in areas such as environmental protection and public health, the European Commission has acknowledged that "its scope is much wider" (European Commission, 2000). Indeed, scholars suggest that the principle is increasingly shaping digital regulation, as reflected in the risk-based response of the AI Act (Howell, 2023).

The EU, therefore, views legal intervention not as a constraint on innovation, but as a precondition for societal trust and technological legitimacy, foundations considered central to the uptake and integration of AI across the single market. In this way, regulation functions as a techno-economic imperative in its own right, a necessary condition for driving long-term innovation and growth.

Central to this framing is the concept of "trustworthiness." The European Commission has expressly stated that "trustworthiness is seen as a crucial feature of European AI" and central to its vision of "human-centric" AI (European Commission, 2020b, p. 4). This "foundational ambition" (European Commission, 2019) is defined by the EU High Level Expert Group on AI as "AI that is legally compliant, ethically adherent, and socio-technically robust" (European Commission, 2020b, p. 3), reflecting aspects of the EU charter of fundamental rights. This normative ambition supports both a political and institutional logic, a rights-based regulatory culture in which public trust is to be constructed through formal legal design.

The AI Act epitomises this regulatory philosophy. Its stated purpose, "to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy AI, while ensuring a high level of protection of health, safety, and fundamental rights…" (Regulation (EU) 2024/1689, 2024, Article 1), operationalises precaution through a risk-based framework. This imposes technical safeguards, reflecting the EU's product-safety logic, effectively extending the New Legislative Framework model into the algorithmic domain. Notably, Annex III designates public sector systems affecting essential services or rights (e.g., welfare eligibility) as "high-risk" (Regulation (EU) 2024/1689, 2024, Annex III), directly subjecting state algorithmic decision-making to stringent oversight. This architecture reflects the EU's core problem framing. Here, trust is not presumed but rather constructed through regulatory compliance, and an underlying techno-regulatory optimism assumes that algorithmically induced harms can be largely mitigated, and trust engendered through pre-emptive regulatory demands.

Within this Act, and of relevance to this article, is the importance placed upon decision-making, with Article 6 and Recital 53 (Regulation (EU) 2024/1689, 2024) underscoring the centrality of the decision-making function in assessing the risk level of a system. Moreover, rather than supplanting previous regulations, the act builds upon protections found in the seminal GDPR, including Article 22, which prohibits certain decisions from being made solely by automated means (Regulation (EU) 2016/679, 2016, Art. 22). The GDPR also guarantees individuals the right to meaningful information about the logic involved in automated processing, often interpreted as a "right to explanation," Articles 13–15. There has been extensive academic and practical debate around this, (Edwards & Veale, 2018; Kaminski, 2018; Wachter et al., 2017) which the AI Act helps clarify, confirming that with high-risk systems "an affected person now has a right to meaningful explanations on the role of the AI system in the decision-making and the main elements of the decision made" (Regulation (EU) 2024/1689, 2024, Article 86). Consequently, the EU's regulatory approach to decisions made by algorithms combines a broad data protection-based restriction on fully automated decisions (GDPR, Article 22) with more targeted oversight through the AI Act's risk-based framework, again pointing to a techno-regulatory optimism. Further, this also reveals a regulatory silence, the assumption that technical transparency equates to substantive accountability, when, in practice, explanation rights often fail to address underlying power asymmetries or structural inequities.

Yet despite its rights-forward posture, recent developments reveal growing tension between the AI Act's normative ambitions and economic pragmatism. Reports suggest efforts to dilute certain provisions for a more innovation-friendly environment (Espinoza & Dubois, 2025) while techno-regulation optimists warn they are losing the narrative battle. As UN AI Advisory Board co-chair Carme Artigas contends, European companies believe the "absolute lie" that the AI Act is killing innovation (Greenacre, 2024). This friction materialised during the AI Act's late-stage negotiations, where the major economies of France, Germany, and Italy pushed to dilute the regulatory burdens for industry (Perrigo, 2023). The pressure persists post-adoption, with the European Commission VP for digital policy Henna Virkkunen recently emphasising the need to avoid "creating more reporting obligations for our companies," while cutting "red tape" (Foy & Moens, 2025). This shift signals the battle over competing techno-economic imperatives within the EU's governance logic, where competitiveness and regulatory burden are now being weighed more heavily. Perhaps "the world's regulatory superpower" (Malloy, 2023), which has often "led the charge on digital regulation" (Hobbs, 2020), is not immune to the sway of innovation and investment at the price of regulatory accountability for ADM. Consider, for example, the quiet withdrawal of the EU's AI Liability Directive, just days after the private-public €200-billion InvestAI fund was announced in February 2025.

To summarise, the EU's governance of ADM is shaped by a precautionary political rationality rooted in rights-protection and public trust, an institutional logic grounded in layered risk-based legal oversight, and a techno-economic imperative that seeks to align innovation with regulation. The overarching framing of a "trust deficit" positions ADM as a domain requiring active regulation to safeguard rights and maintain public confidence. However, recent discourse around scaling back regulatory obligations reveals a growing tension within this model, one that perhaps reflects the broader trend noted above, where the EU's commitment to regulation is increasingly tempered by global investment pressures and the perceived need to avoid excessively burdensome regulation.

### *6.3. China*

Since the release of the Next Generation AI Development Plan in 2017, authorities have consistently emphasised AI's economic potential and strategic value, with the stated aim of becoming a world leader in AI by 2030. This agenda includes public sector transformation, with a concerted push to use algorithmic technologies to increase efficiency, exemplified by the Supreme People's Court's directives to integrate AI into judicial processes, as discussed in Section 4. In this context, China's emerging regulatory framework for ADM in the public sector is shaped by the state's broader techno-economic imperative to maximise the economic and strategic benefits of algorithmic technologies through indigenousness innovation and centralised technological control.

A distinguishing feature of China's approach is a clear emphasis on ensuring that the deployment of algorithmic technologies does not pose risks to political and social stability (Gong & Dorwart, 2024; National Technical Committee, 2024; Sheehan, 2023). Algorithms are seen as economically necessary tools to improve services, enforce laws, and promote trust in society, but they can also create stability risks if not properly controlled, with official discourse warning of dangers such as the spread of misinformation or destabilising public opinion. As a result, many commentators argue that China's regulatory approach is predominantly driven by state interests rather than individual rights, as exemplified by initiatives like the widely criticised social credit scoring system (Boyer, 2022; Chin & Lin, 2022; Roberts et al., 2021; US Department of Defense, 2018; Zeng, 2020). In this logic, the "problem" is not necessarily the erosion of individual freedoms but the state's diminished capacity to maintain control. Regulation, therefore, often centres on ex-ante content control and continuous monitoring rather than ex-post mechanisms for individual redress. This approach is embedded in the Xi-era political rationality of "holistic (overall) national security" (总体国家安全观), which, as Blanchette (2020, para. 2) notes, "has come to subsume nearly all elements of policymaking and political considerations." Under this framework, security is redefined as an all-encompassing imperative that includes political, cultural, and societal stability, elevating ideological conformity and social cohesion to matters of national security, including those arising from emerging technologies (Liao, 2025).

In terms of specific governance, in the early 2020s, China's regulatory landscape for ADM moved to a more formal oversight. This period is sometimes referred to as a regulatory crackdown (Cao, 2025; Hsu, 2021). A key milestone at this time was the Personal Information Protection Law (Creemers & Webster, 2021), widely regarded as China's GDPR-like data privacy law, and notably one of the first policies to regulate ADM. It mandates that automated decisions derived from personal data be carried out transparently, fairly, and without discrimination, and grants individuals the right to an explanation and the ability to refuse certain automated decisions (Creemers & Webster, 2021). However, it contains broad exemptions for state agencies, arguably weakening protections for individuals and reinforcing a problem representation that concentrates upon protecting state interests. Indeed, the Personal Information Protection Law reflects an intriguing silence found throughout Chinese regulatory policies, which predominantly problematize algorithmic systems deployed by private platforms, casting the state as either a neutral regulator or a trustworthy user of ADM. Risks associated with state-led uses, such as those in surveillance, policing, or the Social Credit System, receive little scrutiny. As such, issues that are prominent in Western AI debates, such as due process for automated decisions or independent oversight, receive far less attention in Chinese discourse.

Reinforcing the above arguments, many Chinese policies contain a recurring requirement for algorithmic technologies to uphold "core socialist values" (Central Committee of the Communist Party of China, 2013), ensuring they do not generate outcomes that contradict the ideology of the Communist Party (Ye, 2023). For example, the Cyberspace Administration of China adopted mandatory provisions like the Internet Information Service Algorithmic Recommendation Management Provisions, which primarily addressed content curation algorithms, requiring aspects of transparency, user opt-out provisions, alongside the cultivation of "positive energy" (Cyberspace Administration of China, 2021, Art. 6), in other words, alignment with the party-state's ideological priorities. The Cyberspace Administration of China later followed with Measures for the Management of Generative AI Services (Cyberspace Administration of China, 2023), establishing content restrictions and security assessments for any public-facing generative AI tools, obligating outputs to adhere to core socialist values.

More recently, in 2024, the National Information Security Standardization Technical Committee (TC260) released its AI Safety Governance Framework, which draws upon previously established principles, including fairness, transparency, and the safeguarding of core socialist values. Whilst not a law, this framework is still influential and will likely impact any future regulations. Sheehan (2023) notes the outcome-based requirements found in these policies, such as the requirement that content again reflect socialist core values. This logic is further apparent in the 2025 AI labelling rules, which mandate both visible and machine-readable labelling of created content, to put an end to the misuse of AI generated technologies and the spread of false information (Allen & Gledhill, 2025, para. 2).

These developments illustrate the unique way ADM is problematized within China's governance of this arena, shaped by a combination of state-centric political rationalities, pre-emptive institutional logics, and techno-economic imperatives that prioritise both ideological cohesion and technological leadership. Political stability and party authority are treated as central regulatory concerns, reframing the "problem" of ADM as a "stability risk," whether that be to social harmony, core socialist values, or national security. Meanwhile, China's techno-economic ambitions position algorithmic systems as essential to domestic modernisation and global competitiveness, embedding AI into public-sector transformation while tightly managing its risks. These dynamics produce a governance model that permits some individual rights, such as transparency and contestability, but does so selectively and often with broad exemptions for state actors.

Interestingly, in what may be a response to a slowing economy, growing pressure to compete with the United States, and a recognition of the perceived economic benefits of algorithmic technologies, China has notably softened elements of its regulatory discourse since 2022. Indeed, Singer and Sheehan (2025, p. 2) note distinct regulatory phases that correspond broadly with the shifts described in Section 3 of this research, a "restrictive 'Crackdown Era' (2020–late 2022), when the CCP reasserted control over tech companies," followed by a more "pragmatic 'Catch-Up Era' (2022–early 2025), that loosened restrictions to boost economic growth." This latter phase is perhaps best exemplified by the 2023 Interim Measures for Generative AI Services, which were noticeably lighter than the original draft following industry pushback (Sun & Zeng, 2024). Notably, Article 3 of the final version commits regulators to a policy of "tolerant and cautious graded management" that seeks to "encourage innovation" (Cyberspace Administration of China, 2023, Art. 3).

## 7. Conclusion

As this Bacchi-inspired analysis reveals, divergent problem framings drive distinct ADM governance approaches across jurisdictions as they engage with increasing use of this technology in the public sector. The US innovation gap framing supports a deregulatory agenda that prioritises market-led innovation. The EU emphasises a trust deficit that warrants stronger regulation to protect fundamental rights and garner trust. Meanwhile, China's repeated desire to maintain social stability and core socialist values results in ADM as a stability risk, requiring some unique outcome-focused regulatory requirements.

These digital empires channel common safety challenges through nationally distinct governance pathways, whether through existing law and federal agencies in the US, new EU rights-based legislation, or China's collectivist regulatory mechanisms. Yet, concurrently, a convergent regulatory softening emerges. This convergence risks a governance paradox: even as states recognise AI's novel risks, their policy actions replicate the very "move fast and break things" ethos that contributed to the 2020s backlash, potentially sacrificing long-term public trust for short-term gains.

The regulatory softening and diminishing post-2020s accountability mechanisms are likely driven by renewed techno-optimism, economic competitiveness pressures, national security imperatives, and/or global leadership ambitions. While most visible in US deregulatory actions, parallel shifts emerge in EU discourse and China's innovation-prioritising actions.

Crucially, despite divergent problem framings (innovation gap vs. trust deficit vs. stability risk), all three digital empires increasingly privilege innovation over accountability, lured by service transformation promises and the elusive prize of sustained economic growth.

### Acknowledgments

The authors wish to thank the School of Law, Queen's University Belfast, for its support and membership agreement, which allowed us to undertake this work. David Mark gratefully acknowledges the support of the Leverhulme Interdisciplinary Network on Algorithmic Solutions (LINAS) during this project.

### Funding

Publication of this article in open access was made possible through the institutional membership agreement between Queen's University Belfast and Cogitatio Press.

### References

Abbott, A. (2024). *Coalition letter opposing California SB 1047*. Law & Economics Center. https://laweconcenter.org/resources/coalition-letter-opposing-california-sb-1047

Advancing Pretrial Policy & Research. (2025). *About the public safety assessment*. https://advancingpretrial.org/psa/factors

A.I. companies face new restrictions on data use. (2024, July 19). *The New York Times*. https://www.nytimes.com/2024/07/19/technology/ai-data-restrictions.html

AI Safety Institute. (2025). *Principles for safeguard evaluation*. https://www.aisi.gov.uk/work/principles-for-safeguard-evaluation

Alessa, H. (2022). The role of artificial intelligence in online dispute resolution: A brief and critical overview. *Information & Communications Technology Law*, *31*(3), 319–334.

Alhosani, K., & Alhashmi, S. (2024). Opportunities, challenges, and benefits of AI innovation in government services: A review. *Discover Artificial Intelligence*, *4*, Article 18.

Allen & Gledhill. (2025, April 2). *China further regulates AI-generated content*. https://www.allenandgledhill.com/cn/publication/articles/30284/further-regulates-ai-generated-content

Anderson, H., Reem, N., & Susas, J. (2025, March 7). *Automated decision-making emerges as an early target of state AI regulation*. White & Case LLP. https://www.whitecase.com/insight-alert/automated-decision-making-emerges-early-target-state-ai-regulation

Arda, O. (2024). The European Union's AI Act: Navigating exemptions and ensuring comprehensive safety. *Journal of European Technology Law*, *15*(2), 45–67.

Atkinson, R. (2019). *A policymaker's guide to the "techlash"—What it is and why it's a threat to growth and progress*. Information Technology & Innovation Foundation. https://itif.org/publications/2019/10/28/policymakers-guide-techlash

Australian Institute of Judicial Administration. (2023). *AI decision-making and the courts: A guide for judges, tribunal members and court administrators*. https://ssrn.com/abstract=4162985

Bacchi, C. (2009). *Analysing policy: What's the problem represented to be?* Pearson Education.

Bensinger, G. (2024, August 21). Big Tech wants AI to be regulated. Why do they oppose a California AI bill? *Reuters*. https://www.reuters.com/technology/artificial-intelligence/big-tech-wants-ai-be-regulated-why-do-they-oppose-california-ai-bill-2024-08-21

Besta, M., Barth, J., Schreiber, E., Kubicek, A., Catarino, A., Gerstenberger, R., Nyczyk, P., Iff, P., Li, Y., Houliston, S., Sternal, T., Copik, M., Kwaśniewski, G., Müller, J., Flis, Ł., Eberhard, H., Niewiadomski, H., & Hoefler, T. (2025). *Reasoning language models: A blueprint*. arXiv. https://arxiv.org/pdf/2501.11223v3

Biden, J. R. (2023). *Safe, secure, and trustworthy development and use of artificial intelligence* (Executive Order 14110). Federal Register. https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence

Big Brother Watch. (2023). *Big Brother Watch's response to the government's consultation the "A pro-innovation approach to AI regulation" white paper*. https://bigbrotherwatch.org.uk/wp-content/uploads/2023/06/Big-Brother-Watch-response-to-Govt-White-Paper-on-AI.pdf

Blanchette, J. (2020). *Ideological security as national security*. Center for Strategic & International Studies. https://www.csis.org/analysis/ideological-security-national-security

Booth, R. (2024a, November 11). AI tool could influence Home Office immigration decisions, critics say. *The Guardian*. https://www.theguardian.com/uk-news/2024/nov/11/ai-tool-could-influence-home-office-immigration-decisions-critics-say

Booth, R. (2024b, November 28). UK government failing to list use of AI on mandatory register. *The Guardian*. https://www.theguardian.com/technology/2024/nov/28/uk-government-failing-to-list-use-of-ai-on-mandatory-register

Boyer, R. (2022). Platform capitalism: A socio-economic analysis. *Socio-Economic Review*, *20*(4), 1857–1885.

Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press.

Brennan, T., & Dieterich, W. (2017). Correctional offender management profiles for alternative sanctions (COMPAS). In F. E. Cullen, P. Wilcox, & J. M. Lux (Eds.), *Handbook of recidivism risk/needs assessment tools* (pp. 49–75). Wiley. https://doi.org/10.1002/9781119184256.ch3

Butlin, P., & Lappas, T. (2025). *Principles for responsible AI consciousness research*. ResearchGate. https://www.researchgate.net/publication/387975909_Principles_for_Responsible_AI_Consciousness_Research

Cabinet Office. (2024). *Generative AI framework for HMG*. UK Government. https://www.gov.uk/government/publications/generative-ai-framework-for-hmg

Cabinet Office. (2025). *Find out how algorithmic tools are used in public organisations*. UK Government. https://www.gov.uk/algorithmic-transparency-records

California State Legislature. (2024). *Safe and secure innovation for frontier artificial intelligence models act* (Senate Bill 1047).

Cao, A. (2025, January 27). China's Weibo adjusts algorithms to improve 'public values' amid government crackdown. *South China Morning Post*. https://www.scmp.com/tech/big-tech/article/3296450/chinas-weibo-adjusts-algorithms-improve-public-values-amid-government-crackdown

Carrasco, M., Habib, C., Felden, F., Sargeant, R., Mills, S., Shenton, S., Ingram, J., & Dando, G. (2023). *Generative AI for the public sector: From opportunities to value*. BCG. https://www.bcg.com/publications/2023/unlocking-genai-opportunities-in-the-government

CB Insights. (2023). *State of AI Q1'23 report*. https://s3-us-west-2.amazonaws.com/cbi-content/reports/CB-Insights_Artificial-Intelligence-Report-Q1-2023.pdf

Central Committee of the Communist Party of China. (2013, December 23). *Decision of the Central Committee of the Communist Party of China on some major issues concerning comprehensively deepening reform*. Xinhua. http://www.gov.cn/jrzg/2013-11/15/content_2528179.htm

Chin, J., & Lin, L. (2022). *Surveillance state: Inside China's quest to launch a new era of social control*. St. Martin's Publishing Group.

Chowdhury, S. (2024). Technology is never neutral: Robodebt and a human rights analysis of automated decision-making on welfare recipients. *Australian Journal of Human Rights*, *30*(1), 20–40. https://doi.org/10.1080/1323238X.2024.2409620

Colorado General Assembly. (2024). *Colorado artificial intelligence act* (Senate Bill 24-205).

Consumer Financial Protection Bureau, Department of Justice, Equal Employment Opportunity Commission, & Federal Trade Commission. (2023). *Joint statement on enforcement efforts against discrimination and bias in automated systems*. https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf

Contreras, R., & Gíl-García, J. (2024). Exploring the negative impacts of artificial intelligence in government: The dark side of intelligent algorithms and cognitive machines. *International Review of Administrative Sciences*, *90*(2), 353–368.

Corfield, G. (2023, September 14). 'British judge uses "jolly useful" ChatGPT to write ruling.' *The Telegraph*. https://www.telegraph.co.uk/business/2023/09/14/british-judge-uses-jolly-useful-chatgpt-to-write-ruling

Courts and Tribunals Judiciary. (2023). *Artificial intelligence (AI): Judicial guidance*. https://www.judiciary.uk/wp-content/uploads/2023/12/AI-Judicial-Guidance.pdf

Creemers, R., & Webster, G. (2021). *Translation: Personal information protection law of the People's Republic of China—Effective Nov. 1, 2021*. DigiChina. https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021

Cyberspace Administration of China. (2021). *Internet information service algorithmic recommendation management provisions*.

Cyberspace Administration of China. (2023). *Interim measures for the management of generative artificial intelligence services*.

Department for Science, Innovation and Technology. (2023). *A pro-innovation approach to AI regulation: Government response*. UK Government. https://www.gov.uk/government/consultations/ai-regulation-a-pro-innovation-approach-policy-proposals/outcome/a-pro-innovation-approach-to-ai-regulation-government-response

Department for Science, Innovation and Technology. (2024). *New records detail how AI helps government make quick, accurate decisions to boost trade, speed up responses and more*. UK Government. https://www.gov.uk/government/news/new-records-detail-how-ai-helps-government-make-quick-accurate-decisions-to-boost-trade-speed-up-responses-and-more

Department for Science, Innovation and Technology. (2025a). *AI opportunities action plan* (CP 1241). UK Government. https://www.gov.uk/government/publications/ai-opportunities-action-plan/ai-opportunities-action-plan

Department for Science, Innovation and Technology. (2025b). *State of digital government review* (CP 1251). UK Government. https://www.gov.uk/government/publications/state-of-digital-government-review/state-of-digital-government-review

Department for Science, Innovation and Technology. (2025c). *A blueprint for modern digital government* (CP 1252). UK Government. https://www.gov.uk/government/publications/a-blueprint-for-modern-digital-government

Department for Science, Innovation and Technology. (2025d). *Prime minister sets out blueprint to turbocharge AI*. UK Government. https://www.gov.uk/government/news/prime-minister-sets-out-blueprint-to-turbocharge-ai

Department for Science, Innovation and Technology & AI Safety Institute. (2025). *International AI safety report 2025* (DSIT research paper series no. 2025/001). Crown Copyright. https://assets.publishing.service.gov.uk/media/679a0c48a77d250007d313ee/International_AI_Safety_Report_2025_accessible_f.pdf

Department for Work and Pensions. (2024). *DWP annual report and accounts 2023 to 2024*. UK Government. https://www.gov.uk/government/publications/dwp-annual-report-and-accounts-2023-to-2024

Department of Education. (2023). *The impact of AI on UK jobs and training*. https://assets.publishing.service.gov.uk/media/656856b8cc1ec500138eef49/Gov.UK_Impact_of_AI_on_UK_Jobs_and_Training.pdf

Department of Homeland Security. (2024). *AI at DHS: A deep dive into our use case inventory*. UK Government. https://www.dhs.gov/archive/news/2024/12/16/ai-dhs-deep-dive-our-use-case-inventory

Digital Watch Observatory. (2023). *Indian judge used ChatGPT in a criminal case*. https://dig.watch/updates/indian-judge-used-chatgpt-in-a-criminal-case

Edwards, L., & Veale, M. (2018). *Enslaving the algorithm: From a "right to an explanation" to a "right to better decisions"*? arXiv. https://arxiv.org/abs/1803.07540

Engel, C., Linhardt, L., & Schubert, M. (2024). Code is law: How COMPAS affects the way the judiciary handles the risk of recidivism. *Artificial Intelligence and Law*, *33*, 383–404. https://doi.org/10.1007/s10506-024-09389-8

Espinoza, J., & Dubois, L. (2025, March 25). EU lawmakers warn against 'dangerous' moves to water down AI rules. *Financial Times*. https://www.ft.com/content/9051af42-ce3f-4de1-9e68-4e0c1d1de5b5

European Commission. (2000). *Communication from the Commission on the precautionary principle* (COM(2000) 1 final). https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0001:FIN:EN:PDF

European Commission. (2019). *Ethics guidelines for trustworthy AI*. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

European Commission. (2020a). *White paper on artificial intelligence: A European approach to excellence and trust*. https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

European Commission. (2020b). *Sectoral considerations on the policy and investment recommendations for*

*trustworthy artificial intelligence*. Publications Office of the European Union. https://futurium.ec.europa.eu/en/european-ai-alliance/community-content/ai-hleg-sectoral-considerations-policy-and-investment-recommendations-trustworthy-ai

European Commission. (2020c). *Digitalisation of justice in the European Union: A toolbox of opportunities* (COM(2020) 710 final). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2020:710:FIN

European Commission. (2021). *Coordinated plan on artificial intelligence 2021 review*. https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review

European Commission. (2023). *AI watch: European landscape on the use of Artificial intelligence by the public sector*. https://interoperable-europe.ec.europa.eu/sites/default/files/custom-page/attachment/2023-02/JRC129301_01_AI_watch.pdf

European Commission. (2024a). *EU study calls for strategic AI adoption to transform public sector services*. https://digital-strategy.ec.europa.eu/en/library/eu-study-calls-strategic-ai-adoption-transform-public-sector-services

European Commission. (2024b). *The potential of generative AI for the public sector: Current use, key questions and policy considerations*. https://interoperable-europe.ec.europa.eu/collection/public-sector-tech-watch/document/potential-generative-ai-public-sector-current-use-key-questions-and-policy-considerations

European Commission. (2025, February 11). *EU launches InvestAI initiative to mobilise €200 billion of investment in artificial intelligence* [Press release]. https://digital-strategy.ec.europa.eu/en/news/eu-launches-investai-initiative-mobilise-eu200-billion-investment-artificial-intelligence

Foucault, M. (1985). *Discourse and truth: The problematization of parrhesia*. Northwestern University Press.

Foy, H., & Moens, B. (2025, February 14). EU scales back tech rules to boost AI investment, says digital chief. *Financial Times*. https://www.ft.com/content/fde53886-4295-4066-a704-b8cf5f388800

Future of Life Institute. (2023). *Pause giant AI experiments: An open letter*. https://futureoflife.org/open-letter/pause-giant-ai-experiments

Gallo, V., & Nair, S. (2023). *The UK's framework for AI regulation*. Deloitte. https://www2.deloitte.com/uk/en/blog/emea-centre-for-regulatory-strategy/2024/the-uks-framework-for-ai-regulation.html

Gong, J., & Dorwart, H. (2024). *AI governance in China: Strategies, initiatives, and key considerations*. Bird & Bird. https://www.twobirds.com/en/insights/2024/china/ai-governance-in-china-strategies-initiatives-and-key-considerations

Greenacre, M. (2024, December 5). EU is 'losing the narrative battle' over AI Act, says UN adviser. *Science|Business*. https://sciencebusiness.net/news/ai/eu-losing-narrative-battle-over-ai-act-says-un-adviser

Gutiérrez, J. (2024). A critical appraisal of large language models in judicial decision-making. In R. Paul, E. Carmel, & J. Cobbe (Eds.), *Handbook on public policy and artificial intelligence* (p. 328–338) Edward Elgar.

Gutiérrez, J. D., & Muñoz-Cadena, S. (2024). *Algorithmic transparency in the public sector: A state-of-the-art report of algorithmic transparency instruments*. Global Partnership on Artificial Intelligence. https://wp.oecd.ai/app/uploads/2024/12/14-Algorithmic-Transparency-in-the-Public-Sector-A-state-of-the-art-report-of-algorithmic-transparency-instruments.pdf

Hacker, P. (2023). The European AI liability directives—Critique of a half-hearted approach and lessons for the future. *Computer Law & Security Review, 51*, Article 105871.

Hadwick, D., & Lan, S. (2021). Lessons to be learned from the Dutch childcare allowance scandal: A comparative review of algorithmic governance by tax administrations in the Netherlands, France and Germany. *World Tax Journal, 13*(4), 609–645. https://www.ibfd.org/shop/journal/lessons-be-learned-dutch-childcare-allowance-scandal-comparative-review-algorithmic

Heikkilä, M. (2022, March 29). Dutch scandal serves as a warning for Europe over risks of using algorithms. *Politico*. https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms

Hobbs, C. (2020, April 8). The EU as a digital regulatory superpower: Implications for the United States. *European Council on Foreign Relations*. https://ecfr.eu/article/commentary_the_eu_as_a_digital_regulatory_superpower_implications_for_the_u

House of Lords. (2024). *Public authority algorithmic and automated decision-making systems bill*. https://bills.parliament.uk/bills/3760

Howell, B. (2023). *The precautionary principle, safety regulation, and AI: This time, it really is different*. American Enterprise Institute. https://www.aei.org/research-products/report/the-precautionary-principle-safety-regulation-and-ai-this-time-it-really-is-different

Hsu, S. (2021, November 1). China's regulatory clampdown on Big Tech: Motivations and the American response. *Institute for China-America Studies*. https://chinaus-icas.org/research/chinas-regulatory-clampdown-on-big-tech

Institute for the Future of Work. (2025). *Final report of the Pissarides review into the future of work and wellbeing*. https://cdn.prod.website-files.com/64d5f73a7fc5e8a240310c4d/679baff5f45270c64b9bda11_TPR-FinalReport-26-01-25v4.pdf

Jung, C., & Desikan, B. S. (2024). *Transformed by AI: How generative artificial intelligence could affect work in the UK—And how to manage it*. IPPR. https://www.ippr.org/articles/transformed-by-ai

Kaminski, M. E. (2018). *The right to explanation, explained*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3196985

Katsh, E., & Rabinovich-Einy, O. (2017). *Digital justice: Technology and the internet of disputes*. Oxford University Press.

Kippin, S., & Cairney, P. (2022). The Covid-19 exams fiasco across the UK: Four nations and two windows of opportunity. *British Politics*, *17*, 1–23. https://doi.org/10.1057/s41293-021-00162-y

Kretschmer, M., Kretschmer, T., Peukert, A., & Peukert, C. (2023). *The risks of risk-based AI regulation: Taking liability seriously*. arXiv. https://arxiv.org/abs/2311.14684

Liao, K. (2025). *Uphold the predominant position of political security*. (Original work published April 2022). https://www.strategictranslation.org/articles/chapter-six-persevere-in-placing-political-security-in-the-predominant-position

Loricchio, L., & Wallace, C. (2024, October 21). Transparency, oversight urged for IRS artificial intelligence. *Tax Notes*. https://www.taxnotes.com/featured-news/transparency-oversight-urged-irs-artificial-intelligence/2024/10/21/7m6nv

Lovely, G. (2024, September 11). SAG-AFTRA and women's groups urge Gavin Newsom to sign AI safety bill. *The Verge*. https://www.theverge.com/2024/9/11/24242142/sagaftra-ai-now-gavin-newsom-safety-sb-1047-letters

Majone, G. (1994). The rise of the regulatory state in Europe. *West European Politics*, *17*(3), 77–101.

Malloy, D. (2023, June 15). The world's regulatory superpower is taking on a regulatory nightmare: Artificial intelligence. *Atlantic Council*. https://www.atlanticcouncil.org/blogs/new-atlanticist/the-worlds-regulatory-superpower-is-taking-on-a-regulatory-nightmare-artificial-intelligence

Mark, D., McInerney, T., & Morison, J. (2024). Regulating automated decision-making in the justice system: What is the problem? In R. Paul, E. Carmel, & J. Cobbe (Eds.), *Handbook on public policy and artificial intelligence*. Edward Elgar Publishing. https://www.elgaronline.com/edcollchap/book/9781803922171/book-part-9781803922171-34.xml

McKinsey & Company. (2022). *The state of AI in 2022—And a half-decade in review*. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2022-and-a-half-decade-in-review

McKinsey & Company. (2025). *The state of AI: How organizations are rewiring to capture value*. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai

Mergel, I., Dickinson, H., Stenvall, J., & Gasco, M. (2023). Implementing AI in the public sector. *Public Management Review*. Advance online publication. https://doi.org/10.1080/14719037.2023.2231950

Miller, P., & Rose, N. (2008). *Governing the present: Administering economic, social and personal life*. Polity Press.

Milmo, D. (2025, February 3). AI systems could be 'caused to suffer' if consciousness achieved, says research. *The Guardian*. https://www.theguardian.com/technology/2025/feb/03/ai-systems-could-be-caused-to-suffer-if-consciousness-achieved-says-research

Ministry of Justice. (2025, July 31). *AI action plan for justice*. GOV.UK. https://www.gov.uk/government/publications/ai-action-plan-for-justice/ai-action-plan-for-justice

Morison, J., & Harkens, A. (2019). Re-engineering justice? Robot judges, computerized courts and (semi) automated legal decision-making. *Legal Studies*, *39*(4), 618–635.

Morison, J., & McInerney, T. (2025). When should a computer decide? Judicial decision-making in the age of automation, algorithms and generative artificial intelligence. In S. Turenne & M. Moussa (Eds.), *Research handbook on judging and the judiciary*. Elgar; Routledge. https://www.researchgate.net/publication/378610409_When_should_a_computer_decide_Judicial_decision-making_in_the_age_of_automation_algorithms_and_generative_artificial_intelligence

National Audit Office. (2024). *Use of artificial intelligence in government*. https://www.nao.org.uk/wp-content/uploads/2024/03/use-of-artificial-intelligence-in-government.pdf

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework* (AI RMF 1.0) (NIST AI 100-1). U.S. Department of Commerce.

National Technical Committee. (2024). *AI safety governance framework*. https://www.tc260.org.cn/upload/2024-09-09/1725849192841090989.pdf

Nazzaro, M. (2024, September 9). AI employees voice support for California regulation bill. *The Hill*. https://thehill.com/policy/technology/4869225-ai-employees-support-california-ai-bill

Neidig, H. (2018, January 10). Chamber of Commerce President warns against growing 'techlash.' *The Hill*. https://thehill.com/policy/technology/368331-chamber-of-commerce-president-warns-against-growing-techlash

New York State Legislature. (2024). *An act to amend the executive law in relation to requiring state agencies to evaluate and report on their use of artificial intelligence software* (Assembly Bill A.5672).

Office of Management and Budget. (2020). *M-21-06: Guidance for regulation of artificial intelligence applications*. Executive Office of the President.

Office of Management and Budget. (2025). *Memorandum M-25-21: Advancing governance, innovation, and risk management for agency use of artificial intelligence.* Executive Office of the President of the United States.

Office of Science and Technology Policy. (2020). *American artificial intelligence initiative: Year one annual report*. Executive Office of the President.

Office of Science and Technology Policy. (2022). *Blueprint for an AI Bill of Rights: Making automated systems work for the American people*. The White House. https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights

OpenAI. (2024). *Learning to reason with LLMs*. https://openai.com/index/learning-to-reason-with-llms

OpenAI. (2025). *Announcing the stargate project*. https://openai.com/index/announcing-the-stargate-project

Oremus, W. (2023, April 4). The AI backlash is here. It's focused on the wrong things. *The Washington Post*. https://www.washingtonpost.com/technology/2023/04/04/musk-ai-letter-pause-robots-jobs

Organisation for Economic Co-operation and Development. (2023). *OECD digital government index*. https://www.oecd.org/en/publications/2023-oecd-digital-government-index_1a89ed5e-en.html

Organisation for Economic Co-operation and Development. (2024). *Governing with artificial intelligence: Are governments ready?* (OECD Artificial Intelligence Papers, No. 20). https://doi.org/10.1787/26324bc2-en

Organisation for Economic Co-operation and Development, & UNESCO. (2024). *G7 toolkit for artificial intelligence in the public sector*. https://doi.org/10.1787/421c1244-en

Oxford Insights. (2024). *Government AI readiness index 2024*. https://oxfordinsights.com/ai-readiness/ai-readiness-index

Perrigo, B. (2023, August 1). E.U.'s AI regulation could be softened after pushback from biggest members. *TIME*. https://time.com/6338602/eu-ai-regulation-foundation-models

Pew Research Center. (2023). *What the data says about Americans' views of artificial intelligence*. https://www.pewresearch.org/short-reads/2023/11/21/what-the-data-says-about-americans-views-of-artificial-intelligence

Pinchai, S., Hassabis, D., & Kavukcuoglu, K. (2025). *Introducing Gemini: Redefining AI with integrated reasoning*. Google. https://blog.google/technology/google-deepmind/google-gemini-ai-update-december-2024

Public Law Project. (2023). *Written evidence to the Justice and Home Affairs Committee (NTL0046): Technology rules? The advent of new technologies in the justice system*. https://committees.parliament.uk/writtenevidence/39761/html

PwC. (2025). *AI adoption could boost global GDP by an additional 15 percentage points by 2035, as global economy is reshaped*. https://www.pwc.com/gx/en/news-room/press-releases/2025/ai-adoption-could-boost-global-gdp-by-an-additional-15-percentage.html

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). (2016). *Official Journal of the European Union*, L 119.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act). (2024). *Official Journal of the European Union*, L 2024/1689. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Rekenkamer, A. (2024). Netherlands Court of audit, *focus op AI bij de rijksoverheid*. https://www.rekenkamer.nl/publicaties/rapporten/2024/10/16/focus-op-ai-bij-de-rijksoverheid

Roberts, H., Cowls, J., Morley, J., Taddeo, M., & Floridi, L. (2021). The Chinese approach to artificial intelligence: An analysis of policy, ethics, and regulation. In L. Floridi (Ed.), *Ethics, governance, and policies in artificial intelligence* (pp. 23–51). Springer.

Roose, K. (2023, May 30). A.I. poses 'risk of extinction,' industry leaders warn. *The New York Times*. https://www.nytimes.com/2023/05/30/technology/ai-threat-warning.html

Ross v. United States, 23-CM-1067 (D.C. Ct. App) (2025). https://law.justia.com/cases/district-of-columbia/court-of-appeals/2025/23-cm-1067.html

Schneider, I. (2025). *Reclaiming digital sovereignty: The EU's role in the geopolitics of digital governance* (Policy Paper No. 1). Center for the Governance of Change. https://static.ie.edu/CGC/CGC_ReclaimingDigitalSovereignty_PolicyPaper.pdf

Sénécat, A. (2023, December 5). The use of opaque algorithms facilitates abuses within public services. *Le Monde*. https://www.lemonde.fr/en/les-decodeurs/article/2023/12/05/the-use-of-opaque-algorithms-facilitates-abuses-within-public-services_6314051_8.html

Sheehan, M. (2023, July 12). China's AI regulations and how they get made. *Carnegie Endowment for International Peace*. https://carnegieendowment.org/research/2023/07/chinas-ai-regulations-and-how-they-get-made?lang=en

Singer, J., & Sheehan, M. (2025). *China's AI policy at the crossroads: Balancing development and control in the DeepSeek era*. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2025/07/chinas-ai-policy-in-the-deepseek-era?lang=en

Sourdin, T. (2021). *Judges, technology and artificial intelligence: The artificial judge*. Edward Elgar.

Stacey, K. (2023, October 23). UK officials use AI to decide on issues from benefits to marriage licences. *The Guardian*. https://www.theguardian.com/technology/2023/oct/23/uk-officials-use-ai-to-decide-on-issues-from-benefits-to-marriage-licences

Stanford Institute for Human-Centered Artificial Intelligence. (2023). *AI index report 2023*. https://hai.stanford.edu/ai-index/2023-ai-index-report

Stanford Institute for Human-Centered Artificial Intelligence. (2025). *AI index report 2025*. https://hai.stanford.edu/ai-index/2025-ai-index-report

Sun, Y., & Zeng, J. (2024, April 22). China's interim measures for the management of generative AI services: A comparison between the final and draft versions of the text. *Future of Privacy Forum*. https://fpf.org/blog/chinas-interim-measures-for-the-management-of-generative-ai-services-a-comparison-between-the-final-and-draft-versions-of-the-text

Supreme People's Court. (2022). *Chinese courts must implement AI system by 2025*. https://english.court.gov.cn/2022-12/12/c_838810.htm

Taylor, L. (2023, February 3). Colombian judge says he used ChatGPT in ruling. *The Guardian*. https://www.theguardian.com/technology/2023/feb/03/colombia-judge-chatgpt-ruling

Thierer, A. D. (2016). *Permissionless innovation: The continuing case for comprehensive technological freedom*. Mercatus Center at George Mason University.

Trump, D. J. (2019). *Maintaining American leadership in artificial intelligence* (Executive Order No. 13859). Federal Register. https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence

Trump, D. J. (2025). *Remarks on artificial intelligence infrastructure development and an exchange with reporters*. The American Presidency Project. https://www.presidency.ucsb.edu/documents/remarks-artificial-intelligence-infrastructure-development-and-exchange-with-reporters

UNESCO. (2024). *UNESCO global judges' initiative: Survey on the uses of AI systems by judicial operators*. https://unesdoc.unesco.org/ark:/48223/pf0000389786

United Nations. (2016). *UN e-government survey 2016*. https://publicadministration.un.org/egovkb/en-us/reports/un-e-government-survey-2016

US Department of Defense. (2018). *AI, China, Russia, and the global order: Technological, political, global, and creative perspectives*. Defense Technical Information Center. https://apps.dtic.mil/sti/citations/AD1066673

US House of Representatives. (2025). *Majority memorandum for May 13, 2025, Committee on Energy and Commerce markup*. https://docs.house.gov/meetings/IF/IF00/20250513/118261/HMKP-119-IF00-20250513-SD003.pdf

Veale, M., Matus, K., & Gorwa, R. (2023). AI and global governance: Modalities, rationales, tensions. *Annual Review of Law and Social Science*, *19*, 255–274.

Viljoen, S. (2021). The promise and limits of lawfulness: Inequality, law, and the techlash. *Journal of Social Computing*, *2*(3), 284–296.

Virginia General Assembly. (2025). *High-risk artificial intelligence developer and deployer act* (House Bill 2094).

Vogel, D. (2012). *The politics of precaution: Regulating health, safety, and environmental risks in Europe and the United States*. Princeton University Press.

Von der Leyen, U. (2025, May 20). *Speech by President von der Leyen at the Annual EU Budget Conference 2025* [Speech transcript]. European Commission. https://ec.europa.eu/commission/presscorner/detail/nl/speech_25_1284

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, *7*(2), 76–99.

Wang, P. (2019). On defining artificial intelligence. *Journal of Artificial General Intelligence*, *10*(2), 1–37. https://doi.org/10.2478/jagi-2019-0002

Webster, G., Creemers, R., Kania, E., & Triolo, P. (2017). *Full translation: China's "New Generation Artificial Intelligence Development Plan" (2017)*. DigiChina. https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017

Weiss-Blatt, N., Thierer, A., & Barkley, T. (2024). *The AI technopanic and its effects: A primer*. Abundance Institute. https://api.slash.am/storage/v1/object/public/page_uploads/ed9aed01-09a1-4d95-be93-405ccebe50dd/articles/1719857803918/the-ai-technopanic-and-its-effects.pdf

White House. (1997). *A framework for global electronic commerce*. https://clintonwhitehouse4.archives.gov/WH/New/Commerce

White House. (2025a). *Fact sheet: President Donald J. Trump takes action to enhance America's AI leadership*. https://www.whitehouse.gov/fact-sheets/2025/01/fact-sheet-president-donald-j-trump-takes-action-to-enhance-americas-ai-leadership

White House. (2025b). *White House releases new policies on federal agency AI use and procurement*. https://www.whitehouse.gov/articles/2025/04/white-house-releases-new-policies-on-federal-agency-ai-use-and-procurement

White House. (2025c. *Winning the race: America's AI Action Plan*. https://www.whitehouse.gov/articles/2025/07/white-house-unveils-americas-ai-action-plan

White House. (2025d). *Executive order 14179: Removing barriers to American leadership in artificial intelligence*. Federal Register. https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence

White House. (2025e). *Winning the race: America's AI Action Plan*. https://www.whitehouse.gov/ai-action-plan

Williams, M., & Sibley, L. (2022, May 20). *AI report 2022*. Marks & Clerk. https://www.marks-clerk.com/insights/news/102jvti-ai-report-2022

xAI. (2025). *The age of reasoning agents*. https://x.ai/blog/grok-3

Xia, Y. (2024). Research on judicial trial practice issues of internet courts in China. *Science of Law Journal*, *3*, 174–179.

Ye, J. (2023, July 13). China says generative AI rules to apply only to products for the public. *Reuters*. https://www.reuters.com/technology/china-issues-temporary-rules-generative-ai-services-2023-07-13

Yeung, K. (2017). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, *12*(4), 505–523. https://doi.org/10.1111/rego.12158

Zeng, J. (2020). Artificial intelligence and China's authoritarian governance. *International Affairs*, *96*(6), 1441–1458.

Zuiderveen Borgesius, F., & van Bekkum, M. (2021, September 23). Digital welfare fraud detection and the Dutch SyRI judgment. *International Association of Privacy Professionals*. https://iapp.org/news/a/digital-welfare-fraud-detection-and-the-dutch-syri-judgment

## About the Authors

David Mark has completed his PhD within the Leverhulme Interdisciplinary Network on Algorithmic Solutions (LINAS) programme at Queen's University Belfast. His work explores the intricacies of safety, security, and legal compliance in AI decision-making systems. A former barrister, he has an MSc in software development and a wider interest in the transformative effects of algorithmic technologies on the legal sector.

John Morison is a professor of jurisprudence in the School of Law, Queen's University Belfast, and a member of the Royal Irish Academy. He has published widely in constitutional law and theory and on the impact of new technology. Currently, he runs the Leverhulme Interdisciplinary Network on Algorithmic Systems (LINAS), which funds 30 PhD researchers in an interdisciplinary research programme.

Politics and Governance
2025 • Volume 13 • Article 10197
https://doi.org/10.17645/pag.10197

cogitatio

ARTICLE

Open Access Journal

# Destined for Balance? Centralized and Decentralized Approaches to AI Governance

Chenghao Sun and Xiyan Chen

School of Social Sciences, Tsinghua University, China

**Correspondence:** Chenghao Sun (sunchenghao@tsinghua.edu.cn)

**Submitted:** 23 February 2025 **Accepted:** 25 August 2025 **Published:** 8 October 2025

**Issue:** This article is part of the issue "Technology and Governance in the Age of Web 3.0" edited by Chang Zhang (Communication University of China), Zichen Hu (London School of Economics and Political Science), and Denis Galligan (University of Oxford), fully open access at https://doi.org/10.17645/pag.i443

## Abstract

The rapid development of AI and rising concerns over its ethical risks have driven states to adopt centralized or decentralized governance approaches. This article examines the factors influencing states' choices of governance approaches. We hypothesized that states' choices are influenced by three key variables: per capita gross national income, research and development (R&D) capacity, and the level of ethical risks. The fuzzy-set qualitative comparative analysis (fsQCA) method is adopted to analyze how these independent variables impact states' governance choices. Our findings suggest that states that have higher income and stronger R&D capacity tend to adopt a more decentralized governance approach. On the contrary, if a state's income level is high while its R&D capacity is weak, it is likely to take a more centralized approach. Also, there are situations in which states' R&D capacity is relatively weak but their ethical risk level is comparatively high. These states usually employ a relatively centralized approach to ensure technological innovation and risk control. Generally, the influences of a state's income level and R&D capacity outweigh the influence of its ethical risk level. Our framework is tested through case studies of the US, China, Germany, France, Singapore, India, Brazil, and Russia. Inspired by the governance choices of the deviant cases, we also found that a balanced governance approach can facilitate AI innovation while safeguarding human rights and freedom. This requires states to reallocate their governance power and achieve a balance between central and local governments, as well as public and private sectors.

## Keywords

artificial intelligence; centralization; ethics; governance; research and development

## 1. Introduction

With the rapid development and growing adoption of artificial intelligence (AI), its ethical risks have been receiving increasing attention. There arises a question for states about how to govern the emerging technology domestically. Scholars initiated debates over centralized and decentralized governance approaches. Some scholars believe states prefer a centralized approach, which is beneficial to improving resource extraction and integration ability, ensuring consistency in standards, and preventing ethical risks (Cihon et al., 2020; Dafoe, 2018; Hutchcroft, 2001; Radu, 2021). They think a decentralized approach increases the probability of leaking sensitive information and causes alignment problems. It does not necessarily guarantee diversity of data sources and the non-discrimination principle in the AI system (Clifton et al., 2022).

Other scholars regard the decentralized approach as more democratic than the centralized one (Montes & Goertzel, 2019). As Brynjolfsson and Ng (2023) noted, although centralized decision-making can be more efficient, it also leads to concentration of power and resources, which proves to be harmful to democracy. They also highlighted that a centralized approach may hinder innovation in the emerging technology industry, while a decentralized one will not only promote technology research and development (R&D) but will also ensure lower ethical risks (L. Cao, 2022; Chen et al., 2021; Wright, 2023).

Based on the normative analysis of strengths and weaknesses of centralized and decentralized approaches, some scholars seek to examine the types of approaches states have employed by exploring national strategies, regulations, laws, and codes of conduct (Daly et al., 2019; Dixon, 2023; Djeffal et al., 2022; Papyshev & Yarime, 2023; Radu, 2021). But they scarcely explain why states choose a centralized or a decentralized AI governance approach. Therefore, our study follows in the footsteps of previous studies and applies the fuzzy-set qualitative comparative analysis (fsQCA) method to answer the remaining question. We found that there are three factors influencing states' AI governance approaches. The first is the level of per capita gross national income (GNI). Second, from the perspective of technological innovation, states' R&D capacity impacts their choice of governance approach. Third, in terms of safety and security, states' governance approaches can be influenced by the ethical risk levels of data and algorithms.

The article is structured as follows. In the second section, we elaborated on the definitions, characteristics, and evaluative metrics of the dependent variable, i.e., the centralized or decentralized governance approach. We also proposed hypotheses in this section. In the third section, we introduced the reasons behind our choice of the cases and how to operationalize the dependent and independent variables. In addition, the results of the analysis of the necessary and sufficient conditions are reported. In the fourth section, we tested the hypotheses by comparing the cases. In the fifth section, we discussed the fact that the deviant cases indicate a balanced approach to facilitate AI development and reduce ethical risks. This finding has significant implications for global AI governance. Finally, we conclude by acknowledging the limitations of our study and elucidating the implications of the article.

## 2. Conceptual Framework and Hypotheses

Technology governance presupposes technological progress—without advances or real-world applications, governance is moot. However, regulation has always struggled to keep up with the multiplying harms and

risks of AI due to its rapid development and deployment (Kaliisa et al., in press). To analyze how states choose AI governance approaches, we take the degree of centralization or decentralization of their governance approaches as a dependent variable. States' income level, R&D capacity, and ethical risk level are taken as independent variables.

### *2.1. States' AI Governance Approaches*

Before examining why states adopt certain AI governance approaches, it is necessary to define and characterize the prevailing governance configurations. Centralized governance is a top-down approach consisting of a hierarchical system in which the power to govern AI is concentrated in a few entities, such as central government agencies (McNealy, 2022). On the contrary, a decentralized approach is characterized by the absence of a central authority. Thus, governance power is distributed among multiple entities, including local governments, small and large corporations, and research institutions (Liu et al., 2024). However, in practice, the distinction between states' AI governance approaches is not a dichotomy (Pierre & Peters, 2005). Most states require both centralized and decentralized approaches to govern AI effectively, with the relative importance of each shaped by states' historical and institutional contexts.

Based on the aforementioned definitions and characteristics, we construct a multi-dimensional evaluative framework for assessing AI governance configurations. The first dimension is the role of central government, including how much AI governance power is concentrated in the central government or a central agency (Liu et al., 2024). When a central authority concentrates more governance resources and decision-making power, the states' AI governance approach leans toward a centralized configuration. If power is more evenly distributed, the configuration will be more decentralized.

The second dimension considers the engagement of local governments and non-state actors. States that adopt a more decentralized AI governance approach tend to promote multistakeholder collaboration in AI innovation, pursuing rapid technological iteration. In contrast, states that employ a more centralized approach place less emphasis on such collaborative innovation.

The third dimension is the transparency and auditability of AI systems, gauging how much system design and function, personal data use, and automation processes and levels involved in decision-making are disclosed to stakeholders (ISO, 2022, p. 30). A decentralized approach puts more emphasis on the openness of AI systems and on external accountability. On the contrary, a centralized approach is inclined to ensure the opacity of AI systems to maintain control of AI development and governance.

### *2.2. Hypotheses*

Zeng et al. (2024) introduced the AI Governance International Evaluation (AGILE) index to depict the global landscape of national AI governance. The findings revealed a positive correlation between the index and states' income situation. This suggests that development forms the foundation for effective governance. According to modernization theory, with the development of states' economy, social structures become complex, labor processes begin to require the active cooperation of employees, and new groups emerge and organize (Przeworski & Limongi, 1997). As a result, the governance system will become decentralized. On this basis, we propose the first hypothesis:

H1: The higher a state's income level, the greater its tendency to adopt a decentralized AI governance approach.

As Vijayakumar (2021) noted, technological progress serves as a crucial mechanism for economic growth because it offers opportunities for enhancing productivity and creates new business models. But the situations in states with varying levels of R&D capacity can be very different. For advanced economies, AI will increase efficiency, total output, and per capita income by saving on labor (Boix, 2022). Furthermore, Vijayakumar (2021) suggested that AI advancements in one industry are often accompanied by similar progress in other domains. The economic advantages brought by advanced AI R&D capacity will benefit political, military, and social development, and international status. First, AI revolutionizes the process of data collection and analysis. For instance, politically, AI can empower political participation (Savaget et al., 2019). Socially, it allows more timely and accurate poverty identification and classification (Visvizi, 2022). In addition, AI can enhance automatic decision-making and task execution. For example, militarily, AI supports efficient and effective use of unmanned autonomous systems and can undertake dull, dangerous, and dirty tasks (Schraagen, 2023). More importantly, harnessing the aforementioned advantages, states will gain leadership and influence globally in both soft and hard power domains (Rebolledo, 2025).

Multiple actors have participated in the R&D process of AI technology, including government agencies, the private sector, academic institutes, and NGOs. Although the contributions of all parties should not be underestimated, there is no denying that the private enterprises are the main driving force behind AI R&D. For instance, Vijayakumar (2021) proved that annual private investment in AI is positively related to GDP growth in terms of both current and lagged effects. Moreover, local governments have a deeper understanding of the AI development situation in their own jurisdiction. Introducing regulation in a relatively small area can be beneficial to local autonomy and capacity building. Therefore, to fully tap into enterprises' potential for innovation, cut down coordination costs, and enhance national strength, some states with strong AI R&D capacity tend to take the decentralized approach. They distribute the governance power to businesses and local governments.

For middle- and low-income economies, AI R&D capacity is relatively weak. It's difficult for them to generate as much profit as the advanced economies do because the positive impact of automation will be mediated by the cost of moving up in the production ladder from low-value-added to high-value-added activities (Boix, 2022). What's more, due to the improvement of productivity by applying AI, advanced states will "re-shore" production domestically to minimize distribution and transportation costs. This may further lead to economic backsliding of middle- and low-income states. However, Vijayakumar (2021) proved that automation is costly in the short term but beneficial in the long term. Firms that initially invest in automation can gain a competitive advantage over firms that lag behind. Moreover, more R&D-intensive firms pay higher wages on average, with lower-skilled workers benefiting more from working in these firms than higher-skilled workers (Aghion et al., 2017). As a result, although states with low R&D capacity may not benefit from AI development in the short term, in reality, they still put emphasis on technological innovation and strive to catch up with advanced economies. For them, fragmented resources can reduce innovation efficiency, especially when the R&D capacity of companies and research institutes needs enhancement. Since government investment (X. Y. Cao et al., 2023) and cautious data integration and sharing (Omaar, 2024) help improve R&D efficiency, central governments of middle- and low-income economies may play a dominant role in AI development. In this sense, we formulate two hypotheses:

H2a: The stronger the AI R&D capacity of a state, the more it tends to adopt a decentralized AI governance approach.

H2b: The weaker the AI R&D capacity of a state, the more it tends to adopt a centralized AI governance approach.

The development and application of AI generate unexpected consequences and pose new forms of risk. Politically, AI can be used to produce fake news, which is much more persuasive than human-generated news (Kouroupis, 2023). Political communication is seriously damaged since it loses its natural, direct, and original dimensions (Kouroupis, 2023). Thus, the fairness of elections will be undermined, and democracy will also be tampered with through the deceiving of voters. Militarily, an AI model trained on biased historical data may not withstand contact with the realities of the world as it currently is (Schraagen, 2023). Besides, concerns exist that uncontrolled AI in autonomous weapons systems could result in catastrophic outcomes. Socially, AI trained by biased data may be harmful to job recruitment and criminal justice (Farina et al., 2022).

The risks need to be addressed by developing suitable means of governance (Taeihagh, 2021). The visibility, prioritization, and political framing of the risk level vary by governance system and media ecology. These constructions, rather than the "risk itself," influence states' governance orientation. In contexts where ethical risks are constructed as high, states tend to take a decentralized approach to manage risks case by case without hindering innovation. Conversely, when constructed risks are low, states aim to keep the risks at a low level and balance innovation with public interests, so they seek to adopt a more centralized governance approach to ensure that progress remains controlled and cautious (Rebolledo, 2025). Accordingly, we put forward two hypotheses:

H3a: The more publicly politicized and institutionally acknowledged ethical risks are within a state, the more likely the state is to adopt inclusive or balanced governance measures.

H3b: In states where ethical risks are suppressed or reframed as security threats, centralized governance is more likely.

## 3. Data and Method

The majority of research on AI governance takes the form of qualitative analysis (Birkstedt et al., 2023; Dafoe, 2018; Mäntymäki et al., 2022). We try to combine the case-oriented qualitative and variable-oriented quantitative methods to comprehensively analyze states' AI governance approaches.

### *3.1. Case Selection and Variable Measurement*

As for how to choose cases, Berg-Schlosser and De Meur (2009) argued that first, the cases must share enough background characteristics, which in turn can be considered as "constants" in the analysis. So it is indispensable to clearly delimit the outcome of cases before analysis. Second, a maximum of heterogeneity over a minimum number of cases should be achieved.

Based on the twofold guidance, we chose the AI governance cases of the US, China, Germany, France, Singapore, India, Brazil, and Russia. The reasons are that first, AI represents a nascent technological domain, thus not all states have started to govern it. The selected states are relatively advanced in terms of AI development and have embarked on establishing AI governance frameworks. Second, through systemic analysis, we found their AI governance approaches exhibit distinctive characteristics. On this basis, we systematically analyzed and explained why states adopt different governance approaches.

There are several indicators chosen to measure the dependent variable. Firstly, Radu (2021) argued that national documents form the basis for regulatory configurations. Therefore, we used the number of specialized AI governance national strategies and laws in force as of December 2024 as the indicator to measure the capacity of the eight states' central authority in AI governance. The source of the national-level documents is the OECD AI Policy Observatory. Secondly, we used the number of local AI policies and laws in force by December 2024 to measure the extent of local governments' participation in AI governance. The documents are from the official websites of the eight states' local governments. Thirdly, the Global Index on Responsible AI constitutes the largest global data collection on responsible AI. The scores of non-state actors show the performance of the private sector, academia, and civil society. We used the scores as an indicator to measure non-state actors' level of participation in AI governance. Fourthly, states that adopt a decentralized AI governance approach tend to release more open AI models and datasets, and have more active developer communities, while those who implement a centralized governance approach are less likely to keep their AI systems transparent and establish developer communities. Therefore, we used the number of open AI models and datasets, as well as the number of developer communities, to measure the degree of transparency and auditability of states' AI systems. The data are from the report of the AGILE index. Considering that there are multiple indicators used to measure the level of decentralization or centralization, we adopted the entropy weight method (Zhu et al., 2020) and linear weighted sum method (Stanimirovic et al., 2011) to preprocess the data and output the weighted combination of the values.

For independent variables, to begin with, we used per capita GNI to measure the income level of the eight states. According to the World Bank, per capita GNI reflects the average before-tax income of a state's citizens and the state's level of economic development. The per capita GNI of 2023 reported by the World Bank is employed in this study.

Bryan and Teodoridis (2024) asserted that the efficacy of AI governance depends on regulators' knowledge about the benefits of the technology. Furthermore, how much a state can benefit from AI development depends on its progress in AI, which is tied to both academic research and market applications. Therefore, the level of states' R&D capacity is measured by indicators including the number of published articles, granted patents, developed systems (Perrault & Clark, 2024), and supercomputers by 2024 (TOP500, 2024), and the average proportion of total AI private investment to GDP (current US dollars) from 2017 to 2023 (Zeng et al., 2024). Likewise, we adopted the entropy weight method and the linear weighted sum method to deal with the multiple indicators.

In addition to the aforementioned variables, ethics, the moral principles concerning right and wrong, are also important for AI governance. The ethical risks of AI arise from several dimensions, including privacy, fairness, and explainability (IBM AI Ethics Board, 2024; Perrault & Clark, 2024). Risks related to potential harms may affect organizations, consumers, or create broader detrimental effects on society.

There is admittedly a lack of consensus on robust and verifiable methods for measuring ethical risks across different AI use cases (National Institute of Standards and Technology, 2023). The reasons are that first, the speed and scale of the adoption of AI outpace the identification and response to the concerns raised (Taeihagh, 2021). Second, there can be a significant variation in how the components of ethical risks are interpreted (Roberts et al., 2023). For instance, Novelli et al. (2023) criticized the categorization of risks in the EU AI Act as coarse-grained, and proposed an assessment framework based on specific AI scenarios.

Measuring risk at earlier stages of the AI lifecycle can yield different results than at later stages. Moreover, risks presented when AI systems are tested in a virtual environment may differ from the risks posed when that same system is deployed in the real world. Scholars have indicated that risks can be evaluated by observing the existing models' behavior in practice and recorded incidents (Leipzig, 2023; Piorkowski et al., 2023). This kind of measurement in a real-world environment reflects the relatively authentic risk levels of AI models, especially given the black-box nature of AI. Therefore, we measured the ethical risks of AI by considering both subjective and objective dimensions. First, we use the number of AI ethical risk incidents reported by the eight states' governments between 2017 and 2023 to evaluate the risk levels of different states. Since the cases are self-reported by individual countries, this measurement dimension is relatively subjective.

Second, AI ethical risks can also be evaluated based on states' consensus regarding fundamental values, which is more objective. It is commonly recognized that the employment of AI poses the ethical risk of biases (Margetts, 2022; Milan & Beraldo, 2024; Roberts et al., 2023; Taeihagh, 2021). The nondiscrimination of AI is especially important because biased decision-making might worsen already-existing social inequality (Modi, 2023). Moreover, the implications of biased AI are widespread across various domains, including healthcare, employment, criminal justice, financial services, and education. The primary source of bias in AI is societal prejudices reflected in training data, which are amplified and perpetuated through algorithms (Shrishak, 2024). If someone has access to the internet, their data may be collected and used for AI training. Thus, we use the internet gender divide and the share of the underprivileged who use the internet to measure the risk of bias. The data are collected from the OECD's Going Digital Toolkit.

### *3.2. Analysis and Results*

Using the fsQCA method, we analyzed the eight states' approaches to AI governance. The reasons why we chose this method are that first, fuzzy sets are simultaneously qualitative and quantitative, for they incorporate both kinds of distinctions in the calibration of the degree of set membership. Second, the method is suitable for analyzing complex causality in small samples.

After obtaining the weighted values of the dependent variable using the entropy weight method and the linear weighted sum method, we adopted the three-value anchoring method to directly calibrate the data, converting them into fuzzy membership scores that range from 0 to 1 (Rihoux & Ragin, 2009). We took the three-value scheme using the scores 0.95, 0.50, and 0.05 (Ragin, 2008) to indicate the degree of membership in the set of the values of dependent variable. Accordingly, we set the breakpoints at 0.671, 0.137, and 0.067, which means that when the weighted values of the indicators are greater than or equal to 0.671, the states are considered as having full membership in the set of "decentralized AI governance approach." If the values are lower than 0.067, the states are regarded as having full nonmembership in the same set. The crossover point is 0.137, meaning that the states with this value are neither fully in nor fully out of the set. Using the

fsQCA software, we calibrated the values in Table 1. Values approaching 1 indicate stronger membership in the "decentralized AI governance approach" set.

The average, maximum, and minimum calibrated values of the dependent variable are 0.47, 0.97, and 0.02, respectively. And the standard deviation of the values is 0.328. So there are obvious differences in the AI governance approaches of the eight states. Among them, the AI governance approaches of the US and China are the most decentralized, while Russia adopts the most centralized governance approach.

**Table 1.** Measurement and calibration of states' AI governance approaches.

| State | Measured Value | Calibrated Value |
|---|---|---|
| US | 0.490432 | 0.88 |
| China | 0.768079 | 0.97 |
| Germany | 0.278046 | 0.69 |
| France | 0.154122 | 0.52 |
| Singapore | 0.101853 | 0.18 |
| India | 0.101859 | 0.18 |
| Brazil | 0.119386 | 0.32 |
| Russia | 0.048180 | 0.02 |

Next, we calibrated the independent variables. For per capita GNI, we employed the indirect method of calibration. In 2024, according to the World Bank, states with a per capita GNI lower than 1,145 US dollars are classified as low-income states. States with a per capita GNI ranging from 1,146 to 4,515 US dollars are lower-middle-income states. States with a per capita GNI from 4,516 to 14,005 US dollars are upper-middle-income states. High-income states are those whose per capita GNI is higher than 14,005 US dollars. According to the concept of infrastructural power—the capacity of the state to penetrate civil society and to implement political decisions logistically (Mann, 1984)—we interpreted income status as a proxy for infrastructural power to determine the governance landscape. On this basis, we adopted a four-value anchoring method, using the numerical values of 1, 0.67, 0.33, and 0 to indicate the degree of membership in the set of "high income states." These four values sequentially represent "fully in," "more in than out," "more out than in," and "fully out" (Rihoux & Ragin, 2009). States with a per capita GNI greater than 14,005 US dollars were coded as fully in the set of high-income states. States whose per capita GNI is greater than 4,515 US dollars were coded as more in than out. Those with a per capita GNI greater than 1,145 were coded as more out than in. And those with a per capita GNI of 1,145 or lower were coded as fully out. The next step is to estimate the indirectly calibrated values of per capita GNI of each case, using per capita GNI as the independent variable and the qualitative codings as the dependent variable. We used the Stata software to construct a fractional logit model using the fractional polynomial regression procedure (Ragin, 2008). The predicted values are reported in Table 2.

For R&D capacity, drawing on the theory of absorptive capacity, which argues that the ability to recognize the value of new, external information, assimilate it, and apply it is critical to innovative capabilities (Cohen & Levinthal, 1990), we adopted a three-value anchoring method. The value of 0.794 corresponded to the score 0.95, indicating that cases with values higher than 0.794 were considered fully in the set of "strong R&D capacity." Additionally, the value 0.017 was scored 0.05, meaning that cases with values lower than 0.017 are fully out of the set of "strong R&D capacity." The crossover point was 0.099, meaning that the cases with

this exact value were neither fully in nor fully out of the set. The measured and calibrated values are shown in Table 2. These thresholds ensured that calibration differentiated between global leaders, emerging players, and innovation laggards.

As for ethical risk, the levels of perceived risk influence how complex the governance webs are (Renn, 2008). We continue to use a three-value anchoring method to distinguish between low-exposure, emerging-risk, and high-exposure systems. The value of 0.564 was scored 0.95, indicating that cases with a value higher than 0.564 were fully in the set of "high ethical risk level." The value of 0.0297 corresponded to the score 0.05, meaning that cases with a value lower than 0.0297 were fully out of the set. The crossover point was 0.093, meaning that cases with this exact value were neither fully in nor fully out of the set. The measured and calibrated values are shown in Table 2.

**Table 2.** Measurement and calibration of states' per capita GNI, R&D capacity, and ethical risk level.

| State | Per Capita GNI | Calibrated Value | R&D | Calibrated Value | Ethical Risk | Calibrated Value |
|---|---|---|---|---|---|---|
| US | 80,450 | 1 | 0.993 | 0.98 | 0.582106 | 0.96 |
| China | 13,390 | 0.834275 | 0.425 | 0.80 | 0.112447 | 0.53 |
| Germany | 54,800 | 1 | 0.133 | 0.54 | 0.074146 | 0.29 |
| France | 45,180 | 1 | 0.078 | 0.32 | 0.039882 | 0.07 |
| Singapore | 70,590 | 1 | 0.120 | 0.52 | 0.024255 | 0.04 |
| India | 2,540 | 0.331074 | 0.046 | 0.12 | 0.531632 | 0.94 |
| Brazil | 9,280 | 0.629858 | 0.017 | 0.05 | 0.174996 | 0.63 |
| Russia | 14,250 | 0.874792 | 0.018 | 0.05 | 0.050464 | 0.12 |

After calibrating the dependent and independent vare we analyzed the necessary and sufficient conditions for a state's choice of AI governance approach. Necessary conditions are those that must be present for the outcome to occur, but their presence does not guarantee that occurrence. With fuzzy sets, a possible necessary condition is signaled when the instances of the outcome constitute a subset of instances of a condition (Rihoux & Ragin, 2009). The closer the consistency score is to 1, measuring the extent to which the outcome set is a subset of the condition set, the more likely the condition is necessary for the outcome. For condition (independent) variables that meet the consistency threshold, their coverage must be further examined. The coverage of a condition variable measures the extent to which it explains the outcome variable. We took 0.9 as the consistency threshold and 0.5 as the coverage threshold (Schneider & Wagemann, 2012). According to these standards, only per capita GNI is a necessary condition for a state's decentralized AI governance approach. The value of its coverage is 0.543. This result confirms H1, indicating that if the income level of a state is high, the state will be more likely to adopt a decentralized AI governance approach.

For sufficiency, if a condition (independent) variable or a configuration of condition variables is a sufficient condition for the outcome (dependent) variable, it means that all cases where the condition or the configuration of conditions is present must necessarily exhibit the outcome variable. However, cases showing the outcome do not necessarily exhibit the conditions (Ragin, 2000).

**Table 3.** Results of the necessary condition analysis.

| Outcome (Dependent) Variable | Condition (Independent) Variable | Consistency | Coverage |
|---|---|---|---|
| Degree of Decentralization (Y) | Per Capita GNI | 0.963903 | 0.543370 |
| | ~ Per Capita GNI | 0.182374 | 0.515582 |
| | R&D | 0.773936 | 0.860947 |
| | ~ R&D | 0.505319 | 0.411255 |
| | Ethical Risk | 0.619681 | 0.650838 |
| | ~ Ethical Risk | 0.611702 | 0.520362 |
| Degree of Centralization (~ Y) | Per Capita GNI | 0.848048 | 0.539089 |
| | ~ Per Capita GNI | 0.281669 | 0.897951 |
| | R&D | 0.358491 | 0.449704 |
| | ~ R&D | 0.889151 | 0.816017 |
| | Ethical Risk | 0.500000 | 0.592179 |
| | ~ Ethical Risk | 0.705189 | 0.676471 |

Notes: "~" represents negation; the membership of a case in the negation of fuzzy set A simply subtracts its membership in set A from 1.

We used the truth table of independent and dependent variables for sufficient condition analysis. Due to our small sample size, we set the frequency threshold as 1 (Rihoux & Ragin, 2009). Also, we set the threshold of raw consistency as 0.8 (Rihoux & Ragin, 2009) and the threshold of PRI consistency (Proportional Reduction in Inconsistency) as 0.65 (Greckhamer, 2016). Then, we used the fsQCA software to generate three solutions: the complex solution, the intermediate solution, and the parsimonious solution. Because of the limited diversity of our sample, there exist logical remainders. The complex solution excludes all counterfactuals in logical reminders, while the intermediate solution contains easy counterfactuals, and the parsimonious solution contains both easy and difficult counterfactuals. So the assessment of sufficiency of the conditions relies mainly on the intermediate solution, supplemented by the parsimonious solution. The results are reported in Tables 4 and 5.

**Table 4.** Sufficient conditions for a decentralized AI governance approach.

| Parsimonious Solution | | | | Intermediate Solution | | | |
|---|---|---|---|---|---|---|---|
| | Raw coverage | Unique coverage | Consistency | | Raw coverage | Unique coverage | Consistency |
| R&D | 0.773936 | 0.773936 | 0.860947 | Per capita GNI * R&D | 0.773936 | 0.773936 | 0.860947 |
| Solution coverage | 0.773936 | solution consistency | 0.860947 | Solution coverage | 0.773936 | solution consistency | 0.860947 |

Note: "*" represents the logical AND.

According to Table 4, we found that the configuration of high income and strong AI R&D capacity is a sufficient condition for a decentralized AI governance approach. Moreover, strong R&D capacity is the core condition. Solution coverage and consistency of the parsimonious and intermediate solutions are greater than 0.75, so the results demonstrate relatively strong explanatory strength (Schneider & Wagemann, 2012). The results confirm H2a—greater AI R&D capacity correlates with a higher likelihood of adopting

**Table 5.** Sufficient conditions for a centralized AI governance approach.

| Parsimonious Solution | | | | Intermediate Solution | | | |
|---|---|---|---|---|---|---|---|
| | Raw coverage | Unique coverage | Consistency | | Raw coverage | Unique coverage | Consistency |
| ~ R&D | 0.889151 | 0.889151 | 0.816017 | Per capita GNI * ~ R&D | 0.744275 | 0.383206 | 0.858531 |
| | | | | ~ R&D * ethical risks | 0.476415 | 0.115346 | 0.897778 |
| Solution coverage | 0.889151 | solution consistency | 0.816017 | Solution coverage | 0.859621 | solution consistency | 0.862715 |

Notes: "~" represents negation; "*" represents the logical AND.

decentralized AI governance. But H3a is not verified, suggesting that a high level of ethical risks has little impact on whether states choose a decentralized AI governance approach or not.

We also found, as Table 5 shows, that the configuration of high income and weak AI R&D capacity is a sufficient condition for a centralized AI governance approach. Aside from this, the configuration of weak AI R&D capacity and high ethical risk level is another sufficient condition for states to adopt a centralized AI governance approach. Furthermore, weak R&D capacity is the core condition of the two kinds of configurations. The results are reliable because solution coverage and consistency of the parsimonious and intermediate solutions are greater than 0.8. Thus, H2b is verified. It is noteworthy that a high level of ethical risk positively influences states' centralized AI governance approach, which is contrary to H3b.

To test the robustness of the three configurations, we reset the threshold of consistency to 0.85, with other thresholds held constant. The outcome of the necessary condition analysis remains the same. What's more, the configurations of high income and weak AI R&D capacity and weak AI R&D capacity and high ethical risks level are still sufficient conditions for more centralized governance approaches. The solution coverage is 0.859621, and the solution consistency is 0.862715. However, the configuration of high income, strong AI R&D capacity, and high ethical risks level, rather than the configuration of high income and strong AI R&D capacity, is a sufficient condition for a decentralized AI governance approach. The solution coverage is 0.531915, and consistency is 0.947867. Consequently, the configuration of high income and strong AI R&D capacity is not robust, but high income and strong AI R&D capacity are still important determinants.

## 4. Case Study

In this part, we triangulated fsQCA results with case studies by, first, mapping sufficient pathways shown by the fsQCA software to empirical evidence from policy documents, and second, contextualizing deviant results. The types of cases are shown in Table 6.

The comprehensive analysis of necessary and sufficient conditions suggests that governance configurations are shaped not only by functional considerations but also by historical and institutional legacies of industrial, digital, and political reforms (Pierson, 2000). First, if the income level of a state is relatively high and it has

**Table 6.** Typology matrix of AI governance configurations by institutional control and innovation coordination.

| | High Innovation Coordination | Low Innovation Coordination |
|---|---|---|
| High Institutional Control | Singapore | Russia, Brazil, India |
| Low Institutional Control | US, China, Germany | France |

strong AI R&D capacity, the state will adopt a more decentralized approach to governing AI technology, reflecting both its contemporary capacities and the evolution of multistakeholder governance norms. Cases exhibiting membership scores greater than 0.5 in both the condition and the outcome sets are the US (0.98, 0.88), China (0.80, 0.97), and Germany (0.54, 0.69).

The reasons why these states adopt a decentralized governance approach are as follows. First of all, preceding decentralized governance steps induce further movement in the same direction. Also, due to their relatively high income level, the division of labor has become more specialized, and social structures have become complex. In the US, the tradition of dispersed authority—rooted in its federal system and reinforced by past digital governance policies—facilitates a decentralized approach. Multiple stakeholders have participated in AI governance, consistent with the US National Artificial Intelligence Research and Development Strategic Plan (National Science and Technology Council, 2023). There is no federal law or executive order to govern AI. However, states in the US have already enacted laws. Besides this, many US technology corporations have issued ethics statements on their AI activities, like Microsoft's AI Principles. Also, US not-for-profit organizations and foundations have actively supervised the AI governance process (Daly et al., 2019). In August 2023, Accountable Tech, the AI Now Institute, and Electronic Privacy Information Center (EPIC) jointly released the "Zero Trust AI Governance" framework.

In China, experimental localism, long used in economic policy pilots, underpins the encouragement of provincial-level AI strategies. For instance, Beijing launched its AI Plus action plan in 2024. Additionally, Shanghai enacted the first provincial-level AI regulation in 2022. Shenzhen also introduced measures to build itself into an AI-pioneer city in 2023. Moreover, China upholds the principle that the market should play a dominant role in determining AI development roadmaps and establishing industrial standards (State Council of the People's Republic of China, 2017).

Germany also puts emphasis on multistakeholder governance: 13 out of 16 German states have developed their own AI strategy or agenda as of 2025. Discussion groups and cooperation platforms have been built, representing multiple actors involved in AI governance. For example, Platform Industry 4.0 (2015), Learning Systems (2017), Digital Hub Initiative (2017), and Regulatory Sandboxes (2018) all help establish distributed nodes to promote interinstitutional communication and cooperation among the private sector, academia, and civil society.

The second reason is that the states with advanced AI R&D capacity seek to sustain their "first mover" advantages in AI and enhance competitiveness. The US benefits from its unparalleled AI R&D capacity and tends to augment its strength to compete with China. Economically, AI innovation in life sciences, personal devices and computing, banking and finance, and energy management is strongly correlated with GDP growth at present and in the future (Vijayakumar, 2021). Militarily, as then US Secretary of Defence Mark Esper said, "Whichever nation harnesses AI first will have a decisive advantage on the battlefield for many,

many years" (Konaev et al., 2020). The US Department of Defence's Data, Analytics, and Artificial Intelligence Adoption Strategy (2023) noted that AI can bring military advantages like enabling efficient and precise strategic decisions, and deploying continuous advancements in technological capabilities to creatively address complex national security challenges. These contribute to deterring potential aggressors and winning great-power competitions with US strategic competitors, especially China. Socially, the US Department of State clarified that AI advances are providing great benefits to social well-being in areas including precision medicine, environmental sustainability, education, and public welfare. Geopolitically, based on the aforementioned benefits, AI can help comprehensively increase national strength and empower the US to consolidate its global leadership.

As the second most advanced state in AI R&D, China has led the development of large language models, which are now widely used in areas such as transportation, e-commerce, education, and office productivity, promoting intelligent upgrading and the digital transformation of traditional industries. Further to this, as a key enabler of new quality productive forces (新质生产力), AI enhances the inclusiveness of China's development by improving resource allocation and service efficiency ("'Rengongzhineng+' funeng xinzhi shengchanli fazhan," 2025). To continue facilitating economic development, enhancing governance capacity to safeguard social stability, and improving global competitiveness, China plans that by 2030, its AI theories, technologies, and applications should achieve globally pioneering levels. This will make China the world's primary AI innovation center. Also, China can achieve visible results with intelligent economy and society applications. Further, these lay an important foundation for China to become a leading innovation-style nation and an economic power (State Council of the People's Republic of China, 2017).

Germany aims to ensure that innovation will not be hindered. In addition to this, it seeks to establish "AI Made in Germany" as an international trademark for modern, secure, and public-interest-oriented AI applications based on the European canon of values (The German Federal Government, 2020).

Singapore is a deviant case. Schneider and Wagemann (2012) stated that cases with membership in condition set $> 0.5$ and membership in outcome set $< 0.5$ are deviant cases for consistency. According to the fsQCA software, Singapore's membership in the set of "per capita GNI * R&D capacity" is 0.52, while its membership in the set of decentralized AI governance approach is 0.18. The reason for Singapore to adopt a less decentralized approach is that it tends to strike a balance between AI innovation and public interests. Its path reflects a tradition of centralized developmental planning, as in the Smart Nation initiative. Although there are no specific laws in Singapore that directly regulate AI, the Singapore government has developed frameworks and tools to guide AI deployment and promote the responsible use of AI. For example, the Model AI Governance Framework (Personal Data Protection Commission of Singapore, 2020) was formulated to guide the private sector in addressing ethical and governance issues; AI Verify (The Info-communications Media Development Authority and Personal Data Protection Commission, 2022) aims to help organizations validate the performance of their AI systems against AI ethics principles through standardized tests; and the National Artificial Intelligence Strategy 2.0 was updated in 2023, outlining Singapore's commitment to building a trusted and responsible AI ecosystem.

Second, relatively high-income but lower R&D capacity states tend to adopt more centralized governance approaches to fully tap into their economic potential and accelerate innovation. Typical cases reported by fsQCA are Russia (0.875, 0.980) and Brazil (0.630, 0.680).

The President of the Russian Federation Vladimir Putin declared in 2017, "Whichever country becomes the leader in artificial intelligence will become the ruler of the world" ("Who Vladimir Putin", 2017). Russia has a statist tradition of technological development and an ambition to enhance its national power and global status by improving its capacity for AI innovation. Thus, a centralized AI governance approach is employed to achieve its geopolitical goal. State-owned Russian companies that are delegated and supervised by the central government play a dominant role in AI governance. The Russian government believes that, unlike private companies, state-owned enterprises will not exert a destabilizing influence on its political system. For instance, despite Yandex's status as Russia's leading tech firm, its uneasy relationship with the Kremlin may limit its interaction with the Russian government and other state-owned firms (Petrella et al., 2021). Depending on the government's level of trust, state-owned companies can gain policy support from the government, which will be beneficial not only for achieving Russia's strategic goals, but also for the companies' interests. Russian state-owned bank Sberbank has been the main driving force of the National Strategy for the Development of Artificial Intelligence. The strategy facilitates research on algorithms and mathematical methods, as well as the improvement of both the quality and scale of AI-related talent development (Prezident Rossiyskoy Federatsii, 2019). The company has also played a leading role in drafting and advancing the AI Roadmap in Russia. More than 20% of the investment budget allocated by the Roadmap will be spent on Sberbank's internal operational processes, while other spending will boost the ecosystem that Sberbank can benefit from (Petrella et al., 2021).

Although the Russian government has realized the importance of the private sector in technological innovation, the function of private companies is limited. Also, cooperation between state-owned and private companies is ineffective. For example, while the AI Alliance Russia, supervised by the Ministry of Economic Development, said that it will foster collaboration on AI between the public and private sectors, little visible cooperation has occurred (Petrella et al., 2021).

Similar to Russia, the Brazilian central government takes the lead in AI governance to accelerate its AI development. Advances in AI are expected to benefit Brazil across the social, economic, and diplomatic sectors. However, Brazil faces significant challenges that impede its AI innovation, including a lack of AI talent and the inability to install high-performance supercomputers dedicated to AI and to expand data centers. To optimize resource management and overcome these challenges, Brazil adopts a relatively centralized AI governance approach. It has developed the Brazilian AI Plan under the guidance of the National Council for Science and Technology. The Plan emphasizes leadership of the Brazilian government in promoting partnerships between different actors in the AI innovation and regulation ecosystem (Conselho Nacional de Ciência e Tecnologia, 2025).

A deviant case is France, whose membership in the condition set is 0.68 while its membership in the outcome set is 0.48. France seeks to equip itself with a competitive AI research capacity and to disseminate AI within the economy. It also facilitates the responsible development of AI by ensuring multistakeholder participation. As a result, although France's income is relatively high and its R&D capacity is relatively weak, its AI governance approach is less centralized. In 2017, the French government launched the National AI Strategy as part of "France 2030," which calls for the initiation of AI projects. For instance, the IA Booster France 2030 program is aimed at stimulating the innovation and effective governance of French small and medium-sized enterprises. Moreover, in July 2023, the French Data Protection Authority (CNIL) opened a public consultation on its AI action plan to ensure the rights of end-users. It sought the opinions of all concerned public and private actors.

Third, states with weak AI R&D capacity and high ethical risk adopt a more centralized AI governance approach to incentivize technological innovation and control risks. India (0.88, 0.82) is a typical case. Half the Indian population lacks access to the internet—the excluded half is primarily women, rural communities, and Adivasis (Sambasivan et al., 2021). As reported by the OECD, the difference between the share of men who are internet users and the share of women is 10.1 percentage points as of 2024, substantially higher than OECD members' average of 2.9 percentage points. Additionally, data from Statista shows that in 2023, 51% of people in India perceived that AI would replace their current job, compared to 36% globally. Considering that a company's self-management rules are ineffective in curtailing AI ethical risks (Joshi, 2024), the Indian government tends to control the risks through a centralized approach. For example, in 2023, a revised Digital Personal Data Protection Act was passed to safeguard personal data used in AI R&D.

Although India recognizes that the ethical risks of the emerging technology may cause harm, it gives more priority to facilitating technological advancement through centralized governance. Following the traditional tenets of liberal economy, Indian policy discourse is predominantly economically focused, considering the economic gains that AI offers to India, such as increased productivity, new revenue streams, and cost savings in public services (Bhalla et al., 2024). For instance, the National Strategy for AI (NITI Aayog, 2020) stated that the role of the state should be conceived as a "facilitator" or "enabler" for private enterprises to propel innovation and economic growth. Furthermore, the Indian government intends to open up "non-personal" and anonymized datasets from the vast files of information collected by public agencies for data mining and analysis (Ministry of Electronics and Information Technology, 2022).

## 5. Discussion

### *5.1. The Future of AI Governance*

According to the results reported by the fsQCA software, states' income level and AI R&D capacity play important roles in impacting states' AI governance choices. In contrast, the influence of the ethical risk level is marginal. This shows that states put more emphasis on AI development than on risk management. Due to the black box nature of AI technology, it is hard to fully understand how AI operates. Besides this, AI has grown rapidly in recent years, so AI governance struggles to keep pace with its development (Meek et al., 2016). According to the "Collingridge dilemma" (Genus & Stirling, 2018), intervening in AI development with risk control measures either too early or too late will be detrimental to society. Therefore, it is understandable why states are cautious in risk control when AI is only partially understood. Additionally, since AI has not demonstrated substantial risks or disastrous consequences, policymakers, the private sector, and the public do not take the issue seriously enough.

However, a common characteristic shown in the deviant cases is that their ethical risk consideration is beyond that of the typical cases. As a result, their AI governance approaches are either less decentralized or less centralized than the typical cases. This indicates that in the future, if ethical risks become more evident and states have to put more emphasis on risk management, they may adopt a balanced governance approach. For instance, during the Covid-19 pandemic, Chinese central and local governments, as well as civil society, jointly employed an Integrative Coordination Governance approach (Dang et al., 2021). Through this approach, the governments were in charge of discovering social problems in real time and proposing solutions accordingly, while technology companies and NGOs were responsible for optimizing algorithms to

adapt to the demand for governance. Meanwhile, under the supervision of the governments, companies reduced the ethical risks caused by AI as far as possible, which is beneficial to long-term development.

### *5.2. Towards a Theory of Balanced AI Governance*

Based on the above empirical analysis, the balanced approach is conceived not as a static midpoint, but as dynamic coordination between state and non-state actors, iterative policy feedback loops, and adaptive mechanisms such as regulatory sandboxes or mission-oriented experimentation (Mazzucato, 2016). Such a balance features vertical central–local government coordination to align strategic objectives, horizontal public–private partnerships to leverage expertise and resources, and temporal management of the trade-off between short-term innovation gains and long-term risk mitigation.

A balanced approach proves to be beneficial to the improvement of R&D capacity and ethical risk control. For example, in March 2018, the Russian Ministry of Defense issued a statement ignoring the potential of private companies for AI innovation and self-regulation, while proposing the leadership of the Russian government and state-owned enterprises in AI governance. One year later, the Russian government introduced three AI-specific policy documents that leaned heavily on the private sector, emphasizing the increased decentralization of the Russian AI governance approach. This change acted as one of the causes of the improvement of Russia's R&D capacity from 2018 to 2019. The Stanford AI Vibrancy tool shows that the increase in the number of AI journal publications and patent grants from 2018 to 2019 is greater than the increases both from 2017 to 2018 and from 2019 to 2020. In Singapore, the Monetary Authority of Singapore provides supervisory guidance to all financial institutions. It also works with industry, sharing best practices for risk management efforts and facilitating industry collaboration through programs such as Project MindForge (Monetary Authority of Singapore, 2024). Therefore, the level of AI ethical risk emanating from Singapore's financial sector is relatively low.

The balanced approach reciprocally influences the independent variables, helping address prominent issues quickly and enhancing the effectiveness of regulations. Thus, a balanced approach may not only become a widely accepted domestic AI governance approach, but could also profoundly impact the current global AI governance landscape.

Local, regional, national, international, and non-governmental actors are comprised in the global AI governance ecosystem, which leads to the fragmentation of the system (OECD, 2024). Geopolitical competition further hampers international interoperability, exacerbates ethical risks, and poses barriers to trade and investment. Simply resorting to techno-authoritarianism or unregulated marketism will be ineffective in aiding the emergence of a synergistic, anticipatory, and multistakeholder global AI governance system. Only the balanced approach offers a promising pathway for global AI governance. Its principles align with ongoing initiatives such as UNESCO's Recommendation on the Ethics of AI, emphasizing inclusiveness, accountability, and adaptability. To ensure these principles translate into practice, advanced and developing economies, technology giants, and small and medium-sized businesses should coordinate their interests through global platforms, fostering a governance order that is equitable and resilient.

## 6. Conclusion

The world is undergoing a fundamental technological shift in the age of AI. Although AI can be harnessed to benefit industries and society, ethical risks including bias, privacy leakage, and job displacement may be harmful to human rights (United Nations System Chief Executives Board for Coordination, 2024). Therefore, proper governance is needed to make the most of the opportunities brought by AI and to mitigate its ethical risks. There are debates about how to govern AI and maximize its advantages (Brynjolfsson & Ng, 2023; Cihon et al., 2020; Dafoe, 2018). Our study aims to contribute to the debates by determining the variables that influence states' AI governance approaches.

Our work combined qualitative with quantitative analysis by adopting the fsQCA method. We chose the US, China, Germany, France, Singapore, India, Russia, and Brazil as the cases about which data were collected, analyzed, and used to test our hypotheses. With the aim of analyzing the underlying factors influencing states' choices of AI governance approaches, we established a framework in which states' income level, R&D capacity, and ethical risk level are taken as independent variables and states' AI governance approach is the dependent variable. We found that states that have higher income and stronger R&D capacity tend to adopt a decentralized governance approach. On the contrary, if a state's income level is high while its R&D capacity is weak, it is likely to take the centralized approach. Also, there are situations in which states' R&D capacity is relatively weak but their ethical risk level is comparatively high. These states usually employ a centralized approach to ensure technological innovation and control risks. Generally, the influence of states' income level and R&D capacity outweighs the influence of their ethical risk level.

Furthermore, we found that there are deviant cases in which states intend to adopt a less decentralized or less centralized approach to balance AI development and risk management. Consequently, we infer that neither a highly decentralized nor a highly centralized approach can effectively reconcile the tension between R&D capacity and ethical risks. Only a balanced approach offers the potential for simultaneously fostering technological advancement and mitigating ethical concerns.

There are limitations in our study. First, although we measured the ethical risks from multiple dimensions, due to data limitations, a more accurate evaluation of a state's risk levels could not be achieved. Second, the research method is also limited. While fsQCA provides systematic pattern recognition, the sample size is small, so diversity of results is not guaranteed. Moreover, we selected typical and deviant cases and potentially overlooked the edge-case insights.

Nevertheless, our results have important implications. The integrated use of fsQCA and case studies enables a comprehensive explanation of states' AI governance choices. In addition, we proved that the combination of per capita GNI and R&D capacity, as well as the combination of R&D capacity and ethical risk level, can impact states' choice of AI governance approach. More importantly, through the analysis of the deviant cases, we found that a balanced governance approach is ideal for promoting innovation and managing risks.

Our framework provides insights for Web 3.0 governance. Governance of decentralized technologies such as blockchain protocols and DAOs (decentralized autonomous organizations) also faces the problem of how to balance development and security. Our findings imply that emphasizing government regulation and multistakeholder participation simultaneously can help mitigate the dilemma and inform the design of more resilient blockchain and DAO governance structures.

## Acknowledgments

The authors would like to thank the reviewers and editors for their very useful comments and feedback.

## Funding

This study has received financial support from Tsinghua University Initiative Scientific Research Program (no. 2023THZWJC16).

## Conflict of Interests

The authors declare no conflict of interests.

## References

Aghion, P., Jones, B. F., & Jones, C. I. (2017). *Artificial intelligence and economic growth* (NBER Working Paper No. 23928). National Bureau of Economic Research.

Berg-Schlosser, D., & De Meur, G. (2009). Comparative research design: Case and variable selection. In B. Rihoux & C. C. Ragin (Eds.), *Configurational comparative methods: Qualitative comparative analysis (QCA) and related techniques* (pp. 19–32). Sage.

Bhalla, N., Brooks, L., & Leach, T. (2024). Ensuring a "responsible" AI future in India: RRI as an approach for identifying the ethical challenges from an Indian perspective. *AI and Ethics*, *4*, 1409–1422.

Birkstedt, T., Minkkinen, M., Tandon, A., & Mäntymäki, M. (2023). AI governance: Themes, knowledge gaps and future agendas. *Internet Research*, *33*(7), 133–167.

Boix, C. (2022). AI and the economic and informational foundations of democracy. In J. B. Bullock, Y. C. Chen, J. Himmelreich, V. M. Hudson, A. Korinek, M. M. Young, & B. Zhang (Eds.), *The Oxford handbook of AI governance* (pp. 707–725). Oxford University Press.

Bryan, K. A., & Teodoridis, F. (2024, September 24). Balancing market innovation incentives and regulation in AI: Challenges and opportunities. *Brookings Institution*. https://www.brookings.edu/articles/balancing-market-innovation-incentives-and-regulation-in-ai-challenges-and-opportunities

Brynjolfsson, E., & Ng, A. (2023). Big AI can centralize decision-making and power, and that's a problem. In B. Prud'homme, C. Régis, G. Farnadi, V. Dreier, S. Rubel, & C. d'Oultremont (Eds.), *Missing links in AI governance* (pp. 65–87). UNESCO; Mila.

Cao, L. (2022). Decentralized AI: Edge intelligence and smart blockchain, metaverse, web3, and desci. *IEEE Intelligent Systems*, *37*(3), 6–19.

Cao, X. Y., Wu, X. L., & Wang, L. M. (2023). Innovation network structure, government R&D investment and regional innovation efficiency: Evidence from China. *PLoS ONE*, *18*(5), Article e0286096.

Chen, Y., Richter, J. I., & Patel, P. C. (2021). Decentralized governance of digital platforms. *Journal of Management*, *47*(5), 1305–1337.

Cihon, P., Maas, M. M., & Kemp, L. (2020). Should artificial intelligence governance be centralised? Design lessons from history. In S. Das, B. P. Green, K. Varshney, M. Ganapini, & A. Renda (Eds.), *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society* (pp. 228–234). The AAAI Press.

Clifton, C., Blythman, R., & Tulusan, K. (2022). *Is decentralized AI safer?* arXiv. https://doi.org/10.48550/arXiv.2211.05828

Cohen, W. M., & Levinthal, D. A. (1990). Absorptive capacity: A new perspective on learning and innovation. *Administrative Science Quarterly*, *35*(1), 128–152.

Conselho Nacional de Ciência e Tecnologia. (2025). *IA para o bem de todos: Plano brasileiro de inteligência artificial*.

Dafoe, A. (2018). *AI governance: A research agenda*. Governance of AI Program, Future of Humanity Institute, University of Oxford.

Daly, A., Hagendorff, T., Hui, L., Mann, M., Marda, V., Wagner, B., Wang, W., & Witteborn, S. (2019). *Artificial intelligence governance and ethics: Global perspectives*. SSRN. https://doi.org/10.2139/ssrn.3414805

Dang, S., Ying, Y., & Yu, Y. (2021). *AI canyu zhongguo yiqing zhili de shijian: Zhengfu he shehui de yitihua hezuo zhili*. Institute for AI International Governance at Tsinghua University. http://aiig.tsinghua.edu.cn/info/1025/1184.htm

Dixon, R. B. L. (2023). A principled governance for emerging AI regimes: Lessons from China, the European Union, and the United States. *AI and Ethics*, *3*(3), 793–810.

Djeffal, C., Siewert, M. B., & Wurster, S. (2022). Role of the state and responsibility in governing artificial intelligence: A comparative analysis of AI strategies. *Journal of European Public Policy*, *29*(11), 1799–1821.

Farina, M., Zhdanov, P., Karimov, A., & Lavazza, A. (2022). AI and society: A virtue ethics approach. *AI & Society*, *39*(3), 1127–1140.

Genus, A., & Stirling, A. (2018). Collingridge and the dilemma of control: Towards responsible and accountable innovation. *Research Policy*, *47*(1), 61–69.

Greckhamer, T. (2016). CEO compensation in relation to worker compensation across countries: The configurational impact of country-level institutions. *Strategic Management Journal*, *37*(4), 793–815.

Hutchcroft, P. D. (2001). Centralization and decentralization in administration and politics: Assessing territorial dimensions of authority and power. *Governance*, *14*(1), 23–53.

IBM AI Ethics Board. (2024). *Foundation models: Opportunities, risks and mitigations*. IBM. https://www.ibm.com/downloads/documents/us-en/10a99803d8afd656

ISO. (2022). *Information technology—Artificial intelligence—Artificial intelligence concepts and terminology* (ISO/IEC 22989:2022). https://www.iso.org/standard/74296.html

Joshi, D. (2024). AI governance in India—Law, policy and political economy. *Communication Research and Practice*, *10*(3), 328–339.

Kaliisa, R., Baker, R. S., Wasson, B., & Prinsloo, P. (in press). The coming but uneven storm: How AI regulation will impact AI & learning analytics research in different countries. *Journal of Learning Analytics*.

Konaev, M., Chahal, H., Fedasiuk, R., Huang, T., & Rahkovsky, I. (2020). *U.S. military investments in autonomy and AI: A strategic assessment*. Center for Security and Emerging Technology. https://cset.georgetown.edu/publication/u-s-military-investments-in-autonomy-and-ai-a-strategic-assessment

Kouroupis, K. (2023). AI and politics: Ensuring or threatening democracy? *Tribuna Juridică*, *13*(4), 575–587.

Leipzig, S. D. (2023). *Trust: Responsible AI, innovation, privacy and data leadership*. Forbes Books.

Liu, Y., Lu, Q., Zhu, L., & Paik, H. Y. (2024). Decentralised governance for foundation model based AI systems: Exploring the role of blockchain in responsible AI. *IEEE Software*, *41*(5), 34–42.

Mann, M. (1984). The autonomous power of the state: Its origins, mechanisms and results. *European Journal of Sociology*, *25*(2), 185–213.

Mäntymäki, M., Minkkinen, M., Birkstedt, T., & Viljanen, M. (2022). Defining organizational AI governance. *AI and Ethics*, *2*(4), 603–609.

Margetts, H. (2022). Rethinking AI for good governance. *Daedalus*, *151*(2), 360–371.

Mazzucato, M. (2016). From market fixing to market-creating: A new framework for innovation policy. *Industry and Innovation*, *23*(2), 140–156.

McNealy, J. (2022). Adding complexity to advance AI organizational governance models. In J. B. Bullock, Y. C. Chen, J. Himmelreich, V. M. Hudson, A. Korinek, M. M. Young, & B. Zhang (Eds.), *The Oxford handbook of AI governance* (pp. 572–583). Oxford University Press.

Meek, T., Barham, H., Beltaif, N., Kaadoor, A., & Akhter, T. (2016). Managing the ethical and risk implications of rapid advances in artificial intelligence: A literature review. In D. F. Kocaogulu, T. R. Anderson, T. U. Daim, D. C. Kozanoglu, K. Niwa, & G. Perman (Eds.), *2016 Portland International Conference on Management of Engineering and Technology (PICMET)* (pp. 682–693). IEEE.

Milan, S., & Beraldo, D. (2024). Data in movement: The social movement society in the age of datafication. *Social Movement Studies*, *23*(3), 265–284.

Ministry of Electronics and Information Technology. (2022). *National Data Governance Framework Policy (draft)*. https://www.thehinducentre.com/resources/67557000-National-Data-Governance-Framework-Policy_compressed.pdf

Modi, T. B. (2023). Artificial intelligence ethics and fairness: A study to address bias and fairness issues in AI systems, and the ethical implications of AI applications. *Revista Review Index Journal of Multidisciplinary*, *3*(2), 24–35.

Monetary Authority of Singapore. (2024). *Artificial intelligence model risk management: Observations from a thematic review*. https://www.mas.gov.sg/-/media/mas-media-library/publications/monographs-or-information paper/imd/2024/information-paper-on-ai-risk-management-final.pdf

Montes, G. A., & Goertzel, B. (2019). Distributed, decentralized, and democratized artificial intelligence. *Technological Forecasting and Social Change*, *141*, 354–358.

National Institute of Standards and Technology. (2023). *Artificial Intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf

National Science and Technology Council. (2023). *The National Artificial Intelligence Research and Development Strategic Plan*. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/05/National-Artificial-Intelligence-Research-and-Development-Strategic-Plan-2023-Update.pdf

NITI Aayog. (2020). *National Strategy for Artificial Intelligence*. https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf

Novelli, C., Casolari, F., Rotolo, A., Taddeo, M., & Floridi, L. (2023). Taking AI risks seriously: A new assessment model for the AI Act. *AI & Society*, *39*(5), 2493–2497.

OECD. (2024). *Futures of global AI governance: Co-creating an approach for transforming economics and societies*. https://www.oecd.org/content/dam/oecd/en/about/programmes/strategic-foresight/GSG%20Background%20Note_GSG(2024)1en.pdf/_jcr_content/renditions/original./GSG%20Background%20Note_GSG(2024)1en.pdf

Omaar, H. (2024). *How innovative is China in AI?* Information Technology & Innovation Foundation. https://itif.org/publications/2024/08/26/how-innovative-is-china-in-ai

Papyshev, G., & Yarime, M. (2023). The state's role in governing artificial intelligence: Development, control, and promotion through national strategies. *Policy Design and Practice*, *6*(1), 79–102.

Perrault, R., & Clark, J. (2024). *Artificial Intelligence Index 2024*. Stanford University Human-Centered Artificial Intelligence.

Personal Data Protection Commission of Singapore. (2020). *Model Artificial Intelligence Governance Framework* (2nd ed.). https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf

Petrella, S., Miller, C., & Cooper, B. (2021). Russia's artificial intelligence strategy: The role of state-owned firms. *Orbis*, *65*(1), 75–100.

Pierre, J., & Peters, G. (2005). *Governing complex societies: Trajectories and scenarios*. Palgrave Macmillan.

Pierson, P. (2000). Increasing returns, path dependence, and the study of politics. *American Political Science Review*, *94*(2), 251–267.

Piorkowski, D., Vejsbjerg, I., Cornec, O., Daly, E. M., & Alkan, Ö. (2023). AIMEE: An exploratory study of how rules support AI developers to explain and edit models. *Proceedings of the ACM on Human-Computer Interaction*, *7*(CSCW2), Article 255.

Prezident Rossiyskoy Federatsii. (2019). *Ukaz Prezidenta Rossiyskoy Federatsii ot 10.10.2019 g. No. 490: O razvitii iskusstvennogo intellekta v Rossiyskoy Federatsii*. http://www.kremlin.ru/acts/bank/44731/page/1

Przeworski, A., & Limongi, F. (1997). Modernization: Theories and facts. *World Politics*, *49*(2), 155–183.

Radu, R. (2021). Steering the governance of artificial intelligence: National strategies in perspective. *Policy and Society*, *40*(2), 178–193.

Ragin, C. C. (2000). *Fuzzy-set social science*. University of Chicago Press.

Ragin, C. C. (2008). *Redesign social inquiry: Fuzzy sets and beyond*. University of Chicago Press.

Rebolledo, V. G. (2025). Impact of the artificial intelligence on international relations: Towards a global algorithms governance. *Revista UNISCI/UNISCI Journal*, *67*, 9–51.

"Rengongzhineng+" funeng xinzhi shengchanli fazhan. (2025, January 13). *Renminribao*. http://theory.people.com.cn/n1/2025/0113/c40531-40400643.html

Renn, O. (2008). *Risk governance: Coping with uncertainty in a complex world*. Earthscan.

Rihoux, B., & Ragin, C. C. (Eds.). (2009). *Configurational comparative methods: Qualitative comparative analysis and related techniques*. Sage.

Roberts, H., Cowls, J., Hine, E., Morley, J., Wang, V., Taddeo, M., & Floridi, L. (2023). Governing artificial intelligence in China and the European Union: Comparing aims and promoting ethical outcomes. *The Information Society*, *39*(2), 79–97.

Sambasivan, N., Arnesen, E., Hutchinson, B., Doshi, T., & Prabhakaran, V. (2021). Re-imagining algorithmic fairness in India and beyond. In A. Kasirzadeh & A. Smart (Eds.), *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (pp. 315–328). Association for Computing Machinery.

Savaget, P., Chiarini, T., & Evans, S. (2019). Empowering political participation through artificial intelligence. *Science and Public Policy*, *46*(3), 369–380.

Schneider, C. Q., & Wagemann, C. (2012). *Set-theoretic methods for the social sciences: A guide to qualitative comparative analysis*. Cambridge University Press.

Schraagen, J. M. (2023). Responsible use of AI in military systems: Prospects and challenges. *Ergonomics*, *66*(11), 1719–1729.

Shrishak, K. (2024). *AI-complex algorithms and effective data protection supervision: Bias evaluation*. European Data Protection Board. https://www.edpb.europa.eu/system/files/2025-01/d1-ai-bias-evaluation_en.pdf

Stanimirovic, I. P., Zlatanovic, M. L., & Petkovic, M. D. (2011). On the linear weighted sum method for multi-objective optimization. *Facta Universitatis, Series: Mathematics and Informatics*, *26*, 49–63.

State Council of the People's Republic of China. (2017). *Xinyidai rengongzhineng fazhan guihua*. https://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm

Taeihagh, A. (2021). Governance of artificial intelligence. *Policy and Society*, *40*(2), 137–157.

The German Federal Government. (2020). *Artificial intelligence strategy of the German Federal Government*.

The Info-communications Media Development Authority and Personal Data Protection Commission of Singapore. (2022). *Invitation to Pilot AI Verify: AI governance testing framework & toolkit*. https://file.go.gov.sg/aiverify.pdf

TOP500. (2024). *List statistics*. https://top500.org/statistics/list

United Nations System Chief Executives Board for Coordination. (2024). *United Nations system white paper on artificial intelligence governance: An analysis of current institutional models and related functions and existing*

*international normative frameworks within the United Nations system that are applicable to artificial intelligence governance*. https://unsceb.org/sites/default/files/2024-11/UNSystemWhitePaperAIGovernance.pdf

Vijayakumar, H. (2021). The impact of AI-innovations and private AI-investment on U.S. economic growth: An empirical analysis. *Reviews of Contemporary Business Analytics*, *4*(1), 14–32.

Visvizi, A. (2022). Artificial intelligence (AI) and sustainable development goals (SDGs): Exploring the impact of AI on politics and society. *Sustainability*, *14*(3), Article 1730.

Who Vladimir Putin thinks will rule the world. (2017). *CNN*. https://edition.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world

Wright, S. A. (2023). Why decentralize deep learning? In L. Martinez-Villaseñor & A. Barrera (Eds.), *2023 IEEE 15th International Symposium on Autonomous Decentralized System (ISADS)* (pp. 1–6). IEEE.

Zeng, Y., Lu, E., Guan, X., Huang, C., Ruan, Z., Younas, A., Sun, K., Tang, X., Wang, Y., Suo, H., Liang, D., Han, Z., Bao, A., Guo, X., Wang, J., Xie, J., & Liang, Y. (2024). *AI Governance International Evaluation Index*. Center for Long-term Artificial Intelligence; International Research Center for AI Ethics and Governance (CLAI); Institute of Automation, Chinese Academy of Sciences. https://agile-index.ai/AGILE-Index-Report-2024-EN.pdf

Zhu, Y., Tian, D., & Yan, F. (2020). Effectiveness of entropy weight method in decision-making. *Mathematical Problems in Engineering*, *2020*(1), Article 3564835.

## About the Authors

Chenghao Sun is an associate professor and a fellow at the School of Social Sciences, Tsinghua University. He is a council member of the Chinese Association of American Studies. His research interests include China–US relations, transatlantic relations, AI and global governance.

Xiyan Chen is a research assistant at the School of Social Sciences, Tsinghua University, and an analyst at ChinAffairs+. Her research interests include US domestic and foreign policies, AI governance.

**Politics and Governance**
2025 • Volume 13 • Article 10243
https://doi.org/10.17645/pag.10243

# Correction to "Reconceptualizing Technological Leadership: A Relational and Dynamic Framework"

Fang, Y., & Zhang, S. (2025). Reconceptualizing technological leadership: A relational and dynamic framework. *Politics and Governance*, *13*, Article 10243. https://doi.org/10.17645/pag.10243

On page 3, the in-text reference (Kranzberg, 1967) has been corrected as (Kranzberg & Pursell, 1967). The reference list has been updated accordingly:

Kranzberg, M., & Pursell, C. W. (1967). *Technology in Western civilization*. Oxford University Press.

On page 5, the in-text reference (Cusumano, 2020) has been updated as (Cusumano, 2004). The reference list has been updated accordingly:

Cusumano, M. A. (2004). *The business of software: What every manager, programmer, and entrepreneur must know o thrive and survive in good times and bad*. Free Press.

On page 8, two in-text references (Xie, 2020) and (Zhang & Wang, 2021) are corrected into (Mochinaga, 2021). The references have been removed from the reference list and replaced with the correct source:

Mochinaga, D. (2021, June 10). *The digital silk road and China's technology influence in Southeast Asia*. Council on Foreign Relations. https://www.cfr.org/sites/default/files/pdf/mochinaga_the-digital-silk-road-and-chinas-technology-influence-in-southeast-asia_june-2021.pdf

On page 9, two in-text references (Berg, 2020; Perry, 2019) are corrected into (Friis & Lysne, 2021; Zhang, 2024). The references have been removed from the reference list and replaced with the correct source:

Friis, K., & Lysne, O. (2021). Huawei, 5G and security: Technological limitations and political responses. *Development and Change*, *52*(5), 1174–1195. https://doi.org/10.1111/dech.12680

Zhang, Z. (2024). Technology and geopolitics: The social construction of Huawei's 5G controversy in Europe. *Global Media and Communication*, *20*(2), 217–235. https://doi.org/10.1177/17427665241251448

On page 15, in the reference list, the citation for Chan, A. (2021, July 12) included the incorrect date and has been updated as Chan, A. (2021, September 28).

Chan, A. (2021, September 28). *CFIUS, Team Telecom and China*. Lawfare. https://www.lawfaremedia.org/article/cfius-team-telecom-and-china

On page 16, in the reference list, the citation for He, Z. P., & Zhou, M. (2024) included incorrect page numbers as 110–123. The correct page numbers are 110–124,126. The issue number has also been added. The reference list has been updated accordingly:

He, Z. P., & Zhou, M. (2024). China's role, challenges, and responses in building the digital silk road. *Northeast Asia Forum*, *33*(6), 110–124,126. https://doi.org/10.13654/j.cnki.naf.2024.06.008

On page 17, in the reference list, the citation for Rosenberg, N. (1992). included incorrect page numbers as 187–208. The correct page numbers are 181–203. The reference list has been updated accordingly:

Rosenberg, N. (1992). Economic experiments. *Industrial and Corporate Change*, *1*(1), 181–203. https://doi.org/10.1093/icc/1.1.181

On page 17, in the reference list, the citation for The State Council of the People's Republic of China (2017) included an incomplete title. The correct title is *A next generation artificial intelligence development plan*. The reference list has been updated accordingly:

The State Council of the People's Republic of China. (2017). *A next generation artificial intelligence development plan*. https://d1y8sb8igg2f8e.cloudfront.net/documents/translation-fulltext-8.1.17.pdf

On page 17, in the reference list, the citation for US National Science and Technology Council (2016) included an incomplete title. The correct title is *The National artificial intelligence research and development strategic plan* and the reference has been updated with a direct link to the full document:

US National Science and Technology Council. (2016). *The national artificial intelligence research and development strategic plan*. https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/national_ai_rd_strategic_plan.pdf

We apologize for the above errors.

POLITICS AND GOVERNANCE
ISSN: 2183-2463

Politics and Governance is an international, peer-reviewed open access journal that publishes significant and cutting-edge research drawn from all areas of political science.

Its central aim is thereby to enhance the broad scholarly understanding of the range of contemporary political and governing processes, and impact upon of states, political entities, international organisations, communities, societies and individuals, at international, regional, national and local levels.

cogitatio

www.cogitatiopress.com/politicsandgovernance