International Journal of Politics and Governance Issues
Volume 1, Issue 1, Mei 2026
E-ISSN : xxx-xxxx

Digital Sovereignty, Cyber Governance, and Democratic Resilience: Comparative Institutional Analysis of the European Union and China in the Age of Geopolitical Technological Competition

Liwen Matsuda[1]

Liwen Matsuda

School of Global Governance
Waseda University
Email: liwen.matsuda@waseda.jp

***Corresponding Author:** liwen.matsuda@waseda.jp

Citation: Aziz (2026). Digital Sovereignty, Cyber Governance, and Democratic Resilience: Comparative Institutional Analysis of the European Union and China in the Age of Geopolitical Technological Competition (Book Antiqua 14pt Bold). *International Journal of Politics and Governance Issues*, *10*(4), xx–xx. https://doi.org/0000-0000

Published: 20/05/2026

ABSTRACT

The intensification of geopolitical technological competition has transformed digital governance into a central arena of global political contestation. States increasingly frame digital infrastructure, artificial intelligence, cybersecurity, data governance, and platform regulation as matters of national sovereignty, economic security, and institutional resilience. This article examines how contrasting political institutions shape cyber governance and digital sovereignty strategies through a comparative analysis of the European Union and China. While both actors seek technological autonomy and governance control over digital ecosystems, they pursue fundamentally different institutional pathways. The European Union emphasizes regulatory governance, democratic accountability, data protection, and multilevel institutional coordination, whereas China advances a centralized state-centric model integrating cybersecurity governance, industrial strategy, and digital political control. Using comparative governance analysis and institutional political economy approaches, this study investigates how political institutions mediate digital sovereignty implementation, cybersecurity governance, democratic legitimacy, and socio-economic resilience. Drawing on OECD reports, EU regulatory frameworks, Chinese digital governance policies, World Bank governance indicators, cybersecurity governance literature, and international institutional reports, the findings indicate that digital sovereignty is not merely a technological issue but a political-institutional process shaped by

Copyright © 2025 by Author/s. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

governance structures, state capacity, and geopolitical strategy. The article contributes to comparative politics and governance scholarship by developing a framework linking digital sovereignty, institutional coordination, cyber governance, democratic resilience, and sustainable technological development in the evolving global digital order.

Keywords: digital sovereignty; cyber governance; comparative politics; geopolitical competition; democratic resilience; European Union; China; digital governance; artificial intelligence governance; state capacity

INTRODUCTION

The global political order is increasingly shaped by struggles over technological power, digital infrastructure, and cyber governance. Digital technologies are no longer viewed solely as economic instruments or communication tools; they have become strategic assets central to state sovereignty, geopolitical influence, democratic governance, and national security. Governments across the world now regard artificial intelligence (AI), semiconductors, cloud infrastructure, data governance, cybersecurity systems, and digital platforms as foundational components of state capacity and institutional resilience (Farrell & Newman, 2023).

This transformation has accelerated amid intensifying geopolitical fragmentation, growing cyber insecurity, and the politicization of global technological supply chains. The World Economic Forum identifies cyber insecurity and technological fragmentation among the most significant global systemic risks of the coming decade (World Economic Forum, 2024). Similarly, OECD governance assessments emphasize that AI governance, data regulation, and digital public infrastructure increasingly shape democratic accountability, public trust, and economic competitiveness (OECD, 2024). The emergence of digital sovereignty as a governance paradigm reflects broader concerns regarding foreign technological dependence, platform monopolization, cyber vulnerabilities, and institutional exposure to geopolitical disruption.

The COVID-19 pandemic further reinforced the strategic importance of digital governance. States became heavily dependent on digital infrastructure for public administration, health governance, education systems, economic coordination, and crisis communication. However, the pandemic also exposed vulnerabilities concerning digital dependence, cybersecurity fragility, algorithmic governance risks, and unequal technological capacity across political systems (Ansell et al., 2021). Consequently, governments increasingly seek to secure technological autonomy while simultaneously regulating digital ecosystems in accordance with domestic political institutions and governance priorities.

Yet digital sovereignty remains deeply contested conceptually and institutionally. Liberal democratic systems frequently define digital sovereignty through regulatory autonomy, privacy rights, democratic accountability, and rules-based governance. By contrast, centralized authoritarian systems often conceptualize digital sovereignty through state control over cyberspace, data localization, platform

© 2025 by Author/s

governance, and political information management (Creemers, 2022). This divergence reflects broader differences concerning the relationship between the state, markets, citizens, and technological authority.

The European Union (EU) and China provide analytically significant comparative cases because both actors have emerged as major global digital governance powers while embodying contrasting institutional models. The EU advances a regulatory governance framework emphasizing digital rights, data protection, platform accountability, ethical AI governance, and multilevel institutional coordination. Its digital sovereignty agenda seeks to reduce technological dependence while preserving democratic norms and market integration (European Commission, 2023). China, by contrast, promotes a state-centric digital sovereignty model integrating cybersecurity governance, industrial policy, technological self-reliance, and centralized political authority (Kostka, 2023).

The comparison is particularly important because both systems influence the future trajectory of global governance. The EU increasingly shapes international digital regulation through the "Brussels Effect," whereby EU standards influence global corporate and governance behavior (Bradford, 2020). China simultaneously expands digital influence through technological infrastructure investment, platform expansion, digital Silk Road initiatives, and AI industrial strategy (Triolo & Goodman, 2023). Consequently, digital sovereignty has become both a domestic governance issue and an international geopolitical strategy.

Existing scholarship provides important but incomplete explanations regarding these developments. Cyber governance literature emphasizes cybersecurity institutions, digital regulation, and platform governance (DeNardis, 2020). Comparative political economy research examines technological competition, industrial policy, and state-market coordination (Mazzucato, 2021). Governance scholarship analyzes digital public administration and AI governance frameworks (Mergel et al., 2023). International relations literature investigates techno-geopolitics and strategic interdependence (Farrell & Newman, 2023). However, these literatures often remain disconnected from comparative institutional analysis concerning how political systems shape digital sovereignty implementation and democratic resilience.

Several gaps therefore remain. First, there is a theoretical gap concerning how political institutions mediate digital sovereignty governance. Existing studies frequently treat technological competition as primarily economic or geopolitical while underestimating institutional governance dynamics. Second, there is an empirical gap regarding how contrasting governance systems operationalize digital sovereignty through different institutional mechanisms. Third, there is a comparative governance gap because many studies examine either the EU or China independently rather than comparatively. Fourth, there is a democratic governance gap concerning how digital sovereignty affects accountability, transparency, and institutional legitimacy. Finally, there is a sustainability governance gap concerning whether digital sovereignty strategies contribute to long-term socio-economic resilience and stable governance systems.

This article addresses these gaps by developing a comparative institutional framework linking political institutions, cyber governance, digital sovereignty, and democratic resilience. It argues that digital sovereignty is best understood as an institutional governance strategy through which states seek to coordinate

Copyright © 2025 by Author/s. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

technological infrastructure, cybersecurity systems, economic competitiveness, and political legitimacy under conditions of geopolitical uncertainty.

The article advances the following analytical framework:

Political Institutions → Digital Sovereignty Governance → Cybersecurity Coordination → Technological Resilience → Democratic and Socio-Economic Stability

Within this framework, political institutions shape the governance logic underpinning digital sovereignty strategies. Governance structures determine how cybersecurity coordination mechanisms are organized, which in turn influence technological resilience and broader socio-economic stability outcomes.

The article contributes to comparative politics and governance scholarship in four ways. First, it integrates digital sovereignty with comparative institutional governance theory. Second, it provides empirical comparison between democratic-regulatory and centralized-state digital governance systems. Third, it contributes to cyber governance scholarship by linking cybersecurity with political legitimacy and institutional resilience. Fourth, it develops policy-relevant insights concerning AI governance, platform regulation, cyber governance coordination, and sustainable technological development.

The research objective is therefore to analyze how contrasting political institutions in the European Union and China shape digital sovereignty governance and to explain the implications for cyber governance, democratic resilience, and sustainable socio-economic development.

METHODOLOGY

This study employs comparative governance analysis and institutional political economy approaches to examine how political institutions shape digital sovereignty and cyber governance strategies in the European Union and China. The cases were selected through a most-different systems comparative design because both actors possess substantial technological capacity, strategic digital governance agendas, and global influence over cyber governance norms, yet differ fundamentally in political institutional structure, governance legitimacy mechanisms, state-society relations, and regulatory traditions. The European Union represents a multilevel democratic-regulatory governance system emphasizing legal accountability, market regulation, and rights-based governance, whereas China represents a centralized state-centric governance model integrating digital governance with national security, industrial strategy, and political authority. The analysis focuses on five governance variables: institutional coordination capacity, cybersecurity governance architecture, digital regulatory systems, technological industrial strategy, and legitimacy mechanisms. These variables are examined through comparative analysis of AI governance frameworks, cybersecurity laws, platform regulation systems, digital infrastructure policy, and international digital governance strategies.

The empirical analysis draws upon triangulated evidence from European Union digital governance legislation, Chinese cybersecurity governance policies, OECD digital governance reports, World Bank governance indicators, international cybersecurity assessments, academic journal literature, policy implementation reports, and geopolitical technology analyses published between 2020 and 2026. Comparative process tracing is used to identify causal

 © 2025 by Author/s

governance mechanisms linking political institutions with digital sovereignty implementation outcomes, while interpretive institutional analysis assesses how governance systems mediate cybersecurity coordination, digital regulation, and technological resilience. Reliability is strengthened through cross-source verification across international governance datasets, legal documents, and peer-reviewed scholarship. Ethical considerations involve avoiding unverifiable intelligence claims and distinguishing empirically grounded governance analysis from normative geopolitical discourse. The study's limitations include the evolving nature of AI governance regulation and the difficulty of fully isolating digital sovereignty governance from broader geopolitical competition dynamics.

Findings and Discussion

1. Institutional Foundations of Digital Sovereignty

The comparison demonstrates that digital sovereignty is fundamentally shaped by political institutional structures rather than technological capability alone. The European Union and China both seek strategic technological autonomy, yet they pursue this objective through contrasting governance models reflecting different political principles and institutional traditions.

The European Union conceptualizes digital sovereignty primarily through regulatory governance, market coordination, and democratic accountability. Its governance model emphasizes legal harmonization, data protection, platform regulation, and strategic reduction of dependence on foreign technological infrastructure. Major regulatory frameworks such as the General Data Protection Regulation (GDPR), Digital Services Act (DSA), Digital Markets Act (DMA), and AI Act illustrate the EU's effort to institutionalize digital governance through rules-based coordination (European Commission, 2023).

This governance model reflects the EU's broader multilevel institutional structure. Digital sovereignty implementation requires coordination among EU institutions, member states, regulatory agencies, private firms, and civil society actors. Consequently, the EU's governance capacity depends heavily on regulatory legitimacy, institutional interoperability, and transnational coordination.

China's digital sovereignty framework differs fundamentally. The Chinese governance model conceptualizes cyberspace as an extension of state sovereignty requiring centralized coordination, cybersecurity control, and political stability management (Creemers, 2022). Digital governance is closely integrated with national security, industrial modernization, and centralized administrative authority. Regulatory institutions such as the Cyberspace Administration of China coordinate data governance, platform regulation, cybersecurity enforcement, and AI governance within a highly centralized institutional framework.

The comparison reveals that digital sovereignty governance emerges through different institutional logics. The EU seeks governance authority through legal regulation and market governance, whereas China seeks governance authority through centralized administrative coordination and political control. This divergence reflects broader institutional differences concerning democratic governance, state legitimacy, and the role of technology in governance systems.

Importantly, the findings indicate that digital sovereignty is not inherently authoritarian or democratic. Rather, political institutions determine whether digital sovereignty governance prioritizes rights protection, market coordination,

Copyright © 2025 by Author/s. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

centralized authority, or hybrid governance arrangements.

---

2. Cybersecurity Governance and Institutional Coordination

Cybersecurity governance constitutes a central mechanism linking digital sovereignty with institutional resilience. Both the EU and China perceive cyber governance as essential to economic security, political stability, and technological competitiveness. However, their governance coordination systems differ significantly.

The EU's cybersecurity governance architecture is characterized by multilevel coordination among member states, EU institutions, and regulatory agencies. Institutions such as the European Union Agency for Cybersecurity (ENISA) support cybersecurity harmonization and cross-border coordination. The EU also increasingly integrates cybersecurity into broader industrial and geopolitical strategy through digital infrastructure investment and strategic technology policy.

Nevertheless, the EU's governance structure creates coordination challenges. Member states retain significant autonomy over national cybersecurity policy, resulting in uneven implementation capacity and fragmented strategic coordination. The evidence suggests that multilevel governance strengthens accountability and legal oversight but may weaken rapid strategic responsiveness during cyber crises.

China's cybersecurity governance model emphasizes centralized strategic coordination. National cybersecurity institutions possess broad authority to regulate platforms, monitor cyber threats, enforce data governance rules, and coordinate digital infrastructure security. The Chinese governance model enables rapid policy implementation and centralized crisis management.

However, centralized cybersecurity governance also creates governance trade-offs concerning transparency, accountability, and international trust. International observers frequently express concern regarding surveillance governance, data localization policies, and the relationship between cybersecurity governance and political control (Freedom House, 2024).

The comparison demonstrates that institutional coordination structures strongly influence cyber governance resilience. Distributed democratic coordination may strengthen legitimacy but complicate rapid implementation, whereas centralized coordination may enhance strategic responsiveness while increasing risks of governance opacity.

This finding contributes to cyber governance literature by demonstrating that cybersecurity effectiveness depends not solely on technical capability but also on institutional governance structures and legitimacy systems.

---

3. Platform Governance, AI Regulation, and Political Legitimacy

The governance of digital platforms and AI systems reveals deeper differences concerning political legitimacy and state authority. Both the EU and China seek to regulate large technology platforms and emerging AI systems, yet their regulatory objectives differ substantially.

The EU emphasizes democratic accountability, consumer protection, market fairness, and ethical AI

© 2025 by Author/s

governance. The Digital Services Act and AI Act seek to regulate algorithmic systems, platform responsibility, and AI risk management through legal accountability frameworks. This reflects a governance philosophy prioritizing rights protection and democratic legitimacy.

The EU's governance approach has significant global influence because multinational technology firms frequently adapt operations to comply with EU regulatory standards. This phenomenon strengthens the EU's geopolitical influence despite limited technological platform dominance.

China's platform governance model is more directly integrated with political stability and strategic industrial policy. Chinese authorities regulate platforms not only to address market concentration but also to maintain political control, data sovereignty, and national security coordination (Kostka, 2023). AI governance is similarly embedded within broader state-led technological modernization strategies.

The comparison reveals that AI governance is fundamentally political because algorithmic systems shape information flows, economic coordination, and public authority. Consequently, AI governance reflects broader institutional priorities concerning accountability, legitimacy, and political order.

The findings also indicate that public trust in digital governance depends upon institutional legitimacy mechanisms. In democratic systems, legitimacy is frequently associated with transparency, rights protection, and legal accountability. In centralized systems, legitimacy is more strongly associated with governance effectiveness, social stability, and administrative performance.

---

4. Digital Sovereignty and Geopolitical Political Economy

Digital sovereignty increasingly functions as a geopolitical political economy strategy. Both the EU and China seek to reduce strategic dependence on foreign technological infrastructure while strengthening domestic innovation ecosystems and industrial resilience.

The EU's digital sovereignty strategy emphasizes semiconductor policy, cloud infrastructure investment, AI innovation, and digital market regulation. European policymakers increasingly frame technological dependence as a strategic vulnerability affecting economic autonomy and democratic governance capacity.

China's strategy is more explicitly developmental and state-led. Programs such as "Made in China 2025" and AI industrial policy initiatives seek technological self-reliance and global competitiveness through coordinated state investment, industrial planning, and digital infrastructure expansion (Triolo & Goodman, 2023).

The comparison demonstrates that digital sovereignty governance reshapes global political economy structures. Technology governance now influences trade relations, industrial policy, geopolitical alliances, and development trajectories. Consequently, cyber governance cannot be separated from broader questions concerning global governance transformation and strategic competition.

Importantly, however, the findings suggest that sustainable technological development requires balancing strategic autonomy with international interoperability. Excessive fragmentation of digital governance systems risks reducing innovation coordination, increasing geopolitical tensions, and weakening global technological cooperation.

Copyright © 2025 by Author/s. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Table 1. Analytical Matrix of Comparative Politics and Governance Development

Variable	European Union	China	Empirical Evidence	Analytical Interpretation
Political Institution	Multilevel democratic governance	Centralized state-centric governance	EU institutional frameworks; Chinese governance policies	Political systems shape digital sovereignty logic
Digital Sovereignty Strategy	Regulatory autonomy and rights protection	State control and technological self-reliance	GDPR, DSA, Chinese Cybersecurity Law	Governance priorities reflect institutional legitimacy structures
Cybersecurity Governance	Distributed multilevel coordination	Centralized strategic coordination	ENISA reports; Chinese cybersecurity frameworks	Coordination structure influences crisis responsiveness
AI Governance	Ethical and legal accountability	Strategic and state-directed AI governance	EU AI Act; Chinese AI regulations	AI governance reflects broader political authority structures
Platform Regulation	Market fairness and democratic accountability	Political stability and state authority	Platform governance legislation	Regulatory goals differ across governance systems
Public Legitimacy Mechanism	Rights-based democratic legitimacy	Performance and stability-based legitimacy	Governance and trust indicators	Digital governance legitimacy varies institutionally
Industrial Strategy	Strategic autonomy and innovation coordination	Developmental state-led modernization	Semiconductor and AI industrial policies	Technological governance linked to political economy
Sustainability Implication	Institutional legitimacy with coordination complexity	Strategic efficiency with accountability challenges	OECD and World Bank governance assessments	Sustainable digital governance requires balance between coordination and legitimacy

The table demonstrates that digital sovereignty governance reflects broader institutional and political-economic structures rather than purely technological concerns. The EU's governance model emphasizes democratic legitimacy and regulatory coordination, whereas China's model prioritizes centralized coordination and strategic control. Both systems possess strengths and vulnerabilities concerning governance resilience, technological innovation, and

© 2025 by Author/s

international legitimacy.

Theoretical Propositions

Proposition 1: Political institutions mediate the relationship between technological modernization and digital sovereignty governance.
Technological capacity alone does not determine governance outcomes; institutional structures shape how states regulate, coordinate, and legitimize digital governance systems.

Proposition 2: Cybersecurity resilience depends on institutional coordination mechanisms rather than technical infrastructure alone.
Effective cyber governance requires coherent institutional integration among regulatory agencies, political authorities, and governance systems.

Proposition 3: AI governance reflects broader legitimacy structures within political systems. Democratic systems prioritize accountability and rights protection, whereas centralized systems prioritize strategic coordination and political stability.

Proposition 4: Sustainable digital sovereignty requires balancing strategic autonomy with governance legitimacy and international interoperability.
Excessive fragmentation or centralization may undermine long-term technological resilience and governance stability.

CONCLUSION

This article analyzed how contrasting political institutions in the European Union and China shape digital sovereignty governance, cybersecurity coordination, and democratic resilience. The findings demonstrate that digital sovereignty is fundamentally an institutional governance process rather than merely a technological or geopolitical strategy.

The European Union advances a democratic-regulatory governance model emphasizing legal accountability, data protection, and multilevel coordination. This framework strengthens democratic legitimacy and international regulatory influence but also creates implementation complexity and coordination fragmentation. China advances a centralized state-centric governance model integrating cybersecurity, industrial strategy, and political authority. This framework enables rapid coordination and strategic mobilization but raises concerns concerning transparency, accountability, and governance openness.

The article contributes theoretically by integrating comparative governance analysis with cyber governance and digital sovereignty scholarship. Existing literature frequently treats technological competition primarily through geopolitical or economic frameworks while underestimating institutional governance dynamics. This study instead demonstrates that political institutions strongly shape how digital sovereignty strategies are implemented and legitimized.

Copyright © 2025 by Author/s. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Empirically, the article contributes comparative evidence concerning cybersecurity governance, AI regulation, platform governance, and technological political economy. The findings indicate that governance resilience depends upon balancing institutional coordination, democratic legitimacy, technological autonomy, and international interoperability.

The policy implications are substantial. Governments pursuing digital sovereignty strategies should prioritize institutional interoperability, governance transparency, cybersecurity coordination, and accountable AI governance frameworks. Sustainable digital governance requires integrating technological modernization with democratic legitimacy and international governance cooperation.

Several limitations should nevertheless be acknowledged. The study focused primarily on macro-level governance structures and therefore did not fully examine local governance variation, corporate governance dynamics, or civil society digital activism. Future research should investigate how digital sovereignty governance affects developing countries, regional organizations, and global governance institutions.

Ultimately, this article argues that the future global order will increasingly depend upon how political institutions govern digital transformation, cybersecurity, and technological power under conditions of geopolitical fragmentation and accelerating technological change.

REFERENCES

Ansell, C., Sørensen, E., & Torfing, J. (2021). The COVID-19 pandemic as a game changer for public administration and leadership. Public Management Review, 23(7), 949–960.

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

Creemers, R. (2022). China's evolving cybersecurity and data governance regime. China Information, 36(2), 147–168.

DeNardis, L. (2020). The Internet in Everything: Freedom and Security in a World with No Off Switch. Yale University Press.

European Commission. (2023). European Declaration on Digital Rights and Principles. European Commission.

Farrell, H., & Newman, A. (2023). Underground Empire: How America Weaponized the World Economy. Henry Holt.

Freedom House. (2024). Freedom on the Net 2024. Freedom House.

Fukuyama, F. (2014). Political Order and Political Decay. Farrar, Straus and Giroux.

Kostka, G. (2023). China's governance of artificial intelligence and platform regulation. Policy & Internet, 15(2), 189–208.

Mazzucato, M. (2021). Mission Economy: A Moonshot Guide to Changing Capitalism. Harper Business.

Mergel, I., Ganapati, S., & Whitford, A. (2023). Agile governance capacity in the digital era. Government

 © 2025 by Author/s

Information Quarterly, 40(1), 101759.

OECD. (2024). Digital Government Review 2024. OECD Publishing.

Pierre, J., & Peters, B. G. (2020). Governance, Politics and the State (2nd ed.). Red Globe Press.

Triolo, P., & Goodman, S. (2023). Digital Silk Road governance and geopolitical technology competition. Journal of Cyber Policy, 8(1), 55–74.

United Nations. (2024). E-Government Survey 2024. United Nations Department of Economic and Social Affairs.

World Bank. (2024). GovTech Maturity Index 2024. World Bank.

World Economic Forum. (2024). Global Risks Report 2024. World Economic Forum.

Bennett, C. J., & Raab, C. (2020). The Governance of Privacy. MIT Press.

Castells, M. (2021). The Rise of the Network Society (2nd ed.). Wiley-Blackwell.

Cingolani, L. (2022). State capacity and governance reform in the digital era. World Development, 151, 105743.

IMF. (2023). Digitalization and Public Sector Transformation. International Monetary Fund.

UNDP. (2024). Governance for People and Planet. United Nations Development Programme.

Copyright © 2025 by Author/s. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.