International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 13 Issue 10 ǁ October 2025 ǁ PP. 151-158

Digital Sovereignty as National Security: Why Countries Must Build Indigenous AI and Data Infrastructure in an Era of Technological Weaponization

Venkateswara Rao Bobbili
Responsible AI Transformation Evangelist and Architect, Email id: data.bobbili@gmail.com

Abstract
The rise of data as a strategic economic resource, paired with artificial intelligence's transformation of nearly every sector, has reshaped modern national security and global relations. This article provides a comprehensive, case-driven analysis of digital sovereignty, encompassing both data-centric and AI-centric perspectives, establishing it as essential in contemporary geopolitical strategy. Through global policy review and practical case studies, the research lays out how nations must invest in home grown digital infrastructure and software platforms to maintain autonomy, competitiveness, and security. It demonstrates how digital dependencies create security, economic, and governance vulnerabilities that can be weaponized—making digital sovereignty not merely a technological decision but a national security necessity.

Keywords: *Digital sovereignty, data sovereignty, AI sovereignty, geopolitics, national security, digital infrastructure, technological independence.*

Date of Submission: 12-10-2025 Date of acceptance: 26-10-2025

I. INTRODUCTION

In the contemporary digital landscape, control over data, infrastructure, and artificial intelligence defines the boundaries of state power and influence. Digital sovereignty—encompassing both oversight of data flows and mastery of AI capabilities—signifies a nation's formal capacity to govern digital infrastructure and technology, both within and beyond its borders [26]. Never has this issue been more pressing. The global acceleration of digital transformation, highlighted by the COVID-19 pandemic, revealed both the opportunities and dangers embedded in interconnected systems. While advanced digital platforms enabled resilience, they also exposed nations to the risks of dependency on foreign-controlled technology and platforms [25]. These dependencies raise critical concerns regarding security, economic leverage, and the preservation of political autonomy. Major Powers, especially the United States and China, have dramatically sharpened their focus on digital control, triggering new international tensions. Bans and restrictions on Huawei, TikTok, and dozens of other platforms reveal how technology now sits at the core of strategic statecraft [29].

This paper contends that the dual pillars of data sovereignty and AI sovereignty are no longer just technical or regulatory concerns. They have evolved into strategic imperatives that every nation must address as part of their fundamental security and economic policy. The analysis moves from theoretical perspectives and literature, through quantitative and qualitative case studies, to practical policy recommendations.

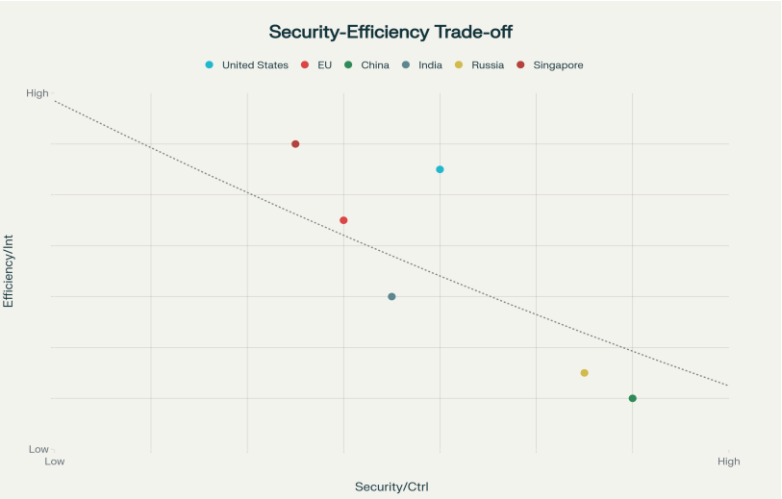

Figure 1: Balancing Security and Efficiency: The National Trade-off in Pursuing Digital Sovereignty

II. LITERATURE REVIEW

2.1 Conceptualizing Digital Sovereignty

The concept of digital sovereignty builds on earlier debates around cyber sovereignty and governance of the internet.[15]describes it as a country's independent ability to maintain and develop its digital assets, skills, and rule-making authority. This encompasses technology competence, legal structures, and the freedom to set policies aligned with national priorities.

[26]Highlight the spectrum between restrictive, protectionist strategies and more open models, favouring regulatory control but allowing transnational flows. Most nations find themselves somewhere in between, blending these models according to their context and perceived risk.

2.2 Data Sovereignty in International Relations

Data sovereignty empowers countries to enforce jurisdiction over data generated by their residents, organizations, and infrastructure [17]. The EU's GDPR is a pioneering framework that asserts comprehensive rules for data handling, inspiring similar moves around the globe [6].

[10] Caution, however, that sovereignty comes with trade-offs. Requiring data localisation, for instance, might shrink economic efficiency, imposing GDP losses that range widely by country and digital integration level.

2.3 AI Sovereignty and Strategic Competition

AI sovereignty, while closely related, centers on ownership, development, and regulation of artificial intelligence. Leading nations have invested heavily in domestic AI R&D, aiming to insulate their economies and critical infrastructures from foreign control or manipulation [27].

Figure 2: Global Digital Sovereignty Strategies: Diverse Approaches to Data and AI Control by Major Nations (2015–2024)

[19] frames AI as a new arena of zero-sum competition, where technological leadership directly translates to economic might and military influence.

2.4 Geopolitical Implications of Digital Dependencies

[14]Introduce the idea of "weaponized interdependence," where connections and networks, rather than isolation, become tools for coercion. Those at the core of digital infrastructure wield outsized leverage—making digital sovereignty a defensive priority for nations worried about exclusion or manipulation.

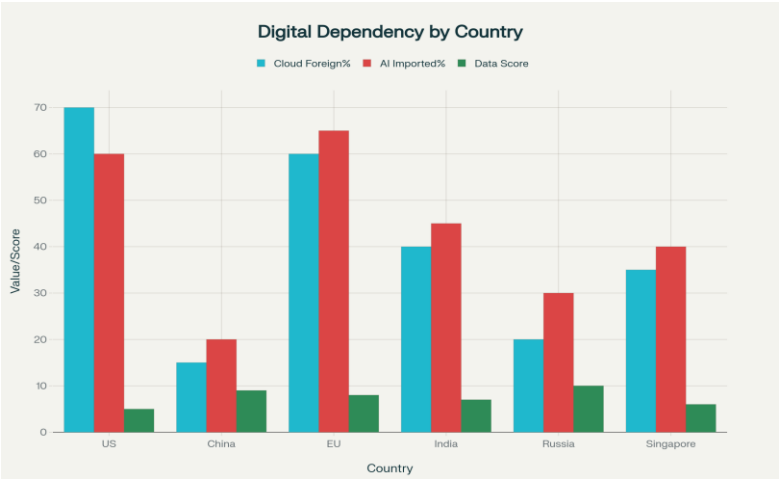

Figure 3: Comparative Metrics of Digital Dependency and Sovereignty across Key Geopolitical Powers (2024)

As [13]and [29]explain, this expansion of "technological nationalism" means states increasingly treat technology policy as central to their power and competitive edge, driving deep government involvement in tech markets and innovation systems.

III. THEORETICAL FRAMEWORK

3.1 Strategic Autonomy as Digital Sovereignty

This study applies the concept of strategic autonomy to the digital domain, echoing EU foreign policy debates [5]. Digital sovereignty becomes not just about independence, but about retaining the option—acting alone where necessary, cooperating when beneficial. From this perspective, national digital sovereignty requires:
Technological competence: The capability to build, maintain, and enhance critical digital systems.
Regulatory authority: Discretion to regulate platforms and activities within domestic boundaries.
Choice in engagement: The ability to opt for partnership, rivalry, or isolation based on state interests.

3.2 The Security-Efficiency Trade-off

Global digital interconnection delivers efficiency gains—economies of scale, specialization, faster innovation. Yet, [2] argue, these benefits come with new exposures. Countries must weigh the efficiencies against security concerns, seeking the appropriate balance for their strategic setting.

3.3 Hierarchies in Digital Networks

[9] adds that global digital networks are hierarchical, not flat. Some nations and firms occupy powerful, central roles, conferring network power that can be exercised for control or exclusion. Recognizing these hierarchies is vital for shaping national policy response.

IV. METHODOLOGY

This research adopts a mixed-methods approach, integrating qualitative case studies and quantitative analysis. Six countries/entities are studied for contrast: the United States, China, European Union, India, Russia, and Singapore each offering a distinct model due to its technological maturity and geopolitical stance. Primary data sources: government documents, industry and academic reports, and statistical indicators covering 2015–2024.

Key metrics include: Foreign versus domestic ownership of cloud infrastructure, The share of domestic versus imported AI technologies, Depth and enforcement of data localization laws, Government procurement and investment in domestic tech firms and R&D budget allocation.

V. CASE STUDIES IN DIGITAL SOVEREIGNTY

5.1 United States: Hegemonic Leadership and Security Strategizing

Historically, U.S. corporations have dominated the global tech sector. Yet rising Chinese capabilities have reawakened security concerns and prompted new sovereignty initiatives [29].

Important policies: CFIUS reforms for scrutinizing foreign tech investments, Export controls covering semiconductors and advanced AI, CHIPS and Science Act ($52B allocated for U.S.-based semiconductor manufacturing), Executive orders fostering leadership in AI and biotech.

The U.S. strategy is one of ongoing technological dominance, seeking to maintain its lead and restrict rivals' access while fortifying critical infrastructure.

5.2 China: Pursuing Comprehensive Digital Autonomy

China's approach is among the most extensive. Through domestic investment, regulatory restriction, and robust support for national champions, it combines independence with innovation [27].

Notable features: The Great Firewall and network controls, Promotion of Alibaba, Tencent, ByteDance, and other giants, Legal compulsions for data localization, Large-scale investment in next-gen AI (New Generation AI Development Plan), Infrastructure deployment (5G, data centres, etc.),

China's system builds internal strength but limits integration with open global platforms.

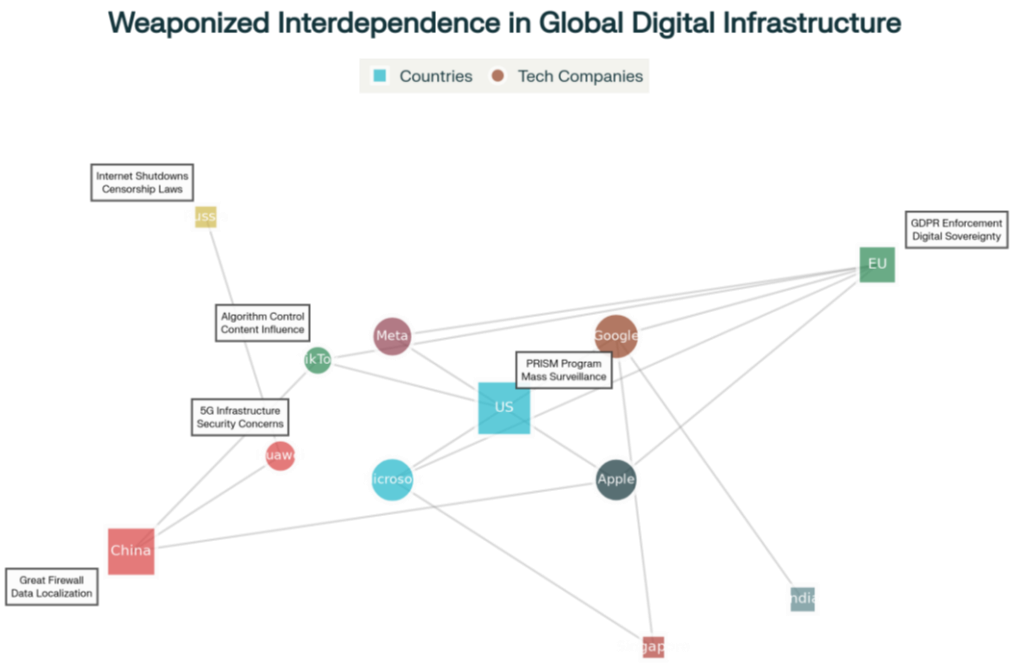

Figure 4: Network Structures and Power: How Global Digital Interdependence Can Be Leveraged for Strategic Advantage

5.3 European Union: Shaping Sovereignty through Regulation
The EU's digital sovereignty model is regulatory, not domination-centered. It leverages its market size and legal influence (GDPR, Digital Services/Markets Acts, Gaia-X, and pending AI Act) to enforce standards and shape governance worldwide [26].

Despite its regulatory prowess, the EU still depends heavily on U.S. and Chinese infrastructure, leading critics to call for deeper investment in indigenous technologies.

5.4 India: Innovation, Inclusion, and Selective Restriction
India's twin strategies—Digital India and Atmanirbhar Bharat—seek to boost self-reliance without losing the benefits of open markets.

Key moves: Banning TikTok, WeChat after border conflicts, Home grown digital infrastructure (UPI, Aadhaar), Incentives for electronics/semiconductors, Critical data storage mandates, Investments in fiber and 5G, India navigates between rapid advancement and concern over foreign dependencies, especially vis-à-vis China.

5.5 Russia: Defensive Sovereignty in an Adversarial World
Geopolitical pressures have driven Russia to increasingly isolate its digital landscape.

Measures include: The "sovereign internet" law separating domestic networks, Compulsory data localization, blocking foreign social platforms, Building native payment/tech platforms, Broad cybersecurity legislation, Russia's digital sovereignty is rooted in defense prioritizing insulation over openness or innovation [24].

5.6 Singapore: Smart Nation, Smart Balance
Singapore adopts national security with global openness under its Smart Nation initiative [30].

Major steps: Investment in infrastructure and AI, Partnerships across sectors, Targeted restrictions for sensitive systems, sophisticated data and privacy laws, Emphasis on international cooperation.

Singapore's example shows how smaller countries can achieve meaningful sovereignty through smart investment and balanced policy.

VI. ANALYSIS: CORE IMPERATIVES FOR NATIONAL DIGITAL INFRASTRUCTURE

6.1 Security and Autonomy

Security is the dominant driver of digital sovereignty. Foreign-operated infrastructure and platforms create exposure on several fronts:

Surveillance/Espionage: Foreign suppliers may access sensitive government, corporate, or personal data [16].
Economic leverage: Dependence can give adversaries the power to disrupt or manipulate markets [11].
Critical infrastructure: Foreign control presents risk to utilities, finance, transit, and other social essentials [20].

6.2 Economic Growth and Innovation

Domestic control is also about retaining value and fostering innovation.
Value capture: Sovereign platforms keep more profits and knowledge within national borders [22].
Innovation ecosystems: Focusing R&D domestically spurs cross-sector growth [7].
Industrial policy: Governments can use sovereignty to direct development of strategic sectors [21].

6.3 Democratic Governance and Social Stability

Content and information control: National systems allow governments to moderate content, strengthen stability, but also raise the risk of censorship [28].
Values and regulation: Sovereignty permits platforms to reflect domestic values around privacy, expression, and rights [31].
Law enforcement: Enforcement of tax, privacy, and content laws is more feasible with homegrown platforms [6].

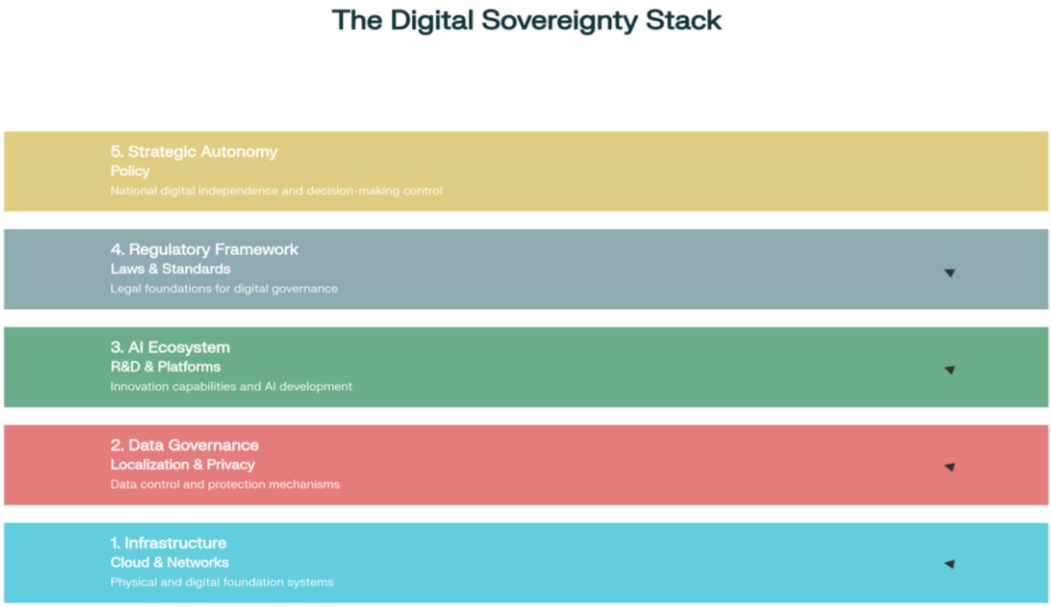

Figure 2: Key Components of National Digital Sovereignty from Foundational Infrastructure to Strategic Policy

VII. CHALLENGES AND COSTS OF DIGITAL SOVEREIGNTY

7.1 Economic Burden

Development investments: Infrastructure and skill-building require major funding, a challenge for smaller economies [32].
Efficiency losses: Mandating data localization or restricting foreign technologies reduces network effects and scale economics [3].

Innovation limits: Overly rigid policies block international collaboration and best practice transfer [18].

7.2 Technical Barriers

Complexity: Building and maintaining independent systems is technologically difficult [1].
Fragmentation: Divergent standards may hurt global interoperability, increase local costs [14].
Talent deficit: Skilled workforce shortages slow the progress of sovereignty ambitions [33].

7.3 Diplomatic Repercussions

Trade disputes: Sovereignty measures frequently clash with trade agreements [8].
Strained relations: Restrictions may hurt diplomatic ties and wider cooperation [29].
Governance fragmentation: Sovereignty undermines shared governance solutions for issues like cybersecurity or privacy [12].

VIII. BEST PRACTICES AND POLICY RECOMMENDATIONS

Digital sovereignty is becoming increasingly complex due to rapid advances in technology, shifting geopolitical dynamics, and deepening societal impacts. Strategic management requires a nuanced and layered approach. Countries should prioritize maximum domestic control and ownership of their critical infrastructure, ensure robust oversight and local development for strategic technologies, and maintain minimum intervention with clear compliance requirements for general digital services.

To support these strategies, investing in human capital is essential. This means enhancing education and skills in computer science, artificial intelligence, data, and cybersecurity, while blending public and private sector incentives for research and innovation. Collaboration between industry and academia should be encouraged to pool expertise and drive new solutions.[34]

On the international stage, nations must actively engage in shaping global standards—balancing multilateral cooperation to influence rules that protect domestic interests, establishing bilateral partnerships that reduce dependency on potentially hostile actors, and participating in technical standards bodies to ensure local needs and values are reflected.

Regulatory development must keep pace with technological change. Policymakers should strike an effective balance between privacy, innovation, and economic growth in data governance, foster fair competition by regulating global digital platforms, and implement strong cybersecurity standards to protect all digital systems.

IX. FUTURE IMPLICATIONS AND EMERGING TRENDS

Technology Trends like Quantum computing, edge computing, and block chain technologies are reshaping security and governance, intensifying the need for sovereignty and introducing new decentralization models, though also posing governance challenges. Whereas Geopolitical Shifts like Ongoing US–China tensions are leading to technological fragmentation. Emerging powers like India, Brazil, and Indonesia are influencing global standards, with regional bodies (EU, ASEAN) offering alternative integration approaches. While Economic and Social Impact in Digital world divides threaten to split nations by tech access. Shifts in sovereignty are changing innovation patterns and influencing cultural aspects such as privacy, democracy, and freedom of expression.

X. CONCLUSIONS

This comprehensive analysis affirms that digital sovereignty anchored in both data and AI mastery is a foundational strategic concern for nations in the 21st century. Across all case studies, the drivers are clear: security, economic reward, and governance independence. Building sovereign infrastructure and software platforms is far beyond a technical preference. It is about establishing national resilience against exploitation and surveillance, economic blackmail, strategic manipulation. Domestic capacity allows nations to capture the value of digital transformation, protect vital systems, and enforce local rules.

Yet, digital sovereignty is resource-intensive and complex. There are costs efficiency setbacks, technical uncertainty, and diplomatic strains. The pursuit must be flexible, balancing autonomy with selective international engagement and ongoing investment in talent and innovation. As quantum computing, AI, and edge architectures mature and geopolitical competition intensifies, digital sovereignty will only grow in salience. Nations that cultivate indigenous digital capacity and strategic agility will thrive in a world shaped by technological rivalry and opportunity.

Ultimately, digital sovereignty epitomizes a new wave of "strategic autonomy" where true independence is the power to choose, adapt, and innovate, not to isolate. While complete self-sufficiency may be unattainable, meaningful control of critical technology is now indispensable for national security, economic prosperity, and democratic integrity.

REFERENCES

[1] Baldwin, R. (2016). The Great Convergence: Information Technology and the New Globalization. Harvard University Press.
[2] Baldwin, R., & Lopez-Gonzalez, J. (2015). Supply-chain trade: A portrait of global patterns and several testable hypotheses. The World Economy, 38(11), 1682-1721.
[3] Basu, P. (2021). Digital sovereignty and the Indian state: From data localization to techno-nationalism. International Studies, 58(3), 245-264.
[4] Bauer, M., Ferracane, M. F., & van der Marel, E. (2014). The costs of data localization: Friendly fire on economic recovery. ECIPE Working Paper, 3/2014.
[5] Biscop, S. (2019). European strategy in the 21st century: New future for old power. Routledge.
[6] Bradford, A. (2020). The Brussels Effect: How the European Union Rules the World. Oxford University Press.
[7] Brynjolfsson, E., Rock, D., & Syverson, C. (2018). Artificial intelligence and the modern productivity paradox: A clash of expectations and statistics. The Economics of Artificial Intelligence, 23-57.
[8] Burri, M. (2017). The regulation of data flows through trade agreements. Georgetown Journal of International Law, 48(2), 407-448.
[9] Çalışkan, M. (2020). Digital hierarchies: The political economy of global technology governance. Review of International Political Economy, 27(4), 800-825.
[10] Chander, A., & Lê, U. P. (2015). Data nationalism. Emory Law Journal, 64(3), 677-739.
[11] Connolly, R. (2018). Russia's Response to Sanctions: How Western Economic Statecraft is Reshaping Political Economy in Russia. Cambridge University Press.
[12] DeNardis, L. (2020). The Internet in Everything: Freedom and Security in a World with No Off Switch. Yale University Press.
[13]Edgerton, D. (2007). The Shock of the Old: Technology and Global History Since 1900. Oxford University Press.
[14] Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. International Security, 44(1), 42-79.
[15] Floridi, L. (2020). Translating digital sovereignty into practice: The European Union as a case study. Philosophy & Technology, 33(3), 359-384.
[16]Greenwald, G. (2014). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. Metropolitan Books.
[17] Hummel, P., Braun, M., Beck, S., & Dabrock, P. (2021). Data sovereignty: A review. Big Data & Society, 8(1), 1-17.
[18] Jones, C. I., & Mack, A. (2014). The Economics of Innovation and Growth. MIT Press.
[19] Lee, K. F. (2018). AI Superpowers: China, Silicon Valley, and the New World Order. Houghton Mifflin Harcourt.
[20] Lewis, J. A. (2020). Cybersecurity and Critical Infrastructure Protection. Center for Strategic and International Studies.
[21] Mazzucato, M. (2013). The Entrepreneurial State: Debunking Public vs. Private Sector Myths. Anthem Press.
[22] McKinsey Global Institute. (2019). Digital China: Powering the Economy to Global Competitiveness. McKinsey & Company.
[23] National Academy of Sciences. (2019). Quantum Computing: Progress and Prospects. The National Academies Press.
[24] Nocetti, J. (2020). Russia's digital sovereignty: How realistic is it? Russia.Nei.Visions, No. 119, Ifri.
[25] OECD. (2020). Digital Government in Chile – Improving Public Service Design and Delivery. OECD Publishing.
[26] Pohle, J., & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4), 1-19.
[27] Roberts, H., Cowls, J., Morley, J., Taddeo, M., Wang, V., & Floridi, L. (2021). The Chinese approach to artificial intelligence: An analysis of policy, ethics, and regulation. AI & Society, 36(1), 59-77.
[28] Roberts, M. E. (2018). Censored: Distraction and Diversion Inside China's Great Firewall. Princeton University Press.
[29] Segal, A. (2020). When China Rules the Web: Technology in Service of the State. Foreign Affairs, 99(5), 10-18.
[30] Tan, E. (2021). Singapore's Smart Nation initiative: Digital transformation and technological sovereignty. Asian Journal of Comparative Politics, 6(2), 145-162.
[31] UNCTAD. (2019). Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries. United Nations Conference on Trade and Development.
[32] World Economic Forum. (2020). The Future of Jobs Report 2020. World Economic Forum.
[33] Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.
[34] Venkateswara Rao Bobbili(2025) Sovereignty in the Age of Artificial Intelligence: Intensifying Debates and New Directions. IRE Journals Volume 9 Issue 3 .ISSN: 2456-8880