INTERNATIONAL JOURNAL OF SOCIAL SCIENCES BULLETIN
ISSN: (E) 3007-1917 (P) 3007-1909
Volume 4, Issue 3, 2026

ARTIFICIAL INTELLIGENCE, DIGITAL SOVEREIGNTY, AND CYBER DIPLOMACY: PAKISTAN'S STRATEGIC POSITION IN THE EMERGING GLOBAL DIGITAL ORDER

Muhammad Umar[*1], **Qaisar Sharif**[2]

[*1]*Student, Department of Marxist Theory, Xian Jiaotong University*
[2]*MS/M.Phil Scholar, International Relations (IR), Balochistan University of Information Technology, Engineering and Management Sciences (BUITEMS) Quetta, Pakistan*

[*1]mu093958@gmail.com, [2]qaisarsharifgondal.buitems.edu.pk@gmail.com

[2]http://orcid.org/0009-0002-8670-1555

Corresponding Author: *
Muhammad Umar
DOI: https://doi.org/10.5281/zenodo.22227282

Received	Accepted	Published
26 January 2026	11 March 2026	25 March 2026

ABSTRACT

Artificial intelligence (AI) is becoming a strategic resource with implications for technological sovereignty, cybersecurity, diplomacy, and national autonomy. This study examines the relationships among AI capability, digital sovereignty, foreign technological dependence, cyber-diplomatic capacity, and Pakistan's strategic position in the emerging global digital order. Grounded in Resource Dependence Theory (RDT), the study conceptualizes AI capability as a strategic resource that can strengthen digital sovereignty and cyber-diplomatic capacity, while foreign technological dependence may constrain these effects. A quantitative, cross-sectional explanatory design was proposed using a structured five-point Likert-scale questionnaire administered purposively to professionals and experts in AI, cybersecurity, digital governance, information technology, technology policy, and international relations in Pakistan. PLS-SEM was selected to assess direct, mediation, and moderation relationships. The conceptual model proposes that AI capability strengthens digital sovereignty, which enhances cyber-diplomatic capacity and strategic position, while foreign technological dependence weakens the AI capability–digital sovereignty relationship. The study highlights the need to strengthen domestic AI capabilities, diversify technology partnerships, improve cybersecurity and data governance, and enhance Pakistan's participation in international AI and cyber governance.

Keywords: *Artificial intelligence capability; digital sovereignty; technological dependence; cyber diplomacy; strategic autonomy; Pakistan*

1. Introduction

AI has evolved from a technological application into a strategic capability affecting economic competitiveness, national security, governance, diplomacy, and international power. Its development depends on computing infrastructure, data, skilled human capital, digital platforms, cloud services, semiconductors, research ecosystems, and technical expertise. Unequal access to these resources can create technological dependence, particularly for developing states.

Digital sovereignty refers to a state's ability to exercise legitimate and effective control over critical digital resources, infrastructure, data, technologies, and policy choices. In the AI era, formal regulatory authority may coexist with dependence on foreign cloud infrastructure, proprietary models, platforms, software, computing resources, and supply chains. Therefore, sovereignty is better understood as

meaningful strategic choice under interdependence rather than complete technological self-sufficiency.

For Pakistan, this challenge is significant because AI offers opportunities in public services, education, health, agriculture, finance, cybersecurity, and industrial development, while the country's ecosystem faces constraints involving specialized skills, research capacity, advanced computing, foreign technology dependence, cybersecurity, and regulatory readiness. Cyber diplomacy provides a mechanism for converting technical capability into international influence through negotiations, partnerships, norm development, and participation in global digital governance.

The study addresses a gap in research by integrating AI capability, digital sovereignty, technological dependence, and cyber diplomacy within a Pakistan-focused framework. It therefore moves beyond AI adoption to examine how domestic capability can support strategic autonomy and international digital influence.

2. Problem Statement

The growing strategic importance of AI creates a dilemma for developing states: AI can accelerate modernization while dependence on foreign technological ecosystems can constrain autonomy. Pakistan has substantial potential to benefit from AI but remains exposed to limitations in advanced computing, specialized talent, research and development, foreign infrastructure and platforms, cybersecurity, and regulatory capacity. Existing literature commonly examines AI governance, digital sovereignty, and cyber diplomacy separately, leaving limited integrated empirical analysis for developing countries such as Pakistan. The central problem is therefore to understand how Pakistan can translate AI capability into digital sovereignty and cyber-diplomatic capacity while managing foreign technological dependence.

3. Research Questions

- What is the relationship between AI capability and digital sovereignty in Pakistan?
- To what extent does digital sovereignty influence cyber-diplomatic capacity?
- How does AI capability contribute to Pakistan's strategic autonomy and position?
- What role does cyber diplomacy play in translating technological capability into international influence?
- To what extent does foreign technological dependence constrain digital sovereignty?
- What institutional, technological, regulatory, and diplomatic capabilities can strengthen Pakistan's role in global AI and cyber governance?

4. Research Objectives

- To assess Pakistan's AI capability across technological, institutional, research, and human-capital dimensions.
- To examine the effect of AI capability on digital sovereignty.
- To determine the influence of digital sovereignty on cyber-diplomatic capacity.
- To evaluate the contribution of AI capability and digital sovereignty to strategic autonomy and position.
- To examine the constraining role of foreign technological dependence.
- To identify capabilities and policy measures required to strengthen Pakistan's role in global AI and cyber governance.

5. Significance of the Study

The study contributes theoretically by extending RDT to the state-level digital environment and linking technological resources with sovereignty and diplomatic influence. Practically, it highlights priorities for AI research, human-capital development, computing infrastructure, data governance, cybersecurity, regulatory capacity, strategic procurement, and supplier diversification. Strategically, it emphasizes that Pakistan need not pursue technological autarky; instead, it should build sufficient domestic capability and bargaining power to maintain meaningful choices within international technological interdependence.

6. Literature Review

6.1 AI and State Power

AI increasingly contributes to instrumental, structural, and discursive forms of state power. It improves information processing, forecasting, public administration, and security while allowing actors controlling critical

infrastructures and standards to influence the choices of others. Global AI governance is fragmented across governments, firms, international organizations, civil society, and technical communities. Developing states therefore require technological and institutional capacity to participate effectively.

6.2 AI Capability and Strategic Autonomy

AI capability extends beyond application adoption to human capital, research, computing, data, cybersecurity, institutional expertise, and innovation. Strategic autonomy does not require self-sufficiency; it requires sufficient domestic capacity and policy alternatives to prevent external dependencies from becoming strategic constraints.

6.3 Digital Sovereignty and Technological Dependence

Digital sovereignty is multidimensional, involving infrastructure, data, regulation, technological autonomy, institutional authority, and strategic choice. Foreign dependence can create lock-in, switching costs, and geopolitical vulnerability. Pakistan's dependence may occur across cloud services, advanced computing, AI models, software, semiconductors, cybersecurity technologies, and technical expertise. Diversification and domestic capability are therefore central to resilience.

6.4 Cyber Diplomacy and Global Digital Governance

Cyber diplomacy encompasses negotiations on cybersecurity, responsible state behaviour, cyber conflict, digital cooperation, data governance, emerging technologies, and international norms. AI increases both the technical complexity of these issues and the opportunities for information analysis, threat detection, and strategic forecasting. Pakistan can strengthen international influence through technical diplomatic expertise, multilateral engagement, regional cooperation, norm development, and technology partnerships.

6.5 Global South and Pakistan

Global South perspectives remain comparatively underrepresented in AI-governance research. Developing countries face distinct constraints involving infrastructure, regulatory capacity, technology dependence, data governance, and geopolitical competition. Pakistan therefore requires a context-sensitive strategy combining selective domestic capability development with diversified international cooperation.

6.6 Research Gap

Four gaps emerge: limited empirical integration of AI capability and digital sovereignty; insufficient specification of the sovereignty–cyber diplomacy relationship; underrepresentation of Global South states; and fragmented Pakistan-specific research. The present study addresses these gaps through an integrated model.

7. Underpinning Theory: Resource Dependence Theory

RDT, developed by Pfeffer and Salancik (1978), argues that dependence on externally controlled resources affects power, strategic behaviour, and autonomy. Applied to the digital state, critical resources include semiconductors, cloud computing, AI models, cybersecurity technologies, software, data-processing capacity, infrastructure, and technical expertise. AI capability is treated as an internal strategic resource; foreign technological dependence represents an external constraint; digital sovereignty represents the capacity to govern and strategically control resources; and cyber diplomacy represents the mechanism through which technological capacity can support international influence.

The theoretical chain is: AI Capability → Reduced Technological Dependence → Digital Sovereignty → Cyber-Diplomatic Capacity → Strategic Position.

8. Hypotheses and Conceptual Model

- H1: AI capability positively affects digital sovereignty.
- H2: AI capability positively affects cyber-diplomatic capacity.
- H3: Digital sovereignty positively affects cyber-diplomatic capacity.
- H4: Digital sovereignty positively affects strategic position.

- H5: Foreign technological dependence negatively affects digital sovereignty.
- H6: Foreign technological dependence negatively moderates the AI capability–digital sovereignty relationship.
- H7: Digital sovereignty mediates the relationship between AI capability and cyber-diplomatic capacity.
- H8: Cyber-diplomatic capacity positively affects strategic position.
- H9: AI capability has a positive indirect effect on strategic position through digital sovereignty and cyber-diplomatic capacity.

Conceptual model: AI Capability → Digital Sovereignty → Cyber-Diplomatic Capacity → Strategic Position, with Foreign Technological Dependence moderating the AI Capability → Digital Sovereignty relationship.

9. Methodology

9.1 Research Design and Population

The study uses a quantitative, cross-sectional explanatory design. The unit of analysis is the individual professional or expert with relevant knowledge of AI, information technology, cybersecurity, digital governance, telecommunications, technology policy, international relations, or cyber diplomacy. The target population includes government institutions, universities and research organizations, technology and AI firms, cybersecurity organizations, telecommunications institutions, think tanks, and relevant policy and diplomatic professionals.

9.2 Sampling and Sample Size

Purposive sampling is appropriate because the study requires specialized respondents. Stakeholder quotas may be used to improve representation across government, academia, technology, cybersecurity, policy, and diplomatic groups. Controlled snowball recruitment may supplement access where necessary. Using Cochran's formula with a 95% confidence level, p = .50, q = .50, and a 5% margin of error gives an initial estimate of approximately 384 respondents; the proposed target is approximately 400–450 usable responses. The actual achieved sample and response rate must be inserted from the final dataset.

9.3 Data Collection and Instrument

Data are collected through a structured self-administered questionnaire using a five-point Likert scale from 1 = strongly disagree to 5 = strongly agree. The instrument includes demographic/professional information and multi-item measures of the five principal constructs. Expert review and pilot testing are used to improve clarity, relevance, and contextual appropriateness.

9.4 Measurement of Constructs

- AI Capability: human capital, R&D, computing and digital infrastructure, organizational readiness, data capacity, innovation, and institutional expertise.
- Digital Sovereignty: control of critical infrastructure, data governance, technological autonomy, cybersecurity resilience, domestic capability, regulatory capacity, and independent technology-policy decisions.
- Foreign Technological Dependence: reliance on foreign cloud infrastructure, computing, AI models/platforms, semiconductors, cybersecurity technologies, proprietary software, technical expertise, and externally controlled platforms.
- Cyber-Diplomatic Capacity: technical diplomatic expertise, international negotiations, policy formulation, multilateral engagement, cybersecurity cooperation, technology partnerships, norm development, and diplomatic response to cyber incidents.
- Strategic Position: strategic autonomy, digital influence, bargaining capacity, technological resilience, global governance participation, partnership diversification, and protection of national digital interests.

9.5 Reliability, Validity, and Bias

Internal consistency is assessed using Cronbach's alpha and composite reliability, with values around .70 or higher considered acceptable. Convergent validity is assessed through factor loadings, AVE, and composite reliability; discriminant validity is assessed through HTMT and the Fornell–Larcker criterion. Where necessary, KMO and Bartlett's test support factor analysis. Common method bias is addressed through anonymity, neutral

wording, separation of construct sections, and appropriate statistical diagnostics. Ethical procedures include voluntary participation, confidentiality, secure data handling, and relevant institutional approval.

10. Data Analysis Plan

Data screening includes completeness, eligibility, duplicate-response, and response-quality checks. Descriptive statistics summarize respondent characteristics and construct distributions. PLS-SEM is used to assess the measurement and structural models because the framework contains multiple latent constructs and direct, mediation, and moderation paths. Reliability, validity, collinearity, path coefficients, bootstrapped significance, R^2, f^2, Q^2, mediation, and moderation are assessed as appropriate.

Important note: The source paper contains placeholders rather than actual respondent counts and statistical coefficients. Accordingly, this shortened version does not invent empirical values or hypothesis decisions. Final numerical results must be inserted from the actual SPSS/SmartPLS output.

11. Results and Interpretation Framework

The final results section should report the achieved sample and response rate, respondent profile, descriptive statistics, reliability and validity, correlations, structural paths, R^2, effect sizes, mediation, moderation, predictive relevance, and hypothesis decisions. The central interpretation should test whether AI capability strengthens digital sovereignty, whether digital sovereignty strengthens cyber-diplomatic capacity and strategic position, whether foreign technological dependence constrains sovereignty, and whether digital sovereignty mediates the pathway from AI capability to cyber diplomacy and strategic position.

The expected theoretical pattern is consistent with RDT: domestic technological resources should strengthen autonomy, while concentrated external dependence should reduce strategic flexibility. However, these statements are hypotheses and should be presented as empirical findings only after statistical testing.

12. Discussion

The study's integrated framework positions AI capability as a strategic resource rather than merely an innovation input. Stronger human capital, research capacity, infrastructure, data capability, and institutional expertise can improve Pakistan's ability to govern critical digital resources. Digital sovereignty is therefore understood as functional capacity to exercise meaningful strategic choice under interdependence, not complete technological isolation.

The proposed positive relationship between AI capability and cyber-diplomatic capacity reflects the increasing technical complexity of international digital governance. Diplomats and policymakers require expertise to evaluate technology partnerships, formulate credible positions, participate in negotiations, and contribute to emerging norms. Digital sovereignty may mediate this relationship because technological resources become strategically valuable when embedded in effective institutions, infrastructure, regulation, and cybersecurity.

Foreign technological dependence is expected to weaken these benefits when critical infrastructure, platforms, computing, software, or AI systems remain concentrated among external providers. The key strategic issue is therefore not international cooperation itself but excessive or concentrated dependence that reduces switching options and bargaining power. Cyber diplomacy can bridge domestic technological capability and international influence by translating technical competence into negotiation, partnerships, norm development, and multilateral participation.

13. Theoretical and Practical Implications

Theoretically, the study extends RDT from organizational dependence to state-level digital governance. It identifies AI capability as a strategic resource, digital sovereignty as a mechanism for converting resources into autonomy, and cyber diplomacy as a mechanism for converting technological capacity into international influence. Practically, government agencies, universities, technology firms, and cybersecurity institutions should prioritize AI-skilled human capital, secure data management, domestic research,

institutional AI literacy, cybersecurity, technology-risk assessment, and supplier diversification.

For policy, Pakistan should integrate AI, cybersecurity, data governance, telecommunications, and foreign policy. International technology partnerships should emphasize knowledge transfer, local capacity building, interoperability, and diversification rather than excessive concentration of dependence.

14. Recommendations

- Develop an integrated national AI sovereignty framework linking AI, cybersecurity, data governance, and foreign policy.
- Strengthen advanced AI, cybersecurity, data science, and technology-policy human capital through universities, scholarships, research grants, and industry partnerships.
- Expand secure domestic and regional computing and research infrastructure.
- Conduct strategic technology-dependency audits and reduce critical concentration on single external providers.
- Establish specialized AI and cyber-diplomacy capacity within relevant institutions.
- Strengthen public–private collaboration among government, universities, technology firms, startups, and cybersecurity organizations.
- Diversify international technology partnerships and prioritize joint research and knowledge transfer.
- Increase Pakistan's participation in international AI, cybersecurity, digital-trade, data-governance, and technology-standard negotiations.
- Link AI development with security-by-design, data protection, model security, incident response, and institutional oversight.

15. Limitations and Future Research

The cross-sectional design limits temporal causal inference, while perceptual survey measures may differ from objective indicators of national technological capability. Purposive sampling limits statistical generalizability, and the Pakistan-specific focus restricts direct comparison with other countries. Digital sovereignty is also multidimensional and evolving, while rapid changes in generative AI, infrastructure, regulation, and geopolitics may affect relationships over time.

Future studies should use longitudinal and comparative designs, combine perceptual and objective indicators, examine additional mediators such as cybersecurity resilience and data-governance capacity, test moderators such as regulatory quality and geopolitical alignment, and use qualitative interviews with diplomats, policymakers, cybersecurity specialists, researchers, and technology executives.

16. Conclusion

AI capability has strategic significance for Pakistan because it affects technological sovereignty, cybersecurity resilience, diplomatic capacity, and strategic autonomy. The study's framework proposes that stronger AI capability can enhance digital sovereignty, which can strengthen cyber-diplomatic capacity and strategic position, while foreign technological dependence can constrain these benefits. Pakistan's most viable pathway is not technological isolation but selective domestic capability development combined with diversified international partnerships, stronger cyber diplomacy, resilient infrastructure, effective data governance, and active participation in global AI and cyber governance.

References

Adler-Nissen, R., & Eggeling, K. A. (2024). The discursive struggle for digital sovereignty: Security, economy, rights and the cloud project Gaia-X. JCMS: Journal of Common Market Studies. https://doi.org/10.1111/jcms.13594

Barrinha, A. (2024). Cyber-diplomacy: The emergence of a transient field. The Hague Journal of Diplomacy, 19(3), 439–466. https://doi.org/10.1163/1871191X-BJA10183

Batool, A., Zowghi, D., & Bano, M. (2025). AI governance: A systematic literature review. AI and Ethics, 5, 3265–3279. https://doi.org/10.1007/s43681-024-00653-w

Belli, L. (2023). To get its AI foothold, Brazil needs to apply the key AI sovereignty enablers (KASE). In S. Feldstein (Ed.), New digital dilemmas. Carnegie Endowment for International Peace.

Broeders, D., Cristiano, F., & Kaminska, M. (2023). In search of digital sovereignty and strategic autonomy: Normative power Europe to the test of its geopolitical ambitions. JCMS, 61(5), 1261–1280. https://doi.org/10.1111/jcms.13462

Falkner, G., Heidebrecht, S., Obendiek, A. S., & Seidl, T. (2024). Digital sovereignty—Rhetoric and reality. Journal of European Public Policy, 31(8), 2099–2120. https://doi.org/10.1080/13501763.2024.2358984

Keith, A. J. (2024). Governance of artificial intelligence in Southeast Asia. Global Policy, 15, 937–954. https://doi.org/10.1111/1758-5899.13458

Mokry, S., & Gurol, J. (2024). Competing ambitions regarding the global governance of artificial intelligence: China, the US, and the EU. Global Policy, 15, 955–968. https://doi.org/10.1111/1758-5899.13444

Payne, K. (2024). The geopolitics of AI. RUSI Journal. https://doi.org/10.1080/03071847.2024.2413274

Pfeffer, J., & Salancik, G. R. (1978). The external control of organizations: A resource dependence perspective. Harper & Row.

Roberts, H. (2024). Digital sovereignty and artificial intelligence: A normative approach. Ethics and Information Technology, 26, Article 70. https://doi.org/10.1007/s10676-024-09810-5

Santaniello, M. (2025). Attributes of digital sovereignty: A conceptual framework. Geopolitics, 30, 788–809. https://doi.org/10.1080/14650045.2025.2521548

Sukumaran, A., Broeders, D., & Kello, M. (2024). The pervasive informality of the international cybersecurity regime: Geopolitics, non-state actors and diplomacy. Contemporary Security Policy, 45(1), 7–44. https://doi.org/10.1080/13523260.2023.2296739

Walter, Y. (2024). Managing the race to the moon: Global policy and governance in artificial intelligence regulation. Discover Artificial Intelligence, 4, Article 14. https://doi.org/10.1007/s44163-024-00109-4

Zaidan, E., & Ibrahim, I. A. (2024). AI governance in a complex and rapidly changing regulatory landscape: A global perspective. Humanities and Social Sciences Communications, 11, Article 1121. https://doi.org/10.1057/s41599-024-03560-x

Almeida, P. G. R. de, & Santos Júnior, C. D. dos. (2025). Artificial intelligence governance: Understanding how public organizations implement it. Government Information Quarterly, 42(1), Article 102003. https://doi.org/10.1016/j.giq.2024.102003

Arshad, A., Nadeem, L., & Waqar, M. (2026). Digital diplomacy: Navigating the cyber war in international affairs. Pakistan Languages and Humanities Review, 10(3), 45–56. https://doi.org/10.47205/plhr.2026(10-III)05

Rehman, H. U., & Wadood, A. (2025). Pakistan and the new frontier of cyber diplomacy: Challenges and strategic opportunities. BTTN Journal, 4(1), 103–124. https://doi.org/10.61732/bj.v4i1.175

IEER
Institute for Excellence in Education & Research