



Review Article

AI, Blockchain, and the New Geopolitical Order How Digital Sovereignty is Reshaping Global Power Politics

Dr. Syed Rizwan Haider Bukhari 

Department of Political Science, Islamia College University Peshawar, Khyber Pakhtunkhwa, Pakistan.

***Correspondence**Dr. Syed Rizwan Haider Bukhari
Email: bukharipalmist@gmail.com**Article History**

Received: March 12, 2026

Accepted: August 28, 2026

Published: September 17, 2026

CitationBukhari, S. R. H. (2026). AI, Blockchain, and the New Geopolitical Order How Digital Sovereignty is Reshaping Global Power Politics. *International Social Research Nexus (ISRN)*, 2(3), 1-10.
<https://doi.org/10.63539/isrn.2026021>**Copyright**© 2026 The Author (s). Published by Scholar Cave. This is an open access article distributed under the terms of the [Creative Commons Attribution 4.0 International License](#).

Abstract

Today, artificial intelligence (AI), distributed-ledger technologies and their related infrastructures are becoming a major part of geopolitical competition. This conceptual and analytical investigation explores the transformation of current notions of sovereignty and state power through control of data, advanced computing, semiconductors, cloud infrastructure, digital platforms, technical standards, and payment systems. A structured qualitative documentary analysis of peer-reviewed scholarship and authoritative policy documents from 2017 to July 2026 was conducted. It puts to work three lenses of analysis: techno-realism, whereby technological capability is becoming a more central element in national power; neo-structuralist/dependency analysis, which highlights asymmetries in technological production and position of networks; and a cyber-geopolitical approach, which analyzes digital infrastructure and data governance as strategic spaces contested between various actors. The analysis suggests that digital sovereignty is most effectively defined by the ability not to be technologically autonomous, but to be able to select policy choices independently while acknowledging and dealing with inextricable inter-dependencies. This change can be seen in the United States-China technology competition, where industrial policy and semiconductor restrictions play a role, as well as in differing methods of cultivating home-grown capabilities and in the digital and data governance policies of the two countries. Blockchain, on the other hand, has not had a single political effect that is felt across the public sector: the experience of public sector suggests that the effect of blockchain is contingent on institutional design and governance. The problem is thus not lack of policies but the implementation capacity in developing countries like Pakistan. While there is a National Cyber Security Policy, a Digital Nation framework, and a national AI policy approved, there is need for greater coordination, competencies, institutional capacity, and risk-based technology governance in Pakistan. The article ends with a conclusion that in the digital age geopolitical influence is more about being able to control strategic technological dependencies and not only about having the digital technologies.

Keywords

Artificial Intelligence, Blockchain, Digital Sovereignty, Geopolitics, Technological Dependency, Cyber Governance, Pakistan.

1. Introduction

The role of technological capability has been significant in international power since the beginning but the digital economy has changed the way and the pace at which power is exerted. The data, advanced computing, semiconductors, cloud services, digital platforms, cybersecurity, technical standards and digitally-mediated finance are now strategic assets as well as commercial inputs. It is not to say that military force, land, industry or natural resources are no longer significant in themselves. Instead, the traditional sources of power are increasingly organized, protected and projected in the context of digital technologies. Rather than being merely an introduction of digital tools to replace physical ones, it is therefore more appropriate to think about contemporary geopolitics as a dialogue between material powers and digitally mediated capabilities (Horowitz, 2018; Farrell & Newman, 2019). Digital sovereignty is a new notion resulting from this change. While there are different definitions, it typically involves the ability of political communities to have meaningful control and choice over data, digital infrastructure, technological standards and critical digital services (Pohle & Thiel, 2020; Santaniello, 2026). The concept of digital sovereignty does not mean full technological independence. Even the biggest of states is highly dependent on modern digital systems, which are deeply interconnected, it is true, and even its own expertise, cloud infrastructure, foreign intellectual property and transnational supply chains are inevitably present. What is the question to ask then is whether dependency can be controlled while not making it unduly vulnerable or outside leverage?

The digital power concentration offers good empirical grounds to consider the issues as geopolitical. The UNCTAD also noted that the value and influence of digital platforms are also highly concentrated in the hands of two countries, the United States and China, who had approximately 90% of the world's largest digital platforms combined, illustrating the highly uneven distribution of value and influence in the "data-driven economy" (UNCTAD, 2021). Meanwhile, the Government's approach is becoming more intrusive. The United States has applied industrial subsidies and export controls to advanced computing and semiconductor manufacturing technologies, while China's national AI strategy explicitly views AI as a strategic technology, and has long-term industrial-development goals (Congressional Research Service [CRS] 2023; State Council of the People's Republic of China [PRC] 2017; U.S. Department of Commerce, Bureau of Industry and Security [BIS] 2022, 2024). The second layer to this debate is blockchain and distributed-ledger technologies, which make the assumption of centralization and state authority more complicated. History of blockchain describes a mechanism that by itself is supposed to be decentralizing, but that isn't always the case in public sector. According to the Organisation for Economic Co-operation and Development (OECD) a majority of government blockchain projects were still in a pilot phase, and results were largely dependent on aspects of governance, institutional fit, and project implementation capacity, as well as the blockchain technology itself (Lindman et al., 2020). Similarly, central bank digital currencies (CBDC) are an example of the increasing strategic significance of digital money, but are not the only architecture or legal design the central banks are considering; they are thinking about various approaches. The BIS survey of 2023 showed that 94% of the central banks that responded were in some stage of exploration of a CBDC (Di Iorio et al., 2024).

These are particularly significant developments for the developing states. While digital technologies can help the public sector modernize, enable financial inclusion, education, health, productivity, they can also increase reliance on foreign cloud providers, software ecosystems, platforms, standards, and technical expertise. In this context, Pakistan is a valuable case study to examine the digital modernization of a developing nation without the enigma of isolation of sovereignty. Importantly, the policy landscape has been changing with the introduction of a National Cyber Security Policy (2021) and the enactment of the Digital Nation Pakistan Act (2025) and the federal cabinet approval of an Artificial Intelligence Policy (2025) (Ministry of Information Technology and Telecommunication [MoITT] 2021, 2025; National Assembly of Pakistan 2025). It is then not a lack of policy, but the coherence, capacity and strategic prioritization of current policy. This article has three questions. How does AI, blockchain and digital infrastructure change the technology - geopolitical power linkage? Second, what is the role of techno-realism, structural-dependency analysis and cyber-geopolitical analysis in the analysis of various aspects of this change? Thirdly, what are the policy implications for the developing countries in general and Pakistan in particular? The article aims at replacing the language of a 'digital revolution' with a more nuanced description of technological capability, interdependence and sovereignty through answering these questions.

2. Literature Review

2.1. Technology as a Source and Instrument of Geopolitical Power

In recent years, the scholarship on technology and international politics has started to view AI as a general-purpose or enabling technology, the geopolitical impact of which hinges on organizational uptake, complementarity, and state capacity. AI, for instance, is better thought of as an enabling technology, not just a weapon or a single platform, [Horowitz \(2018\)](#) argues. The difference is significant because it takes attention off of techno determinism. Having algorithms is not enough for states to have a strategic advantage, they need compute, data, skilled staff, institutional processes, capital and the ability to integrate AI into the economies and governments. Techno-realism is one of the theories that can be used to explain this relationship. The work of [Sukma \(2024\)](#) is a move in the direction of techno-realism, which emerged from realist tradition, and brings technology into the political power analysis more to the center. When deployed responsibly, the approach can be used to outline how those considered as parts of national capability – like AI, semiconductors, cloud capacity, cyber resilience and digital standards – are becoming a part of that. This article does not, however, presume that technology itself is responsible for results. Technological resources are important via institutions, networks, political decisions and through access to complementary capabilities.

2.2. Digital Sovereignty, Network Power, and Strategic Interdependence

The second strand of literature is on digital sovereignty and strategic implications of interdependence. In [Pohle and Thiel \(2020\)](#) digital sovereignty has developed into a comprehensive political concept that includes the ability to act, autonomy and control in digital spaces. By adding to this definition, [Santaniello \(2026\)](#) extends the concept of digital sovereignty beyond territorial aspects to a multidimensional one. These methods have proven to be helpful, especially in recognizing the desire of states to be more autonomous, yet not necessarily separate from global networks. [Farrell and Newman \(2019\)](#) propose a structural explanation for leveraging political power in certain network positions in the form of “weaponized interdependence.” They have developed the key concept that the global networks are not necessarily symmetrical: actors at the heart of the network can be placed at an informational or exclusionary advantage. This can be taken to the cloud, payment, semiconductors, platform ecosystems and standards in the digital economy. This article, therefore, employs a neo-structuralist/dependency approach to explore the social dynamics of the reproduction of asymmetries between advanced and developing economies, as a consequence of the unequal technological capabilities and the unequal network positions. Here the term is not intended to suggest that one, universally adopted ‘neo-structuralist theory of technology’ exists, but rather as an analysis to be used as a lens.

2.3. Cyber-Geopolitics and Infrastructure as Strategic Space

A third literature considers cyberspace and the digital infrastructure as geopolitical spaces. The pertinent geography isn't just virtual. The data center, fiber-optic cables, semiconductor manufacturing, satellite systems, cloud regions, software ecosystems and standards bodies all have real-world geographical, hierarchical and ownership effects. Cyber-geopolitical analysis thus questions who has control over critical digital infrastructures, what are the legal regimes and how data flows between borders, as well as what the technological dependency means for national autonomy. This is done intentionally as ‘cyber-geopolitical lens’ is not meant to denote a singular Cyber Geopolitics theory and is known by many names. This view is also an explanation for why the concept of Data Governance is up for grabs at this moment in time. [UNCTAD \(2021\)](#) documents a variety of divergent attitudes towards cross-border data governance and points out that unequal digital capacities can contribute to growing development disparities. The push for technological sovereignty in Europe also prioritizes resilience, capabilities, and minimizing unnecessary strategic reliance over closure of the economies ([European Parliament, 2021](#)). The literature thus reaches a single conclusion: in the digital age, sovereignty has more and more come to take the form of the management of dependencies within a multi-layer technological system.

2.4. Blockchain, Public Authority, and Digital Finance

While blockchain is often cited as a technology that is decentralizing the authority, it's not that simple in practice. [Lindman et al. \(2020\)](#) demonstrate how the progress of government applications has been impeded by limited pilots, and that there are key institutional design, public value, interoperability, and governance considerations. Despite the fact that the technology that ledger was created with are decentralized systems, it can be used to strengthen administrative coordination because of a permissioned or state-administered ledger. State authority, however, is not necessarily supplanted by a public blockchain as the access, taxation, identity and enforcement remain reliant on institutions. The concept of the CBDC also needs some clarity. Digital sovereign currency could be based on the distributed-ledger technology but does not necessarily need to be blockchain. The survey evidence from the BIS indicates that the central banks are experimenting with CBDCs, particularly in the wholesale segment, and are taking note of the variety of design choices they can make,

rather than a particular technical approach (Di Iorio et al., 2024). Blockchain thus needs to be seen as one potential form of governance, rather than a definitive description of the future of money and/or the state.

2.5. Developing Countries and Pakistan

The literature emphasizes, for developing states, a double challenge. Digital technologies have the potential to foster the development of state capacities and economic modernization, and reliance on imported platforms, cloud services, proprietary software and foreign expertise can limit policy autonomy. This tension is especially significant as openness is a prerequisite for being able to participate in the digital economy, but concentration can lead to dependency if not managed. Strategies based on capability building, diversification, standards, procurement policy and institutional learning, therefore, are viable options than technological isolation. The Pakistan policy landscape is not devoid of regulations, as has been often described, it is much more complex. The National Cyber Security Policy 2021 sets the framework of a national policy on cyber security, the Digital Nation Pakistan Act 2025 gives a statutory mandate to the digital transformation and the federal cabinet approved the Artificial Intelligence Policy 2025, organized on six key pillars and explicitly emphasizing on the responsible, inclusive, and innovative use of AI (MoITT, 2021, 2025; National Assembly of Pakistan, 2025). The two developments move the research question, not from Pakistan's Digital Policy to the question of what Pakistan's policies are mutually reinforcing, institutionally implementable and have a strong link with geopolitical risk management.

3. Methodology

In the conceptual and analytical review design with qualitative analysis of secondary data, this article uses a qualitative method. The methodology of the revised study is structured and documentary to improve its transparency, consistency and verifiability. The evidence-based material is sourced from three main types: peer-reviewed scholarship on topics of AI, Digital sovereignty, International political economy, blockchain governance and technology-related power generated from authoritative reports published by multilateral institutions including UNCTAD, OECD and BIS, as well as primary policy and legal documents from the United States, China, European Union and Pakistan. The primary analysis time frame is from 2017 until July 2026, when the national AI strategies of various countries, semiconductor policies, digital-sovereignty discussions, and digital-government projects have grown more evident in international political and policy discussions. Some of the earlier studies were retained because they offer important theoretical foundations for discussing current developments or serve as historical background for the understanding of developments today.

Sources were selected when they showed a clear relevance to at least one of the key concepts in the study, a clear institutional and/or authorial provenance, a publication status, and were accompanied by adequate bibliographic information so that they could be independently verified. The revised evidence base was not based on materials that could not be authenticated, nor did duplicated sources and commentaries with incomplete publication details appear in it. This process was designed to enhance the quality of the review by minimizing reliance on unpublished or hard to verify material, especially material from 2026, as well as to reduce the self-citation and extend the argument in support of the review to a wider and more self-evidently verifiable pool of scholarship.

The analytical process was carried out in two stages which were connected with each other. The first step was to analyse the literature and policy documents thematically and group them into five areas that are common across the selected documents: technological capability, digital infrastructure and data governance, strategic interdependence, blockchain and digital finance, and policy capacity of developing countries. Secondly, the themes that emerged were analysed from three different complementary theoretical perspectives. Techno-realism was used to analyse how technological capacity can be transformed to strategic and geopolitical power. The neo-structuralism and dependency approach was adopted for an analysis of the asymmetries caused by the differential access to technological production, digital infrastructure, supply chains and critical network nodes. A cyber-geopolitical view was used to gain insights into the way in which cyberspace, data flows, digital standards, communication networks and technological infrastructures are becoming strategic competitive spaces. They are therefore employed in combination in order to offer analytical triangulation more than as if they were alternative theoretical approaches.

The study is a conceptual study and thus does not create an original empirical data set or use an experimental design or statistical testing. Selective reporting of quantitative information is included to support conceptual claims, when it is reported by an authoritative and independently verifiable source. The analysis is not intended to quantify causal relationships, but rather to synthesize the available evidence, understand new patterns in the dynamics between technology

and geopolitical power, and provide policy-relevant conclusions and insights on digital sovereignty, strategic competition, and the role of developing countries in the changing global technological landscape.

4. Thematic Findings and Analysis

4.1. *Techno-Realism: Technological Capability is Becoming a Component of National Power*

The first is that geopolitical competition is now more about development, funding, access to and management of critical technologies. The techno-realism provides an explanation for the increasing shift of the states towards a strategic approach to advanced computing, semiconductors, AI research, cybersecurity and digital infrastructure as strategic sectors, and not just commercial sectors. This is reflected in the United States' CHIPS and Science Act. This bill provided \$52.7 billion to the semiconductor manufacturing, research and development, workforce development and international technology-security efforts (CRS, 2023). A clear and direct industrial policy for strengthening supply chain resiliency and strategic capability. The policy course of China also exhibits a parallel course of capability building. In 2017, the New Generation Artificial Intelligence Development Plan was issued by the State Council, which established AI as a strategic technology and aims to develop a base of the AI industry with an economic value of around RMB 1 trillion by 2030 (State Council of the People's Republic of China, 2017). The significance of these targets is less in the actual attainment of each of the quantitative targets, than in the approach of the State to AI as a tool for economic upgrading, innovation and national competitiveness. That's not the 'techno-realist' reading in which 'AI' becomes geopolitically dominant automatically. Instead, states turn to AI because it has the potential to magnify levels of productivity, information handling, public administration, security capacity, and innovation when paired with compute, data, capital and institutions. The entire technological ecosystem is to be considered, the algorithm itself is not.

4.2. *Cyber-Geopolitical Lens: Infrastructure, Data, and Standards are Arenas of Strategic competition*

The second discovery is that digital infrastructure has turned into an area in which states try to lessen their vulnerability and influence others' decisions. A specific example is the U.S. export-control policy with regard to advanced computing and semiconductor manufacturing. In October 2022, the U.S. Bureau of Industry and Security (BIS) imposed restrictions on the People's Republic of China (PRC) to limit the PRC's access to certain advanced computing and semiconductor-manufacturing technologies, which were then further tightened and enhanced (BIS, 2022, 2024). The measures are indicative of the fact that technological supply chains can be used as a tool of economic statecraft when interpreted by a government from a national security perspective. The process here helps to foster so what can be called "selective technological fragmentation. Does not imply a full decoupling of global digital economy into distinct blocks, as companies, research communities, standards organizations and supply chains continue to interdepend. But the strategic borders on technologies are tighter with export control, investment screening, data-localization laws, procurement laws, and domestic subsidy schemes. Digital sovereignty is thus more and more achieved by means of de-risking and diversification instead of complete separation. Those worries are further compounded with the power centralization in the platform. Countries outside these centers might be concerned about dependence on externally-controlled ecosystems, as, for example, UNCTAD has found that about 90% of the world's largest digital platforms have a market capitalization of the United States and China. The cyber-geopolitical prism now points to the location of infrastructure, the standards, the jurisdiction and the ownership of the content that circulates through the network, rather than just to the content itself.

4.3. *Neo-Structuralist/Dependency Lens: Technological Asymmetry Can Reproduce Structural Inequality*

The third finding is that with digital transformation comes an unequal set of benefits. The combination of these factors creates a superior environment in advanced economies and major technology powerhouses that is responsible for advanced economies' high-tech output. These factors are responsible for the high-tech output at advanced economies and the major technology powers, which are characterized by high density of research ecosystems, capital markets, semiconductor capabilities, hyper scale cloud infrastructure and influential platform firms. Most of the time, developing countries become involved in these systems as consumer countries of foreign technologies. This does not mean there is a necessity to dependence, but it can limit the policy options when essential services are dependent on a few external suppliers, or when the domestic institutions are incapable of assessing, procurement, regulation and adaptation of technology. In this way, the network perspective of Farrell and Newman (2019) can help explain the political salience of dependence that has been brought about by the centralization of control. One of the features of a developing country is that it can be well connected to the global world of digital networks yet have little negotiation over the standard, infrastructure or price that determines how it is connected. A neo-structuralism analysis thus moves the focus away from access to technology to focus on the distribution of productive capacity, ownership, knowledge and power over rule-setting. This approach also helps to avoid a "nationalistic approach" to sovereignty. Most states are economically unable to be self-sufficient in

each technological layer. The more viable goal is strategic optionality, which could be achieved by diversifying suppliers, retaining key domestic capabilities, being able to negotiate from a stronger position and retaining legal and institutional control over key digital functions.

4.4. Blockchain: Political Effects Depend On Governance Design

The fourth conclusion is that blockchain does not have a geopolitical influence. The diversity of the different applications in the public sector does not justify the claim that it has to weaken the state. There are government projects that have considered the use of distributed ledgers to register, identify, store and manage records and administrative processes, although OECD's review highlights that few projects have gone beyond experimentation and that public value is contingent on institutional contexts (Lindman et al., 2020). In some contexts, then, the technology can facilitate a decentralized approach while in other contexts it can help to consolidate administrative coordination. The same is applicable in the case of digital currency. These are the results of the growing pace at which CBDC research is taking place, reflecting state's and central bank's interest in digital monetary infrastructure. However, the 94% statistic from BIS is only for central banks exploring the creation of a CBDC and not financial institutions that are adopting blockchain-based national currencies (Di Iorio et al., 2024). To view CBDC and blockchain as synonymous would thus overestimate the importance of blockchain. The more geopolitically sound takeaway from the situation is that states are trying to work out new payment-sovereignty, monetary-tech, and monetary-architectural strategies to address changes in payments, financial tech, and monetary sovereignty.

4.5. Pakistan: The Key Issue Is Policy Implementation and Strategic Coordination

The fifth finding is that Pakistan should not be termed as having no national digital-policy frameworks anymore. The state has laid a strong strategic and institutional ground (National Cyber Security Policy 2021, Digital Nation Pakistan Act 2025 and approved Artificial Intelligence Policy 2025) (MoITT, 2025, 2021; National Assembly of Pakistan, 2025). This is a major shift from the previous time when policy fragmentation could be considered a more basic gap. The next challenge is to get it up and running across institutions. Digital sovereignty is not just about policy documents, it needs to be backed by the skills of public servants, the interoperability of data systems, the capacity for cybersecurity, transparency during procurement, a sense of ownership and institutional responsibility, a domestic research capability, and the capacity to evaluate external dependencies. The strategic role of Pakistan hinges on the ability to coordinate the current policies in a way that they can be executed with measurable objectives instead of creating them as individual technology projects. The other implication is about diversification. While sovereignty is an imperative, Pakistan needs to understand that it has technology partnerships with the world and shouldn't shy away from global technology ecosystems. A more resilient approach would have been to avoid single-source, single-jurisdictional, single-technology dependency, as well as reliance on international markets, research networks, and investment. Digital sovereignty is open when combined with the risk assessment and strategic choice, in this sense.

5. Discussion

Taken together, the analysis indicates that the use of AI, blockchain, and digital infrastructure is transforming geopolitical competition, but in a not-so-deterministic way as early tech narratives have suggested. The new order will not be just a one in which the most advanced country in AI becomes the most powerful. Power is spread out over a tiered set of activities from semiconductor manufacturing, compute, data, cloud infrastructure, cloud platforms and cloud standards, skilled workers, finance, law and institutional capacity. Political activities aimed at managing these layers so as to keep in place strategic choice are referred to as digital sovereignty.

Analytical lens	Primary mechanism	Evidence emphasized	Interpretive contribution
Techno-realism	Technology as a component of state capability and competition	AI strategies, semiconductor industrial policy, capability-building	Explains why governments increasingly treat digital technologies as strategic assets rather than ordinary commercial goods.
Neo-structuralist/dependency lens	Unequal control of production, expertise, platforms, and network nodes	Concentration of digital platforms, supply-chain dependence, asymmetric network power	Explains how technological interdependence can reproduce hierarchy and constrain developing-state policy autonomy.

Cyber-geopolitical lens	Control over digital infrastructure, data, standards, and jurisdiction	Export controls, data governance, infrastructure ownership, digital-sovereignty policy	Explains why cyberspace has territorial, legal, and infrastructural dimensions that generate geopolitical competition.
-------------------------	--	--	--

The three lenses are complementary as they are working on different levels. Techno-realism is about the incentives for increasing technological capability of the state. Structural analysis can help to understand how that capability is distributed unequally and how interdependence can lead to leverage. Infrastructure and jurisdictions of that leverage are revealed in cyber-geopolitical analysis. It's not that these traditions are interchangeable, the theoretical contribution of the paper is to demonstrate that each of them illuminates a different aspect of the same digital-power structure.

Indeed, this synthesis demands a more nuanced understanding of U.S.-China competition. It is a true competition that is becoming more institutionalised through industrial policy, controls, standards and local capacity development. But it would be too early to say that the world digital economy is now split into two-third countries have agency, and there is interdependence. A more apt description is that of competitive interdependence, with states trying to decrease specific vulnerabilities whilst maintaining access to the benefits of global technology networks.

Policy implication for Pakistan and other developing countries is thus, not to emulate the magnitude of U.S. and Chinese industrial policies. The relevant objective is to understand the critical technological dependency, strengthen technology capacities at home in places where they offer strategic advantage, diversify external technology relationships and establish institutions to govern technology procurement and use. Digital sovereignty should be considered successful if it is resilient, resilient to policy, provides trusted public services and can shift suppliers or technological pathways when needed.

6. Policy Recommendations

It is recommended to focus on the implementation and institutionalization of the current national policy frameworks in Pakistan to best effect rather than developing new policy documents that may be duplicated or overlap with existing policy. The Artificial Intelligence Policy 2025, the Digital Nation Pakistan Act 2025, National Cyber Security Policy 2021 should be given special attention. They should be accompanied by clearly defined institutional mandates, realistic timelines, coordination mechanisms and measurable performance indicators. A unified implementation framework would lessen the fragmentation among government departments and agencies, and provide a harmonized approach to digital transformation, AI governance, cybersecurity and national technology policy.

Meanwhile, Pakistan must carry out a detailed national analysis of critical technologies to measure its reliance on these technologies. The exercise should be used to identify dependencies between the various cloud services, data hosting, semiconductor and computing fabric, digital identity providers, payment systems, cybersecurity services and key software. The goal should be to ensure that the dependence is not a routine one of trade (which may be acceptable within an interdependent global economy) but dependency which could lead to strategic weaknesses. Such an assessment would give the policymakers a more solid foundation on which to make decisions regarding the need for domestic capacity, diversification, redundancy or regulatory protection.

There also needs to be an increase in the interoperability of public digital infrastructure, which must be an integral part of national digital policies. Instead of building individual technological projects in various institutions, there is need to promote the use of common technical standards, establish processes for data exchange, establish institutional accountability, and ensure effective institutional auditing processes. Similarly, in the public sector, there must be governance framework rules for the use of AI, pertaining to data quality, transparency, security, accountability and oversight. Enhanced interoperability between government systems would benefit not only in terms of administrative efficiencies, but also be a step towards minimizing duplication and enhancing the resilience of the national digital infrastructure.

Public procurement can have a significant part to play in technological resilience and minimizing unnecessary dependency. Thus, interoperability, data and system portability, cyber security assurance, long-term maintainability and protection against unwarranted vendor lock-in must be addressed in government procurement policies. These measures should not be used to limit legitimate international competition but instead need to be implemented in ways that do not unnecessarily limit the policy options available in the future. So strategic procurement can be used for both economic and

national-security purposes: it can ensure flexibility and at the same time incentivize suppliers to adhere to increasingly high governance and security standards.

Pakistan's ability to build a human resource and research capacity at home is also going to play a huge role in the long term digital sovereignty. New strategic collaboration and partnership opportunities between universities, public institutions, research centers and private industry should be created in areas like Artificial Intelligence, cybersecurity, data governance, cloud engineering, semiconductor related skills and technology policy. Investing in the creation of technical users of imported systems is not sufficient. It should also be able to assess, audit, modify and adapt external technology as per the institutional and security needs of the country. If such expertise can be developed, then Pakistan may be able to join the technological web of the world more effectively and minimize the risk of passive technological dependence.

Blockchain policy needs to shift from a technology-driven approach to a strong use-case approach, too. Distributed-ledger systems should be deployed only where there is clear added value for the user over the use of traditional databases or current digital systems. Potential blockchain applications should be measured and evaluated with respect to the governance model, data privacy issues, interoperability, financial and operational requirements, cybersecurity requirements, and accountability mechanisms before they're implemented. This would help curb the drive to adopt blockchain simply because it is new technology, and make sure that public sector use is based on real economic or administrative gains.

Pakistan needs to diversify its international technology partnerships and ensure strategic flexibility. The over-dependence on one technology vendor or country or geopolitical region could introduce vulnerabilities to technical standards, cybersecurity, software, cloud and infrastructure. Having several partners and technological ecosystems would enable the country to benefit from foreign experience and investment along with having more policy sovereignty. Therefore, diversification is not to be interpreted as technological isolation, but as a more strategic way to deal with external dependency.

Lastly, there should be a better engagement by Pakistan in regional and multilateral platforms related to digital governance. New international regulations on artificial intelligence, trans border data transfers, digital trade, technical standards and cybersecurity will be a growing influence on developing countries' opportunities and limitations. If Pakistan had been active in these forums, it would have been able to play a role in formulating such rules instead of just adapting to rules which are made elsewhere. Diplomatic action also needs to be more effective in the global digital governance arena, to ensure that the concerns of developing countries are represented in the new international technological reality, such as, for instance, capacity constraints, equitable access to technology, policy autonomy, and digital inclusion.

7. Limitations

The following are some limitations that should be taken into account when evaluating the arguments and conclusion(s) of this study. Firstly, the article is not a systematic review or an original empirical investigation. The results it provides are, therefore, contingent upon the quality, relevance, and scope of the secondary literature, policy documents and institutional sources incorporated in the analysis. While an attempt was made to include the most reliable and authoritative sources, the study does not purport to be comprehensive in its coverage of all of the scholarship and policy developments in AI, blockchain, digital sovereignty, and geopolitical competition. Secondly, the policy context of new technologies is very fluid. The regulatory frameworks of key economies in areas such as AI and semiconductors, cybersecurity, data governance and digital infrastructure are still in a state of dynamic evolution. Therefore, the policy instruments, institutional arrangements or strategic priorities mentioned in this article may have been altered since the end of the reviewed period. This constraint is especially relevant in places where Governments constantly adapt their technology limitations, industrial policies and other regulations to new developments in technology and geopolitics. Thirdly, three different analytic lenses from different theoretical backgrounds are used in the study. No attempt is made to synthesize and integrate techno-realism, neo-structural and dependency-oriented approaches and the cyber-geopolitical analysis into one coherent theoretical model. This method enables the study to investigate various aspects of technological power, structural inequality and strategic rivalry, but can also restrict the number of degrees of theoretical integration that can be accomplished. The framework should thus be considered more as an analytical tool than as a complete theory of digital geopolitics. Last, the focus on Pakistan is national strategic/policy-level. The performance of implementation of individual ministries, provincial governments, regulatory bodies, technology companies, universities, and specific public-sector digital programs are not systematically evaluated. The analysis, therefore, does not quantify the level of implementation of the

current national policies in terms of their operational impacts. Comparative case studies, indicators based on implementation process, institutional assessments, and interviews with policy makers, regulators, researchers, industry and other stakeholders can further contribute to this area for future studies.

8. Conclusion

The material, institutional and strategic underpinnings of geopolitical power are being transformed by artificial intelligence, blockchain and digital infrastructure. The increased importance does not mean that digital technologies have replaced other traditional national strengths like military power, economic assets, industrial power, or control of territory. Instead, new forms of the organization, protection, and projection of such conventional power are increasingly shaped by technological systems. Economic productivity, information control, public administration, strategic industries, military preparedness and the resilience of critical national systems are now impacted by artificial intelligence, advanced computing, data infrastructure, cyber and digital platforms. The semiconductor policies and advanced-computing restrictions, industrial incentives, domestic technological capacity, and data governance are all now inextricably linked with geopolitical strategy, as demonstrated by the intensifying technological competition from the United States and China. The analysis also shows that geopolitical influence is not a by-product of technology and is not independent of its institutional and political context. The strategic value of AI comes with ecosystems that involve computing power, qualified human resources, quality data, research institutes, investment, regulatory power and governance. Blockchain also does not necessarily have a pro-sovereignty, anti-state or decentralising agenda. Political impacts are dependent on its system architecture, institutional control, regulation design and usage. Digital sovereignty shouldn't be seen as a type of technological isolation or as total national self-sufficiency. A more practical one would be the ability of States to take autonomous and meaningful decisions on key digital infrastructure, data, technological standards and strategic dependencies, but still be plugged in to international markets, technological networks and cooperative institutions. The main challenge for developing countries like Pakistan, however, is the transition of the formulation of digital strategies into their implementation. Pakistan already has several key cornerstones in place with its cybersecurity policies, digital transformation policies, and an artificial-intelligence policy. Engaging in these formal commitments must be followed by institutionalization of these capabilities in the long term through coordinated governance, investment in human resources and applied research, stable and interoperable infrastructure, diversified technological cooperation, better information management (data governance), and evidence-based public procurement. Particular care needs to be taken to examine whether there are specific areas of international technological dependence where there are real strategic vulnerabilities, rather than assuming that all international technological dependence is problematic. At a more general level, the new geopolitical landscape will surely have a positive effect on states that will be able to control technological interdependence without compromising their strategic flexibility. The key question will not only be which countries have the most digital technologies, but which will be able to effectively govern them, secure critical systems, build domestic capacities, reduce foreign reliance and influence global standards and institutions which define the digital world. So, in this context, digital sovereignty is becoming more of a strategic decision, institutional capability, and resilience. States that can continue to develop such capacities as they engage in productive international technological networks will be in a stronger position to protect national autonomy and be able to influence the global digital order.

Declarations

Funding

This research received no specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest

The author declares no conflict of interest related to this research work.

Competing Interest

The author declares no competing interests.

References

- Congressional Research Service. (2023). Frequently asked questions: CHIPS Act of 2022 provisions and implementation (R47523). *Library of Congress*. <https://www.congress.gov/crs-product/R47523>.
- Di Iorio, A., Kosse, A., & Mattei, I. (2024). Embracing diversity, advancing together: Results of the 2023 BIS survey on central bank digital currencies and crypto (BIS Papers No. 147). *Bank for International Settlements*. <https://www.bis.org/publ/bppdf/bispap147.htm>.
- European Parliament. (2021). Key enabling technologies for Europe's technological sovereignty. *European Parliamentary Research Service*. [https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU\(2021\)697184](https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)697184).
- Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, 44(1), 42–79.
- Horowitz, M. C. (2018). Artificial intelligence, international competition, and the balance of power. *Texas National Security Review*, 1(3), 36–57.
- Lindman, J., Berryhill, J., Welby, B., & Piccinin-Barbieri, M. (2020). The uncertain promise of blockchain for government (OECD Working Papers on Public Governance No. 43). *OECD Publishing*. <https://doi.org/10.1787/d031cd67-en>.
- Ministry of Information Technology and Telecommunication, Government of Pakistan. (2021). *National Cyber Security Policy 2021*. <https://moitt.gov.pk/Detail/ZTA5MTI4ZWUtMzdhMS00ZDRhLWE0YmUtZjJjNTZhYTdjNzdl>.
- Ministry of Information Technology and Telecommunication, Government of Pakistan. (2025). *Artificial Intelligence Policy 2025: Federal Cabinet approval*. <https://moitt.gov.pk/SliderDetail/NWlyMzEwYzk-tYTIwYy00ZTk0LWI5ODUtYjg5NjZmYTtyMTg2>.
- National Assembly of Pakistan. (2025). *Digital Nation Pakistan Act, 2025 (Act No. 1 of 2025)*. <https://www.na.gov.pk/en/acts-tenure.php>.
- Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4). <https://doi.org/10.14763/2020.4.1532>.
- Santaniello, M. (2026). Attributes of digital sovereignty: A conceptual framework. *Geopolitics*, 31(2), 788–809. <https://doi.org/10.1080/14650045.2025.2521548>.
- State Council of the People's Republic of China. (2017). *New Generation Artificial Intelligence Development Plan (State Council Document No. 35)*. <https://app.www.gov.cn/govdata/gov/201707/20/408540/article.html>.
- Sukma, I. M. (2024). Techno-realism: Navigating new challenges in the contemporary role of technology in politics. *Security and Defence Quarterly*, 46(2), 24–46. <https://doi.org/10.35467/sdq/188303>.
- United Nations Conference on Trade and Development. (2021). Digital economy report 2021: Cross-border data flows and development—For whom the data flow. *United Nations*. <https://unctad.org/publication/digital-economy-report-2021>.
- U.S. Department of Commerce, Bureau of Industry and Security. (2022, October 7). *Commerce implements new export controls on advanced computing and semiconductor manufacturing items to the People's Republic of China*. <https://www.bis.gov/press-release/commerce-implements-new-export-controls-advanced-computing-semiconductor-manufacturing-items-peoples>.
- U.S. Department of Commerce, Bureau of Industry and Security. (2024, December 2). *Commerce strengthens export controls to restrict China's capability to produce advanced semiconductors for military applications*. <https://www.bis.gov/press-release/commerce-strengthens-export-controls-restrict-chinas-capability-produce-advanced-semiconductors-military>.