P-ISSN 2708-6453	Pakistan Languages and Humanities Review	March-April 2026, Vol. 10, No. 2
O-ISSN 2708-6461	https://doi.org/10.47205/plhr.2026(10-II)16	[194-204]

Pakistan Languages and Humanities Review
www.plhr.org.pk

RESEARCH PAPER

Pakistan's Pursuit of Cyber Sovereignty: Digital Governance, National Security, and Emerging Challenges

[1]Bisma Seerat, [2]Zainab Asif and Atiqa Iqbal

1. MS Scholar, Department of Politics & International Relations, GC Women university Sialkot Punjab, Pakistan
2. MS Scholar, Department of Politics & International Relations, GC Women university Sialkot Punjab, Pakistan
3. MS Scholar, Department of Politics & International Relations, GC Women university Sialkot Punjab, Pakistan

***Corresponding Author** | Bismaseerat356@gmail.com

ABSTRACT

The rapid expansion of cyberspace has transformed traditional concepts of state sovereignty, giving rise to the notion of cyber sovereignty, whereby states seek to regulate, secure, and govern their digital domains. This study examines Pakistan's pursuit of cyber sovereignty and evaluates the institutional, legal, and strategic measures adopted to strengthen digital governance and cybersecurity. Employing a qualitative research design based on secondary sources, the study explores the roles of key institutions, including the Ministry of Information Technology and Telecommunication (MoITT), the Pakistan Telecommunication Authority (PTA), and the Prevention of Electronic Crimes Act (PECA) 2016, in shaping Pakistan's cyber governance framework. The paper further analyzes the relationship between cyber sovereignty, national security, and digital transformation within the broader context of global cyber politics. Findings indicate that Pakistan has made notable progress in expanding digital infrastructure, strengthening cybersecurity institutions, and enhancing regulatory mechanisms to protect digital assets and citizens' data. However, challenges such as technological dependence on foreign platforms, limited cybersecurity capacity, shortages of skilled professionals, and the need to balance digital regulation with civil liberties continue to hinder the achievement of comprehensive cyber sovereignty. The study concludes that while Pakistan has established an evolving framework for digital governance, greater investment in technological self-reliance, cybersecurity capacity-building, and international cyber cooperation is essential for strengthening its position in the increasingly contested digital environment.

KEYWORDS Cyber Sovereignty, Digital Governance, Cybersecurity, National Security, Pakistan, Internet Governance, Digital Transformation

Introduction

The digital space has evolved from a basic communication platform into the main battleground for international power struggles between nations. Governments today must manage their operations through a digital landscape that has shifted into a sovereign digital ecosystem which includes national artificial intelligence systems and undersea Telecommunications networks and semiconductor manufacturing processes (CIGI 2026). The current situation shows that cyber threats now connect with physical dangers which result from a single code line or an automated system changing International peace conditions through its actions that match traditional military methods (Security Council Report 2026). The need to secure cyberspace has become essential to national interests

because states must protect their cognitive spaces from AI-driven false information and maintain semiconductor independence in an era of growing technological Gaps.

Some researchers observe that cyberspace contains unique features which provide both advantages and disadvantages to governance. The first set of features displays twin characteristics which enable cyberspace control while facilitating effective governance through easement of operational boundaries. The second set of features creates exceptional challenges because it enables states to operate without any geographic restrictions. A state has cyber sovereignty when it holds the right to control and protect cyberspace and digital systems and online activities through its national laws. Pakistan's case gave a clear point of view by which examine the difficulties and obstacles of gaining digital sovereignty in modern world. The cyber population of Pakistan increases day by day fastly and depends on technology. This unique situation of Pakistan shape its access in digital sovereignty. There are several factors such geopolitical location, economic growth, national security and global traditions of digital governance which influence Pakistan to control over its cyber domain.

Externally, Pakistan has unstable relationship with India and good alliance with china make geopolitically its digital sovereignty more important. The establishment of Pakistan's security consider its digital sovereignty protective need to fend off international digital espionage and shield state's data resources. In Pak_ china relationship Pakistan have faster the in flue of CTT (Chine Telecommunication technology). Because of this influe Pakistan fastly connect with Chines cyber governance

Internally in Pakistan the process of digital sovereignty promotes tensions between legal enforcement and civil freedoms. but laws of prevention digital crimes like PECA (Prevention of Electronic Crimes Act) and PTA (Pakistan Telecommunication Authority) which works as modern content control software provides open portal for complaints. Pakistan highly using its Authorities to implement mass internet disruption and utilize modern cyber monitoring and data filtering Apparatus

In this article Pakistan's versatile forces of its digital sovereignty examines along with exploring how a developing and nuclear armed state follows chaotic frameworks of international cyber politics. Its aim provides brief analysis how international change of traditional sovereignty into digital sovereignty is confined in Post-colonial, safety conscious country.

Literature review

As stated by Neyer, (2022) the importance of technology in achieving cyber sovereignty in global politics he discuss in current situation how technology effects on new forms of political actions. The author said that technology can be harmful for global politics. If we study the history innovation which changes the political dimensions. With the help of Research we can make new patterns for handling technology in new shift.

Pierucci1, (2025) explained the rule of technology in 20th century involvement in political matters which produce the new term digital sovereignty. He examines the tensions of borderless nature of cyberspace between states. The Author also discuss the origin of digital sovereignty and USA involved in promotions of soft power in global politics. He discuss the digital sovereignty from physical to virtual and actions of state which reshaped that idea in modern era. Furthermore he explains that technology is Affective for authoritarian and democratic forms of government.

Due to the extreme innovation in technology, the importance of digital sovereignty in globalization is increasing day by day. For a state, active participation in global digitalization and maintaining control over the state's digital infrastructure is becoming a major challenge in the digital world. Furthermore, the author has explored the main threats (international data flows, cybersecurity, and strong governance of NGOs) that the state faces in achieving a good position in the digital world. These challenges are an obstacle to the development of the country. States need to consider them. In order to control the situation, they need to make updated policies and update them with technological innovation. The governments of many countries are working independently on these challenges for safe participation in the digital world. At the same time, countries are working collectively as members of international organizations. They protect and achieve their national interests in the modern world. (Hawng, 2025)

Nanda, (2025) examines the access of a state to the Internet in the past and also studies the present. In the past, there were no borders set to control the Internet or the digital affairs of a state, but at present, each state is trying to secure and control its Internet and digital activities within its own borders. According to the author, this change is called the regional turn. According to the author, behind these difficulties is the desire to gain power, security interests, economic value and human rights. The author, giving the example of China, says that this is what the Chinese government believes in. If you look, it is not only good for an authoritarian system but also good for a democratic system. Countries like European states and the USA have also supported this idea and are working on it.

Rehman and Wadood (2025) examine the era of cyberspace transforming traditional soft craft into "cyber diplomacy." Focusing on the interpretive layer of virtual networks, the authors experience the misuse of Telegram, Facebook, and YouTube, resulting in the Internet being used to exploit internal socio-political tensions and destabilize state rulers. The authors further state that Pakistan began work on national cybersecurity in 2021, and the study critiques the country's current approach as a response. Finally, the authors suggest that Pakistan should establish a formal cyber diplomacy division within its Ministry of Foreign Affairs, and integrate each Education Commission into the Education Department.

Material and Methods

This study is carried out by employing historical, descriptive and analytical approaches to proceed and draw conclusion. For this purpose, qualitative method with Secondary sources has been used. Complementing these are secondary sources—books, peer-reviewed journal articles, and academic theses—which provide critical analysis and historical background on the evolution cyber sovereignty in international system and how it changes into need controlling national defense, economy and infrastructure of the country.

Results and Discussions

Cyber sovereignty

The playground of Politics, government and international relations has experienced significant transformations because of online developments. States use cyberspace as their latest strategic domain to demonstrate their control over political systems while asserting their territorial rights. The emergence of digital technologies has removed all boundaries that separated internal and external spaces, which has forced society to redefine its

understanding of sovereign authority. The control of cyberspace extends beyond physical territory to include all data and network resources which transmit Information across established territorial limits. States are therefore demanding more of the right to control and protect these online spaces, which is creating the notion of cyber sovereignty.

Article Cyber politics: Exploring the state's notion of Cyber sovereignty during Russian Chinese Iranian and other cyber-attacks the United States has tried to maintain maximum internet freedom, but this has led to disruptions which threaten both public safety and national defense. The United States Capitol experienced an invasion when conspiracy theorists and white supremacists entered the building, which was enabled by foreign disinformation campaigns.

Both Russia and China operate authoritarian governments which take advantage of existing worldwide cyber law deficiencies. The lack of international regulations permits these countries to establish online security measures while they use their powerful cyber capabilities to attack Western nations which creates an unfair advantage for Western nations that maintain unrestricted internet access. (Topor, 2023) The concept of "Cyber Sovereignty" reflects the shift from a borderless internet to a "territorialized" digital space where states assert authority to protect their national interests. Below Is an explanation of these driving forces supported by academic research. In 2026 the concept of Cyber Sovereignty has evolved from the 2010s "Great Firewall" model which focused on state-led censorship and ideological content control to a 2020s system which uses national control over hardware AI models and cloud infrastructure to build digital sovereign systems. The global semiconductor security of contemporary states links to their active control over advanced semiconductor technology and domestic AI system development because these assets function as strategic resources which states must safeguard at all costs.

China: Cyber Sovereignty as Authoritarian State Control

China demonstrates how cyber sovereignty functions as a vital tool for dictatorships to enhance their governmental control over international relations. The Chinese government claims complete authority over cyberspace, which it considers as its sovereign territory that includes all land, sea, and airspace. The country's political system follows an authoritarian system which treats political stability and state security and ideological dominance as vital national interests.

China implements its cyber sovereignty policy through its extensive censorship and surveillance systems with the Great Firewall serving as its primary internet control mechanism. The system enables the state to control information distribution while it establishes blocks against foreign websites and tracks user behavior on the internet. Chinese policy documents promote the concept of "internet sovereignty," which states that each country possesses the Authority to control its online territory according to its own legal system and cultural practices and national security needs.

China uses this model to challenge the Western approach which supports unrestricted access to online resources and International digital networks. Cyber sovereignty in China operates as a government instrument that maintains political order while safeguarding national defense and increasing government power during the digital transformation period.

The United States champions a "Liberal Democratic Model"

The United States Department of State operates under a framework that defines cyber sovereignty as an obligation which maintains a worldwide internet system that functions together and remains accessible to all users. The United States employs "Data Free Flow with Trust" (DFFT) as its main method to control data movement because it believes digital borders must not restrict information flow or violate personal rights but rather maintain unrestricted access to information. The government maintains its primary goal of protecting citizens from international cyber-attacks together with digital suppression while using the internet as a medium for democratic expression and innovative development (Ziolkowski, 2025).

The organization uses Multistakeholder governance as its central operating model which distributes power more equitably beyond traditional state-based control systems. A cooperative system combines government entities with private technology companies and civil society organizations and technical experts like ICANN to establish international digital standards. The United States uses this decentralized system to stop any single enemy from achieving complete power over the internet's operational framework. The strategy protects national interests by maintaining American leadership in international liberal systems while safeguarding the financial interests of worldwide technology corporations

Cyber Sovereignty in Global Politics

Cyber space as Domain of power

Warfare and power projection, consolidating land, ocean, air and space these are counting as 15th domain in international relations. Asymmetric environment in cyber space consists of three layers of domain which is made by humans and this is totally opposite to physical Domains. The first layer includes under water fiber optic networks, IT infrastructure, electrical conductor and production facilities. This layer also called physical layer. Second layer includes data files, software code and routing protocols. This layer called logical layer. The ecosystem of information and human users are included in he third layer. Which is called social layer. The ability of state how it manipulates over its critical infrastructure, flow of information and command over pipeline of major technologies measured its power domain. The traditional framework by Stephen Krasner's explains the topology of sovereignty to prove how a state uses its digital means to achieve sovereignty in its territory and control cross border data streams. If a state controls the hidden technological outposts behind it, it will also dominate historic maritime trade routes or fossil fuel reserves. All of this is synonymous with modernity.

Cyber Warfare and Cyber Espionage

The threat of standard or atomic escalation warfare is high, due to which the cyber domain is used by the state to solve problems of high intensity. As a result, the state stays away from active warfare. The attribution problem and cyber proxy wars are essentially conditions in which people from two countries can attack each other without being aware of it. This is possible because it is not easy to keep cyber tracks secret. It is politically difficult to prove which government ordered a cyber-attack. This gives states a good opportunity to lie. To make matters more complicated, governments rarely use their military. Instead of fighting each other side by side, states hire skilled "proxy" hackers to destroy the infrastructure of the opposing nation and steal its secrets while keeping themselves clean.

The Role of Multinational Tech Companies

Independent countries do not rely on authority in cyberspace in the present era. This is one of the major and profound changes in global politics. It is better if states align with multinational technology companies, directly confronting them. Because multinational technology companies operate the international communications infrastructure as owners. Modern states rely on services, operating systems, and cloud architectures. The result is that such resources are thrown into regional politics. For example, companies can block services for the government based on their cyber capabilities and challenge state authority.

Authoritarian / Non-Western Model

Countries like China, Russia, and Iran emphasize cyber sovereignty. China Russia and other superpowers command its data and internet tasks by data security adaptation, rigid Restriction and their boundaries builds constraints international effects and domestic objection

Democratic / Western Model

Western countries support an open global internet, but enforce laws for privacy and a fair digital marketplace. Laws like the European Union's GDPR, DSA, and DMA force global tech companies to adhere to regional regulations.

International Organizations and Cyber Norms

There is international agreement that existing international law and the principles of state sovereignty apply to cyberspace, as clarified by the UN Group of Experts and the Tallinn Manual.

However, states are divided on how to implement this. Western countries support an open and multi-stakeholder Internet model, while countries such as China and Russia prefer a model based on state control and strict surveillance. As a result of this disagreement, global cyberspace is being divided into different ideological and geopolitical blocs.

Evolution of Cyber governance in Pakistan

The transition of cyber governance in Pakistan began from a general cyber frontier to a robust structure, as a domain directed by the state. Due to the growing demand for national security from the development of massive infrastructure, the state is gradually strengthening its control over cyberspace with the help of new federal institutions and legislative frameworks.

Expansion of cyber space and Telecommunications

Pakistan has increased its footprint in the past two decade. In 2019 there were 17% people who uses internet. According to Household integrated Economic survey from Pakistan Telecommunication Authority expose the usage of internet in present time which is increased more than 57 %. But with passage of time this percentage is increasing. By late 2025 there 194 million people's which have active cellular connection on mobile phone. This population is equally to 75.9% of the total population of Country. This framework is set to accelerate further in the future. The government is advancing its $45 million pre-bid deposit phase for the next-generation 5G spectrum bid.

Programs for cyber transformation

Pakistan's digital transformation has determined by the Ministry of Information Technology and Telecommunications. This transformation includes new initiatives like digital export tax holidays and funds for new projects to raise the digital environment. There are over 180 e governance programs started by National Information Technology Board, Along with Auto-processing of federal council procedures or "e Office" Software over the Government sectors. In first time history of Pakistan lunch its first AI based parliamentary system to optimizing work procedures simultaneously securing it data sovereignty

Growth of Digital institutions

To address cyber weaknesses the Institution of Pakistan Telecommunications Authority established by Pakistan with governed telecom system along with controlling all online content and data protection enforcement. The second major institutions National Computer Emergency Response Team in Pakistan which is work on Centralizes which works on Risks intelligence and Security and the third one National Cyber Crime Investigation Agency which works leading organization Combating data breaches, digital scams and virtual militancy

Legal and Institutional Framework in Pakistan

To enhance Pakistan's role in internal digital governance for strategic change, a diverse stakeholder model is important, from Aware to Action oriented one. In Pakistan, the Act 2016 (which was created to prevent electronic fraud) has been amended to accommodate the changes that have occurred over time and to update the existing framework to deal with ransomware or IoT threats in the modern era. With this modern era, Pakistan has adopted an IT strategy, and the Ministry of Information Technology and Electronic Communication has played a key role in linking the Cyber Security Action Plan to various sectors as well as strengthening the cyber ecosystem at the provincial and national levels. Moreover, the Pakistan Telecommunication Authority has a Digital Alertness Division and a devoted Sectoral Computer Emergency Response Team that works on the portal. On the other hand, the PTA's operational infrastructure, command over illegal IP addresses and enhancing technical capacity in the industrial and telecom sectors. further more in global governance Pakistan can achieve Enduring digital Strength and stronger influence through combining the policy instructions of MOITT with strong enforcement of PTA, efficiently making a safe complaint digital system.

PECA

The state approach of Pakistan is determined through a unified legal and controlling model developed to reduce common weaknesses. On the other hand it Promote internal digital sovereignty. Prevention of Electronic Crimes Act 2016 is the statutory root promote digital security in Pakistan there are same main objectives of this Act

Security of private and sensitive information system

Implementation digital crime rules in ecosystem of state.

PECA is leading some agencies such as Federal investigation Agency which works on investigation of cyber crime, gaining its control to trace, seize, and take legal action against bad online performers.

Pakistan Telecommunication Authority

Along with this agency there is another agency PTA (Pakistan Telecommunication Authority) which works as telecom Modulators

Application of strong technical implementation

Managing data traffic

Monitoring cyber space and preventing illegal IP addresses or content deemed harmful to public attention

PTA perform these duties.

Ministry of Information Technology and Telecommunication

Beyond this all mechanism, state's cyber security bodies directly compelled through policy directives "Ministry of Information Technology and Telecommunication" coordinated encompassing state's digital security plans to protect vital digital public system for international Risks. Sometimes this body confronting strong criticism for the civil society about speech freedom. Some legal writers argue that a strong definition within PECA such as these rules give power to government which can take action against the peoples which spread fake information and promote it

Cybersecurity and National Security Concerns

In the current digital era, cyber security has become an important part of national security. Cyber security is very important for all nations because today every nation is using digital technology for national security. This facility has both advantages and disadvantages. Hackers are able to hack digital data, which leads to the leakage of private information of the nation's residents. In the modern era, while the increasing dependence on digital communication infrastructure has intensified the cyber threat to national security, the previous threats to Pakistan have also increased. Digital services can be affected due to cybercrime. Cyber terrorism is also a major problem. The concerns of the Islamic nation are increasing due to the disinformation campaign, due to which Pakistan is facing many threats.

Regional Context

In regional context there is need to improve cyber structure of Pakistan especially when it competes the neighbor country India. From the geopolitical of warfare tensions among India and Pakistan. Digital development in modern world now becomes a major goal for both countries. Because of historical tension between two states in digital race they both strictly competes each other through air space, land and sea safety. This competition between both states is closely link with the world of hybrid warfare which connects traditional weapons and nontraditional ones such as spread fake information, digit skills, perception building, and propagandas. Both states assembles their digital capabilities like digital intelligence, cyber monitoring and internet effects programs etc. In that sense cyber networks can be used building foreign perceptions, defame Competitors. To avoid all these threats, Pakistan needs to create cybersecurity rules and focus on its infrastructure and communication strategies.

Pakistan's International Cyber Relations

International cyber relations means cyber diplomatic relationship between states in the sense of Digital unity, cyber governance and cooperative behavior in digital space. In

this growing digital world Pakistan become a important part of the foreign digital relations. Furthermore Pakistan play its rules not only response to digital threats, also in foreign Discussion on digital governance and skill building. (Rehman & Wadood, 2025)

The current academic literature identifies the issue of (1) lack of legal framework, (2) cyber capacity, and (3) strategic communication as challenges for Pakistan while also pointing out the opportunities of a more coherent cyber diplomacy framework and enhancing regional cooperation.

Pakistan has also been working on the multilateral aspect of cyber cooperation. The Foreign Office of Pakistan was also part of a cyber capacity-building and policy training program, held with UNIDIR in 2026, demonstrating the country's engagement in international initiatives concerning responsible state behavior in cyber space, international law, voluntary norms, confidence building measures and capacity building programs. This means Pakistan is increasingly recognizing cyber security a part of international 'peace, stability and sustainable development'.

Another key issue is Pakistan's stance on international law in the cyber space. Institutions in Pakistan have also facilitated discussions on the application of the international humanitarian law (IHL) to cyber conflict and have reiterated the need to create more robust legal frameworks to limit the use of cyber and digital technologies in order to ensure civilians' safety and the observance of international law. This is an indicator of Pakistan's efforts to influence international standards but also safeguards its own sovereignty and security concerns (Iqbal, 2025).

The key areas of cooperation between Pakistan and the international community are also in the realm of cybercrime and cyber threats. Working with foreign diplomats and friendly countries to improve digital resilience and tackle the cross-border character of cyber risks is part of the official cybersecurity measures. International cyber relations have now become information sharing, joint capacity building and diplomatic coordination due to the cross-border nature of cyber threats. Defense, diplomacy, and policy reform are essential for Pakistan in the era of a cyber war, digital propaganda, and hybrid warfare. Consequently, foreign policy and security dimensions of cyber relations are now playing a pivotal role in Pakistan's overall foreign policy and security agenda.

Challenges and implications

Revolutionizing global politics is what the transfer to cyber autonomy represents here, in which sovereignty over the digital world is perceived as a fundamental part of the security policy and state action of a state. Today, a sense of interest is not only a physical geography, but also the power to control the data, algorithms and infrastructure that underlie a society's operations. With such "digital gate keeping" the nation would end up in a "vassal state" for foreign tech giants or competing superpowers and loss the control of its economy, culture, political stability**.** Pakistan face some challenges in this modern digital world

Technological Self reliance

Pakistan is mostly depending on international technology this make losing its control on digital space

Poor digital safety system

Pakistan's digital data of citizens, businesses, government vulnerable because of insufficient security infrastructure. The weakness allows Competitors attacks on digital data

Professional skill's weakness

Because of lack of skilled trainees allowed to citizens of Pakistan faces cyber threats. This make big hurdle in way of achieving cyber sovereignty for Pakistan.

Stabilizing safety and liberty Rights

Controlling internet content as well as protecting citizens' rights is a huge challenge.

Transboundary digital safety's Nature

Frequently digital threats started from international boundaries Gaining implementation and command complex

Reliance on international platforms of social media

Pakistan's reliance on foreign platforms curtails its authority to dictate data control and information directives**.**

Conclusions

Sovereignty as Survival finally, "Cyber Sovereignty" is "State Interest" — without the capability to manage, control and run their own cyber space, there is no free agency for a country, it is still subject to outside control, exploitation and loss of national identity. Pakistan also doing efforts for running in digital technology with modern world. In this sense Pakistan also introduce physical infrastructure like Ministry of IT and Telecommunication PTA and PECA 2016 which play its role by performing their duties. Pakistan is taking advantage of its neighbor China to join this modern era but its use in the future may prove to be dangerous. Therefore, Pakistan should professionally prepare its citizens to join the digital outfit so that we too can compete with the world and use digitalization to strengthen our economy and ensure national security.

References

Centre for International Governance Innovation. (2026, January 2).*Digital governance in 2026: The key shifts shaping technology, security and global power.* https://www.cigionline.org/articles/digital-governance-in-2026-the-key-shifts-shaping-technology-security-and-global-power/

Hwang, J. Y. (2025). Digital sovereignty in an era of cyber threats and global connectivity. *International Journal of Multidisciplinary Research Updates,* 9(2), 12–23. https://doi.org/10.53430/ijmru.2025.9.2.0023

Iqbal, G. (2025). *How Does International Law Byte into Pakistan's Cyber Governance*? Stimson Center.

Mueller, M. L. (2020). Against sovereignty in cyberspace. *International Studies Review.* https://doi.org/10.1093/isr/viaa046

Neyer, J. (2022)After global governance: Technological innovation and the new politics of sovereignty in internet governance. *Zeitschrift für Politikwissenschaft*, 32(2), 361–382. https://doi.org/10.1007/s41358-021-00290-3

Pierucci, F. (2025). Sovereignty in the digital era: Rethinking territoriality and governance in cyberspace. *Digital Society*, 4(27) https://doi.org/10.1007/s44206-025-00189-4

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

Topor, L. (2023, March 7). Cyber sovereignty: The case of cyber borders and cyber blocs. *Journal of International Affairs*. https://jia.sipa.columbia.edu/news/cyber-sovereignty-case-cyber-borders-and-cyber-blocs

Ziolkowski, K. (2025). *Sovereignty in cyberspace – American and Russian conceptions*. DivaPortal