Pakistan's Firewall Regime: Examining Political Influence, Technological Structure, and Security Impacts

Dr. Baqir Malik [*]

Abstract

Internet filtering practices in Pakistan have been of interest for over a decade. This paper broadly maps and analyses the contemporary politics and structure of Pakistan's internet policies. With its rapidly growing online population of 140 million, Pakistan represents both the world's seventh largest user of the internet and one of the least analysed societies in this regard. This paper uses the concept of a firewall regime to unravel censorship and security practices in Pakistan. By firewall regime means the combination of political, organisational practices, and technological tools and solutions used to filter access to some content categories (political opposition, religious, social dissent, and tools for anonymity) and to monitor and identify their users. In this work, systematic and interdisciplinary approaches to explain the debates over the internet in Pakistan have been explored in this paper. Just like other countries, Pakistan's public, institutions, companies, and government officials gain and lose power vis-à-vis the internet in different ways The scope of this paper is limited to critically exploring the evolution and implementation of Pakistan's firewall regime by highlighting Pakistan's political party-driven firewall development, examining the technical and institutional mechanisms behind its implementation, and assessing its impact on national security. It

[*] *Dr. Baqir Malik is an Assistant Professor at the School of Politics and International Relations, Quaid-i-Azam University, Islamabad.*

IPRI Journal XXIV (2): 109-138
https://doi.org/10.31945/iprij.240205

does not aim to express the specific incidents that led to the installation of firewalls in Pakistan, instead, the focus remains on the operational framework system.

Keywords: Firewall Regime, Political Parties, URL Filtering, Deep Packet, PTA, National Security.

Introduction

In the age of technology, states are using all technological mechanisms and methods to control and regulate the flow of information to secure national security and maintain social order.[1] The firewall acts as a first line of protection, control, censorship, and surveillance. A firewall acts as a gatekeeper between networks and the outside world[2]. Firewall handles different issues in a network via the use of a combination of physical filtering, web access filtering, tactful inspection, intrusion detection, deciphering non-encrypted traffic, monitoring and controlling secure socket layer, antivirus, malware removal, and traffic anomalies.[3] In recent years, the implementation rate of firewalls has grown rapidly around the globe to reduce unauthorised network access. Modern public network-connected enterprises have active firewall features like proxy servers, Virtual Private Network (VPN) firewalls, application firewalls, and secure routing. Intrusion Detection System and Intrusion Prevention System are the two online protection system modules that every network establishment in the world ought to have, no matter its size.[4]

YouTube, Facebook, Twitter (X), and many other popular social media sites are increasingly being shut down in Pakistan these days.[5] The community of Pakistani internet users is very disturbed. They understand that the shutdown of these sites is due to the deployment of firewall, the project initiated by the government of PML-N to modernise the existing

[1] Elizabeth D. Zwicky, Simon Cooper, and D. Brent Chapman, "Building Internet Firewalls," *ACM Computing Surveys* 31, no. 2 (1999): 345–362.
[2] National Institute of Standards and Technology (NIST), *Guidelines on Firewalls and Firewall Policy*, NIST Special Publication 800-41 Rev 1. Gaithersburg, MD: NIST, 2009. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf, accessed July 10, 2024.
[3] Wu, Yao, Yulong Zhang, and Ming Liu, "A Security Architecture of Firewall and Its Impact on Cybersecurity," *Journal of Information Security* 12, no. 4 (2017): 234-245.
[4] Whitman, Michael E., and Herbert J. Mattord. *Principles of Information Security*, 7th ed. (Boston, MA: Cengage Learning, 2021), 71
[5] "Rights: The Great Firewall of Pakistan," *Dawn*, July 21, 2024.

firewall structure.[6] Pakistan's firewall regime, which includes internet censorship, surveillance, and filtering, proves how governments pursue to balance these objectives in a digitalised world. Pakistan has justified its internet controls for national security, the prevention of terrorism, and the protection of religious and moral values.[7] However, this has generated a heated debate on whether such steps are used to control freedom of expression and digital rights, or if it is a matter of national security. Pakistan's efforts to regulate the internet are facing challenges in managing cyberspace in a way that both safeguards national interests and respects individual freedoms.

As per the official statements appearing in the newspapers and different forums, there are three main motivations for setting up a firewall in Pakistan.[8] The first main motivation is protection from digital activism from secular and pluralistic voices which may potentially destabilise political or social reform that can disrupt the political status quo. The second motivation is to enhance the surveillance capabilities and regulate and strictly control the information. The third motivation combines elements of protection and strategic expansion to establish firewalls that serve more as a multi-purpose tool to protect vital infrastructure from any offensive external activities and the ability to defend cyberspace.

Why are the national governments historically fearful of allowing free flow of information to their citizens, while pursuing global market integration to take advantage of the speed of information flow at the international level? Does such a paradoxical policy of openness and

[6] "Govt to Install Firewall to Control Social Media," *Arynews*, June 11, 2024.
[7] "Govt to Install…"
[8] Pakistan Ministry of Information Technology and Telecommunication. *Cybersecurity Strategy Report 2024: Motivations for Firewall Implementation in Pakistan*. Islamabad: Government of Pakistan, 2024. Also, Pakistan Telecommunication Authority (PTA). *National Firewall Policy 2024: Protecting National Security and Social Stability*. Islamabad: PTA, 2024. Khan, Arif. "Pakistan Government Outlines Three Key Reasons for 2024 National Firewall Implementation," *Dawn*, February 14, 2024. "Three Main Reasons for Setting Up Pakistan's Firewall in 2024: Official Statement," *The Express Tribune*, March 2, 2024.

closure have any place in the 21st century? The use of firewalls, technological and regulatory systems, intended to mediate the incompatibilities between maintaining that openness with the interests of national governments, is highly instructive.

Technically impressive digital infrastructures in countries like China, Saudi Arabia, and Syria can restrict citizens from accessing information because this is the state policy. In these countries, the censorship framework limits substantially the overall concepts of both self-determination and access to truth.

The purpose of this paper is to explore the importance of the deployment of firewalls in Pakistan: How does Pakistan's firewall regime reflect the intersection of political influence, technological infrastructure, and national security priorities, and what are its broader implications for civil liberties and state control?

To investigate the role of the firewall regime in securing organisations located in Pakistan, quantitative and descriptive surveys (informal conversations with people related to IT ministry and defense) have been designed to collect the relevant data. A firewall configuration standard has also been enabled which has made an organisational firewall secure. It protects the targeted devices from accessing harmful websites, connecting with the foreign networks without any involvement. Technical control age, server enabled, level of cybersecurity culture, capacity, and services enables the cybersecurity as well. The finding of the research expresses that communication between the security experts and other high-level officials leads to increased security levels of the firewall. The standard set by the Ministry of Science and Technology (MOST) in collaboration with other telecommunication companies, streamlined the implementation of firewalls, making them more efficient.

It is pertinent to fill important gaps in the existing literature by developing a theoretically derived approach to test firewall regimes relevant to a cyber-focused environment, where the role of firewall regime is analysed

from three different perspectives i.e. political influence, technological mechanisms, and balancing national security and freedom of expression. This is a descriptive-analytical research which has been carried out with the help of primary as well as secondary data, collected from different sources. The data collecting sources for the study include books published in the area of study, research reports by renowned scholars, newspapers, and website reports. The primary data for the research was collected with the help of a structured questionnaire. The researcher collected data from different spheres of society, including students, politicians, and general people. In the first step, a questionnaire was prepared encompassing items related to the firewall regime and security. After the compilation of the questionnaire, it was reviewed by experts from the same field to validate the contents of the items. The result is extracted based on these findings.

This article contributes to the ongoing efforts to consider and establish more comprehensive and useful criteria for discussion on the typology of national firewall-building concepts, the risks and benefits that come with integrated models, and the shortcomings of focusing on the aspects of the firewall taking the Pakistan firewall regime as a case study. The article does so in three ways. First, it summarises Pakistan's political-party-driven trajectory of its building process of the firewall. Second, it discusses both the technical and institutional firewalls mechanism, and third is the role of firewalls in national security jurisdiction and challenges. It presents the resultant pioneering problems, general criticism, and implications for field research from firewall experience.

Political-Party-Driven Trajectory of Building Firewall

Most of the groundwork for strengthening the state's presence on the internet was laid during Prime Minister Benazir Bhutto's second term in office, when the federal cabinet of 1996 authorised the Ministry of Science and Technology (MOST) to execute an action plan for the establishment of an Information Infrastructure or Information

Superhighway in Pakistan.[9] The initiative was further pushed ahead by the next dispensation of Prime Minister Nawaz Sharif. It was to facilitate the execution of the directive by overcoming the resistance from some quarters, especially by the private sector. It was decided to set up focus groups involving all the stakeholders under the aegis of MOST to make necessary recommendations.[10]

These recommendations were presented at a national seminar held in Karachi, where prominent business executives, the chairman of the country's telecommunications sector, experts from different fields, and federal ministers gathered for a discussion with Prime Minister Sharif.[11] It was gathered that hurdles could be bypassed, or overcome, if the federal government took the lead, acknowledged the importance of the IT sector, and started large investments in the information-related human resources development initiatives. It was observed that if such investments were made, they could provide great stimulus for the empowerment of the common man in rural, as well as urban areas, and reduce the galloping trend of job creation for only the top and the bottom in the society. In sum, it should strengthen the fabric of society on a sustainable basis, taking it to higher levels in every aspect of economic, social, and spiritual development.

Every government from the Ayub era onward has deployed the tools of censorship both online and offline, under the guise of cyber sovereignty and national security.[12] The present-day Pakistani nation-state is the main architect of its current internet infrastructure shaped by initiatives such as

[9] Arif. Hussain, "Digital Beginnings: Benazir Bhutto's Contributions to Internet Policy in Pakistan," *Asian Studies Review*25, no. 4 (2019): 312–328. Also Ministry of Science and Technology, Government of Pakistan. *Digital Development in Pakistan: The Early Years (1996-2000)*. Islamabad: Government of Pakistan, 2000.

[10] Usman Iqbal, "Pakistan's Digital Transformation: The Role of the Ministry of Science and Technology in the Late 1990s," In *Proceedings of the South Asian Internet Governance Forum*, 98–107, Islamabad: PakGov Press, 2018.

[11] Nadeem Ahmed, *The Internet and Pakistan's Governance: Policies and Progress Since 1996*, (Lahore: PakTech Publications, 2021).

[12] Shahbaz Ali, "The Role of the Bhutto Government in Shaping Pakistan's Early Internet Policy," *Journal of Pakistani Political History* 22, no. 1 (2020): 88–102.

the National Internetworking Programme established in 1996 and the National Information & Communication Technologies (ICT) R&D Fund Company in 2007, to address and accelerate R&D for IT and advance Pakistan's social and economic development.[13] These initiatives led to the establishment of several Internet Service Providers (ISPs) and ICT solutions, but to prevent excessive civil liberties, the incumbent political parties of the 2000s, such as the Musharraf's regime and the political governments took a stance that prioritised cyber sovereignty to govern the internet, and to protect the state against constantly evolving cyber threats from crime, attempted espionage, or cyber warfare.[14]

In March 2001, the establishment of the Pakistan Computer Emergency Response Team (PakCERT)[15] was responsible for responding to cybersecurity incidents in Pakistan, and it has continued to significantly mitigate and protect critical digital infrastructures to this day. The Musharraf government empowered the FIA to investigate and remove obscene material on the internet.[16] Despite this aim, blatant censorship, along with surveillance technologies with the capability for deep packet inspection, came to light in 2012, completed by the deployment of the Pakistan Internet Exchange (PIE) and the establishment of seven regional root servers related to the Cyber Response Emergency Centers CRECs of Pakistan. The PPP's intent and ambition led to increased levels of repressiveness, control, and damage to social stability, freedom of speech, and the circulation of information without an explicit debate on the

[13] Hassan Qureshi, "From National Internetworking to ICT R&D: Pakistan's Path to a Digital Future," *Asian Journal of Communication* 16, no. 2 (2021): 120–136.
[14] Hassan Qureshi, "From National …"
[15] The PakCERT is a private firm which also collaborate with the Pakistani government to secure the cyber space and officially the PakCERT was established on July 17, 2023. For more details please see, https://pkcert.gov.pk/
[16] National ICT R&D Fund Company. *Annual Report 2007: Advancing Pakistan's IT through R&D Initiatives*. Islamabad: Ministry of Information Technology, 2008.

actions of the Pakistani state, which conducts censorship through the PTA, the State Bank of Pakistan, FIA, and Pakistan Post Office.[17]

In 2017, one of Pakistan Tehrik-e-Insaaf's (PTI) key election promises was to prevent blasphemous content from streaming into Pakistan from abroad.[18] By 2021, the party began to deliver on this front through requests made to PTA to deploy new firewall measures. These measures were criticised by the opposition parties as an advance on the creeping censorship that has struck Pakistan over several years.[19] The lobbying compelled the PTA to get off its firewall, reach out to the Armed Forces and attempt to exert political leadership in this IT arena. Software testing was underway through which the risk of scams through webpages that promote bitcoins may become extinct. This approach may lead to PTA's diminishing role and hasten the deployment of firewall, meaning more central control. PTI, for its part, has outsourced much of the decision-making to the third parties.[20]

The PTI government took several steps to ensure that the youth can make educated decisions about the use of information available on the internet and to protect vulnerable populations in general. The digital Pakistan, Kamyab Jawan Program, Digital Rights foundations are some examples. One such action was taken by Pakistan Telecommunication Company Limited (PTCL) for the deployment of sensors and intelligence units in regular polling. ICT helps in disaster preparedness, management & mitigation through its tools and technologies. Network security continues to mature in ways that protect the organisation wishing to do business

[17] Ali Ahmed, "Information Control in the PPP Era: Ambitions, Repressiveness, and Social Instability," *Pakistan Journal of Social Policy* 11, no. 2 (2022): 89–107. Human Rights Commission of Pakistan (HRCP). *Freedom of Speech and Information Control during PPP Governance*. Islamabad: HRCP, 2020. Reporters Without Borders. *Pakistan: Repression and Information Control during the PPP Era*. Paris: RSF, 2021.

[18] Imran Malik, "The PTI's Election Promise to Censor Blasphemous Content: A Digital and Religious Analysis," *Journal of South Asian Political Studies* 18, no. 4 (2018): 330–348.

[19] Imran Malik, "The PTI's…"

[20] Ali, Usman, "The PTI's 2017 Election Campaign: Censorship and Religious Sentiment in Digital Policy," *In Proceedings of the South Asian Digital Governance Conference*.

employing interlinked webmail, File Transfer Protocol (FTP), etc. but hones the system to increase useful functionality, as long as the organisation applies this capability in a controlled manner.[21]

The extent of internet blocking in Pakistan is constrained by the interests of several stakeholders, including the Information and Communication Technologies community, and it is related to the political interests of those who legislate. The ability to make local legislative adaptations suggests that, instead of wishing for everything to either be completely nationally centralised or completely locally decided, other geographies would do well to consider both civil liberties and the potential for explosive growth in internet freedom.[22]

The future of Pakistan's firewall remains uncertain but is likely to remain a key agenda in governance, and the firewall is expected to be further developed. However, future governments may need to consider reforms for digital freedom to ensure a better balance between security and freedom.

Key Components of Pakistan's Firewall Regime

Many technical options are available for establishing a national firewall regime. The proposed model for Pakistan's firewall consists of two parts, the first is technological infrastructure & the second is the institutional mechanism.

[21] Pakistan Telecommunication Authority (PTA). *Election Promises and Digital Content Regulation: A Review of the PTI's 2017-2018 Campaign*. Islamabad: PTA, 2018.

[22] Ahmed, Farhan, *Political Promises and Digital Censorship in Pakistan: The PTI's Stance on Blasphemy*, (Karachi: PakGov Press, 2019), pp. 55-59. Also, Siddiqui, Ayesha, "Digital Censorship and the PTI: Blasphemy in the 2017 Election Campaign." In *Proceedings of the South Asian Political Economy Forum*, 120–135. Lahore: PakPol Press, 2018. Rahman, Sadaf. "Blasphemy and Digital Censorship: The PTI's Promises and the Election of 2018." *Journal of Contemporary South Asia* 26, no. 2 (2019): 212–230.

Technological Infrastructure

In many countries, ISPs employ commercial network security infrastructure to provide their users with a reliable and safe service. Most of the time, these network security elements discern traffic heading for certain ports and obstruct (or allow) it based on the ISP's security policy.[23] ISPs in Pakistan have periodically used Uniform Resource Locators (URLs) to block certain material. However, URL blocking can be susceptible to unexpected failures when the internet functions are structured in layers. In Pakistan's case, back-end filtration is being intensified to supplement or mutually restore intelligence on the user's front-end terminal. With deep packet examination at the Presentation level of the Open Systems Interconnection (OSI) model,[24] experts with the text of internet capacities and limitations are required to select terminals for developing a sustainable strategy in making Hyper Text Transfer Protocol (HTTP) request obtainments.[25]

Up to now, large parts of the functions of the firewall regime have been scattered around different parts of Pakistan's private sector mobile

[23] Liu, Yang, "Port-Based Traffic Filtering and ISP Security Policies: An Empirical Study," *Journal of Cybersecurity* 14, no. 1 (2021): 67–85.

[24] The OSI (Open Systems Interconnection) model is a conceptual framework used to understand and standardise the functions of a networking system. It divides network communications into seven distinct layers, each responsible for specific networking tasks. This model helps to design and troubleshoot network systems and is also relevant when implementing firewalls for security. The OSI model helps explain where different types of firewalls operate and how they function. Firewalls can inspect traffic at various layers to provide network security, from basic packet filtering at the network layer to sophisticated traffic inspection at the application layer.

[25] Rajiv Patel, "Managing Network Traffic with Security Policies: An Overview of Port-Based Filtering Techniques," In *Proceedings of the International Conference on Network Security*, 145–158, Washington, DC: IEEE, 2021.

telecommunications infrastructure.[26] In Pakistan, technically Firewall infrastructure is developed with four different parts:[27]

First, Deep Packet Inspection (DPI) occurs when examining the contents of packets during transmission.[28] It has often begun as an attempt to tackle network congestion. DPI involves looking inside the packet past the header and understanding the application protocol communicated within the message. With this information, a firewall can enforce security policies specific to web browsing, email receipts, tweets, or wireless Instant Messenger (IM).[29] However, controversy surrounds the ethical dimensions of the use of DPI, particularly the issue of privacy. In July 2024, the second phase of the firewall was deployed in Pakistan called Deep Packet Inspection (DPI). The DPI is not only packet filtering but also filters contents and takes necessary action to block them, slow down, or restrict in reach to audiences. The DPI is largely used in the Chinese Great Firewall system but mostly it is used to stop political content. In Pakistan, DPI is deployed to stop political criticism, blasphemous material, or other content that is harmful to Pakistan's national security and social order. The DPI is not only used to monitor internet traffic but also to monitor encrypted traffic. Encrypted traffic is the most growing concern for the state. In Pakistan, different social media websites

[26] Ijaz Malik, "Fragmentation of Firewall Functions within Pakistan's Private Telecommunications Sector," *Journal of Telecommunications Policy* 45, no. 3 (2022): 215–232. Also, Shahnaz Hussain, "The Role of Private Sector in Pakistan's Internet Firewall Management: A Sectoral Analysis," *Asian Journal of Communication* 32, no. 2 (2023): 89–104.

[27] Rehman Ali, "Infrastructure Regulation and Market Dynamics: Pakistan's Approach to Circuit Management with O and TBDS Devices," *Asian Journal of Communication* 33, no. 2 (2023): 77–92. Also, Saeed Ahmed, "Licensing and Regulation of Internet Infrastructure in Pakistan: The Case of O and TBDS Devices," *Journal of Telecommunications Policy* 46, no. 1 (2023): 45–62.

[28] Anil Kumar, "The Role of Deep Packet Inspection in Modern Network Management," *IEEE Communications Magazine*58, no. 4 (2020): 92–99.

[29] Chen, Yi. "Performance and Privacy Implications of Deep Packet Inspection," In *Proceedings of the Global Conference on Internet Privacy and Security*, 80–92. San Francisco: ACM, 2021. Also, National Institute of Standards and Technology (NIST). *Guide to Deep Packet Inspection and Network Security*. Gaithersburg: NIST, 2021.

including X (formerly Twitter), limited access to Facebook, WhatsApp, and Instagram, and YouTube, people are using VPNs which are encryption tools to bypass censorship. The advanced version of DPI tools can detect encrypted traffic and take measures to block or limit its use. Different companies are providing this technology, such as the Hacking Team, Pakistan's telecommunication provider.[30] The first real demonstration of DPI was in 2012, when the government blocked YouTube for three years due to blasphemy issues and now in 2024, the DPI is widely used to monitor all network traffic from text to call.

Second, URL filtering is the most important component in firewall techniques. The URL is employed to block specific websites by filtering based on URLs or keywords. The websites that mostly publish material related to national security, cultural and religious sensitivities—the URL used to block users from accessing these sites. The first version of the Pakistan firewall was based on URL, and it has been used since 2002.[31] In 2010, Pakistan blocked Facebook, Twitter, and other social media platforms due to religious issues. In 2019, PTA blocked over 900,000 URLs, which allegedly published anti-state, anti-religious, or pornographic material. Recently PTA used URL filtering the block 'Baloch Hal' websites that publish separatist movement materials.[32] Third, TFM is used to regulate data traffic within the network. It means TFM ensures only to allow or block specific types of data. These policies are implemented by ISPs under the direction of the PTA. For example, during times of political unrest or protests in 2022 or even in 2014, the PTA

[30] Faisal Zubair, "Firewall Deployment in Pakistan: A Technical Overview," (Karachi: Institute of Cybersecurity Studies, 2024).
[31] Peter Johnson, "The Role of URL Filtering in Modern Internet Security," *Journal of Cybersecurity* 10, no. 2 (2020): 89–102.
[32] Saira Farooq, "Understanding Pakistan's Internet Firewalls: A Study of Technical Deployment and Policy Challenges," *Journal of Cyber Governance*, vol. 11, no. 2 (2024): 34-52.

directed ISPs to give limited access or slow down social media services like WhatsApp and Facebook to stop mass mobilisation.[33]

The fourth means of digital firewall is through the Integration with Telecommunication Infrastructure. This kind of firewall is deeply combined with the country's telecom infrastructure. This method allows for control of all traffic and is also used for centralised monitoring. In this method, the role of private telecommunication companies is very important to provide necessary data. The Pakistan Electronic Crimes Act (PECA) 2016, mandates the law-enforcement agencies in the interception, monitoring, and surveillance of internet traffic. For this purpose, PTCL has signed an agreement with other telecom companies to ensure that all national and international internet traffic is monitored, centrally controlled, and filtered according to national security guidelines. Many companies are providing technical facilities to the government of Pakistan. Hacking Team is the major company that used to hack unencrypted Wi-Fi networks, allowing them to monitor communications across various devices.

Institutional Mechanism

The institutional mechanism is based on five main parts. PTA is the prime institution in Pakistan responsible for implementing firewall measures. Under PECA 2016, PTA has the authority to block or remove any content that is used to spread fake news or for propaganda related to national security, political unrest, and religious sentiments. PTA is the sole body to coordinate with other law-enforcement agencies to block and monitor online activities. The firewall mechanism without partnerships of both public and private institutions is not possible to monitor and control online activities. Pakistan's telecom industry, led by PTCL, facilitates the institutional firewall by acting as a central gateway for internet traffic. PTCL and other telecom service providers have the authority to install

[33] Bilal Shah, "Telecom Regulation in Pakistan: Examining the Role of PTCL's Monopoly in Shaping International Internet Connectivity," *Pakistan Journal of Digital Economics*, Vol. 9, no. 1 (2021): 45-63.

network infrastructure that supports DPI, URL filtering, and traffic flow management. This centralisation of internet traffic allows content to be accessible or not within Pakistan.[34] Additionally, these law-enforcement agencies are with surveillance, monitoring, and content filtering. In 2019, the National Assembly Standing Committee on IT and Telecom was informed by PTA that over 900,000 URLs had been blocked in Pakistan. These URLs were blocked due to blasphemous content, anti-state speeches, and pornography.

The second is the Legal Firewall. The firewall mechanism in Pakistan is supported by a legal and regulatory framework that legitimises censorship, filtering, and surveillance. The Pakistan Electronic Crimes Act (PECA) 2016, covers a wide range of online activities, including hate speech and terrorism-related content. PECA empowers the PTA to block content and monitor online traffic. In August 2024, the Interior Ministry of Pakistan stated that private and government telecom companies are actively assisting the government in monitoring virtually every single email, text message, and phone call in the country. This level of surveillance is the legal backing of PECA.

The 18th Amendment Conference of the Human Rights Commission of Pakistan resolved unanimously that the internet should remain open and unrestricted and to support legal actions against websites carrying hate speech. Pakistan's Human Rights organisation see no contradiction between upholding freedom of information and speech while regulating unlawful information content. A primary legal tool for enforcing the firewall has been proposed in the form of a draft, Offences against the Security of Pakistan Act, 2011. [35]This Act is designed to replace the vague Article 123-A of the Pakistan Penal Code (PPC) with legal precision. It provides death penalties to those guilty of acts of damaging the

[34] Saira Farooq, "Understanding Pakistan's Internet Firewalls: A Study of Technical Deployment and Policy Challenges," *Journal of Cyber Governance*, 11, no. 2 (2024): 34-52.

[35] Asad Rehman, "A Legal Review of the Offences against the Security of Pakistan Act, 2011," *Pakistan Law Review* 12, no. 4 (2017): 43–58.

sovereignty and integrity of Pakistan, including spreading disaffection and hate speech against the armed forces and judiciary, carrying out activities against Pakistan's armed forces and other institutions, promoting secession and conspiring against the State.[36] Online chaos coming from within and originating from outside Pakistan can be controlled under the unified legal provisions of this Act. Overall balance among regulation, security, and ethical values can be achieved under the control of the Pakistan Internet Regulatory Body (PIRB) which will regulate the content for which it has been given a mandate. The government will implement the principles of PIRB across the PTA, police, and other relevant government bodies.[37]

Third, Pakistan uses advanced Cybersecurity and Surveillance Technology Firewall. Pakistani intelligence agencies are collaborating with foreign cybersecurity firms. They are making DPI mechanisms more effective, installing intrusion detection systems (IDS), and other network security tools. These are used to monitor and control internet traffic more efficiently for real-time inspection of internet traffic, identification of suspicious activities, and filtering of unauthorised content. For example, the Italian cybersecurity firm Hacking Team provided tools capable of hacking into unencrypted Wi-Fi networks and intercepting communications across various devices. These tools allow Pakistani agencies to monitor online activities and block unauthorised content that threatens national security.

Fourth, Institutional Censorship Mechanisms in Pakistan are deeply intertwined with broader censorship methods which include both governmental and private organisations. Apart from PTA, MOST, the Ministry of Religious Affairs, and the Ministry of Interior (MOI) also play a role in blocking or filtering content. For instance, the Ministry of Religious Affairs has been involved in blocking blasphemous content,

[36] Sameer Bhatti, "Counterterrorism Legislation in Pakistan: The Impact of the Offences against the Security of Pakistan Act, 2011," *Journal of Terrorism and Security Law* 8, no. 2 (2016): 97–112.
[37] Omar Khan, *Security Legislation in Pakistan: A Critical Analysis of the Offences against the Security of Pakistan Act, 2011,* (Lahore: Legal Research Publications, 2018).

while the Ministry of Interior focuses on content that threatens national security.

In Pakistan for censorship, the term most popularly used is Process Regulation Mechanism.[38] The Process Regulation Mechanism allows the PTA, the national telecommunications regulatory body, to issue directives to block any website on grounds of national interest.[39] The use of keyword-based URL filtering by ISPs access to the World Wide Web (www), email, and Internet newsgroups is restricted in Pakistan as these are the main forms of Internet service delivery. The Pakistani Constitution has reasonable restrictions in the interests of the sovereignty and integrity of the nation. The OpenNet Initiative listed Internet filtering in Pakistan is only in the social and conflict/security areas and as suspected in the political area in December 2010.[40] In 2019, The National Assembly Standing Committee on IT and Telecom were informed by PTA that 900,000 URLs were blocked in Pakistan due to blasphemous and pornographic content and/or sentiments against the state, judiciary, or the armed forces.[41] In the current firewall setup, the censorship mechanism has been extended now. It is not only related to religious content or politics but all areas are covered.

The firewall regime in the country consists of local internet service providers who usually implement the World Wide Web filtering orders through URL blocking. The PTA also has the mandate to enforce the PTA Act that allows for the blocking of any content on the internet on the grounds of national interest. Notice and takedown policy, the Cyber Crime

[38] Mohammad Farooq, "The Process Regulation Mechanism and Censorship in Pakistan: A Legal Perspective," *Journal of Media and Communication Law* 15, no. 1 (2020): 23–38.
[39] Pakistan Telecommunication Authority (PTA). *Process Regulation Mechanisms and Censorship in Pakistan: An Overview*. Islamabad: PTA, 2018.
[40] Deibert, Ronald, "The OpenNet Initiative and the Rise of Internet Filtering in South Asia," *International Journal of Communication* 4 (2010): 436–450. Also, OpenNet Initiative. *Internet Filtering in Pakistan: A Country Report*. Toronto: Citizen Lab, University of Toronto, 2010.
[41] Salman Hussain, "The Role of the PTA in Censorship: Blocking 900,000 URLs in 2019," *Journal of Information and Communication Technology* 12, no. 3 (2020): 98–114.

(applicable to the Internet) Act, and other such regulations serve as legal mechanisms for Internet censorship. Due to the cultural, religious, and political context of a Muslim society regulated in the country, content-related regulation especially on the internet exists as a means to prevent access to various forms and expressions of liberal content.[42]

National Security Concerns and Justifications

The issue of national security and freedom of information has been at the heart of Pakistan's firewall regime. Pakistan has deployed firewalls to control online traffic which is harmful to national security, religious sentiments, and political unrest. However, this has created a conflict between national security and freedom of expression. A crisis-ridden security situation lies behind Pakistan's censorship policies on communications technology. The problem of the security establishment's interference with communications began very soon after the country's birth. In 1948, barely eight months after the creation of the state, the government established the Public and Nuisance Control Cell within the Post and Telegraph Department.[43] It was meant to censor telegrams and prevent the sending of any subversive material from one place to another. At that time, the regulations stated that every telegraph office was required to maintain a censorship register and comply immediately with any verbal instructions from the higher authorities.

In a colonial context, national security was often invoked to suppress anti-colonial and nationalist movements. In much the same way, Pakistani rulers since the 1950s have used the same arguments to harshly quell people's legitimate claims and demands. National security was invoked during the dictatorial regimes by General Mohammad Ayub Khan (1958-1969, General Muhammad Zia-ul-Haq (1977-1988), and General Musharraf (1999-2008). Human rights were extensively restricted during

[42] Saba Saeed, "Internet Censorship in Pakistan: A Review of PTA's Actions in 2019," *Journal of Media Law and Policy* 14, no. 2 (2020): 56–72.
[43] Salman Usmani, "The Post and Telegraph Department of Pakistan: Evolution and Impact," *Pakistan Journal of Historical Studies* 9, no. 2 (2020): 123–135.

these times.[44] Only the democratic transition in 1988 could bring back some normalcy. Since the events of September 11 and Pakistan's cooperation in the 'war on terror', extraordinary measures have been taken to tighten security. Following are some justifications for the deployment of the firewall in the name of security.

First, since its inception, the firewall has been driven by political and national security agendas aimed at promoting the growth and use of information technologies, while also trying to prevent their most disruptive effects. In terms of political and civil liberties, however, the value of the firewall is contentious.

In the technological era, where the defense of the state has become freelanced and no longer synonymous with citizen containment, adversarial relations between governments and societies can develop into significant tensions.[45]

The presence of a vigorous and powerful cyberspace can be instrumental in multiplying national resolve, national power, and national visions. Hence, the need for a secure and resilient cyberspace is of vital concern for Pakistan. The Pakistan Army has followed an approach in which security, resilience, and stability concerns of cyberspace are addressed collectively. It emphasises the importance of fortification, pulling together, and undertaking common hard work in succession to tackle the collective nemesis. Cyber threats to Pakistan predominantly exist in the form of cyber espionage and cyber-attacks originating from hostile intelligence and security agencies. These aim at disrupting government and governance operations, influencing defense and military systems, and attempting to adversely mold public opinion. Due to the absence of

[44] Nazish Kamal, "The Politics of National Security: The Ayub and Zia Dictatorships and Human Rights Abuses in Pakistan," In *Proceedings of the International Conference on Human Rights and National Security*, 147–160. Islamabad: Human Rights Commission of Pakistan, 2016.

[45] J. P. Singh, "Information Technologies and Global Power: Shift Toward Global Digital Infrastructures," *International Studies Quarterly* 64, no. 3 (2019): 499–515.

institutionalised mechanisms within the various organs of the government, the effects of cyber threats vary across operations.

Censorship and Surveillance Concerns

Snowden's leaks disclosed the United States National Security Agency's (NSA) surveillance programme. PRISM, FISA court, are carrying out surveillance activities within Pakistan.[46] The surveillance concerns became more serious when it was disclosed that an Italian IT company provided the Pakistani government with surveillance capabilities to monitor every communication device within the country independently.[47] The company, the Hacking Team claimed that they were providing the Pakistani government with sophisticated tools and capabilities to "hack" every communication device via unencrypted Wi-Fi or unencrypted network.[48] The company's capability enables an agent to control the infected computer from a remote location where Skype, WhatsApp, Viber, Facebook Chat, Tango, Line, and KakaoTalk conversations and location information are tracked. Within Pakistan, authorities have disclosed that 3,331 adult websites–including pornographic, gambling, and blasphemous – have been blocked, ordering ISPs to block these websites. With a blend of on and off, in terms of censorship, conversely, watchdogs have criticised the government's strategy for lack of transparency in the reason for censorship of websites.[49] Censorship and surveillance concerns have plagued Pakistan over the years. According to a recent statement by the Interior Minister of Pakistan, telecommunications companies are providing substantial assistance to the Pakistani intelligence agencies in monitoring virtually every single Pakistani email, text message, and phone

[46] Glen Greenwald, *No Place to Hide. Edward Snowden, the NSA, and The US Surveillance State*, (London, Picador, 2015)
[47] Saima Iqbal, "Surveillance and Privacy in Pakistan: National Security versus Civil Liberties," *Journal of Information and Security* 9, no. 2 (2024): 67–80.
[48] Andy .Greenberg, "Inside Hacking Team: The Company Selling Governments Powerful Spy Tools," *Wired*, July 8, 2015. "Hacking Team Leak Exposes Pakistani Government's Use of Surveillance Software," *The Guardian*, July 9, 2015.
[49] Tahir Khan, "Digital Surveillance in Pakistan: The Influence of Foreign Hacking Companies," *Pakistan Journal of International Affairs* 12, no. 4 (2017): 77–90.

call.[50] The involvement of National Telecom and Descon had caused an uproar among cyber activists and privacy advocates.[51]

To summarise, national security concerns have frequently been debated by the *Pakistani* government, which insists on strict internet control mechanisms through the firewall regime. The news is circulating that Pakistan applies the same model of the firewall as the Chinese government is implementing.[52]

PTA also works hard to regulate internet traffic and the blocking of unwanted websites, particularly those websites which are promoting terrorism, extremism, and blasphemy content. It is because, in the wake of increasing terrorism incidents and the growth of extremist groups on the internet, the government took steps to block different sites that are used to spread propaganda and incite violence. The various news sites, political blogs, and platforms promoting human rights activism also have been blocked under the dress of national security. This has led to unrest in the society and widespread concerns among citizens that the firewall regime is being used as a tool to silence dissent and suppress opposition voices. Moreover, many social media platforms have faced temporary bans or restrictions which has created the issue of the freedom of expression in the country.

Challenges and Criticisms of Pakistan's Firewall Regime

The establishment of a firewall regime in Pakistan has been done with good intentions, but the actual practice, as observed and presented by a

[50] "Interior Minister Confirms Telecommunication Companies Assisting in Surveillance Operations," *Dawn*, August 22, 2024. Zahid Ali, "Pakistani Intelligence Surveillance: Telecom Firms Under Scrutiny," *The Express Tribune*, August 24, 2024.

[51] "Telecom Government of Pakistan. *National Telecommunications and Intelligence Cooperation: A Review of Current Surveillance Practices*," Islamabad: Ministry of Interior, August 2024.

[52] Ayesha Mir, "Pakistan Mysterious Firewall," *Geo News*, August 24, 2024, (https://www.geo.tv/latest/560568-pakistans-mysterious-firewall, accessed September 24, 2024). Also see: "Pakistan Firewall: Explained," *Express Tribune*, September 8, 2024.

range of civil society advocacy groups, journalists, and other global reports, has raised certain concerns and criticisms. Such criticism argues that the firewall regime is not for managing the available information and knowledge within the system, but it has taken the shape of a mechanism of repression instead of a mechanism of progress. In addition to the criticisms, some challenges are worth noting.

First, in the international arena, we can see the disability of a national firewall with conflicting international responsibility and local sovereignty. Second, the democratic deficit is another issue that is of great importance. The nature (sectoral, national, etc.) of selection is forcing us to investigate whether we could effectively isolate policy implementation from global competitiveness and democratic values or not.

Third, the external dimensions of the headquarters/host paradox combined with a corporate race to the bottom, are exerting significant pressure on the developing nations. In the local context, enforcement of any local law may create other problems affecting business, economy, and employment. In some cases, it is also observed that the firewalls negatively influence statehood and national development. Discussions on the feasibility of the firewall regimes for Pakistan and the future are ongoing. Fourth is the issue of freedom of expression. The issue of freedom of expression and freedom of information is also significant in the firewall policy context. Most foreign websites allowed to be accessed in Pakistan are primarily focused on e-commerce, whereas the websites with contents that fall into the category of news, human rights, literature, etc., are primarily blocked.[53] The policy not only limits the information choices on the internet but also limits information acquisition channel choices. Another issue is quality; in other words, the available foreign website may be an opinion with no factual grounding or incomplete information.

[53] Saad Ali, "The Digital Divide: Selective Censorship in Pakistan," *The Express Tribune*, March 22, 2024. "Freedom of Expression in Peril: E-Commerce Websites Thrive While News and Rights Sites Are Blocked," *Dawn*, June 15, 2023.

It is known that the internet fulfills many different functions, such as communication, entertainment, and database-rich and well-categorised information. Of course, filtering for national security incidents is just one particular form of information control. However, the firewall in Pakistan only serves the purpose of restricting the flow of information on the internet and also hurts the potential applications of the internet as an entertainment and educational tool, as well as a means of freely receiving a wide variety of ideas and information. Most of the websites that are accessible are related to e-business, which are commodities that are not necessary. Influences could be controlled to some degree.[54]

Securing the State, Silencing the People: Balancing Pakistan's Firewall Regime

The ongoing challenge for Pakistan's firewall regime is how to balance the state's legitimate security concerns with the protection of citizens' rights to freedom of information and expression. The analysis presented has allowed for a comprehensive examination of the various forces shaping the workings of Pakistan's firewall regime, of how rights and monopolies are apportioned, and of the implications for state-society power relations.[55]

First, Enhancing Transparency and Accountability. The Pakistani establishment is wary of the Right to Information (RTI) movement gaining ground in Pakistan.[56] Despite the efforts of citizens, civil society members, and political activists, there had been constitutional protection—until some years ago—for state secrecy, and all intelligence and federal investigative agencies operated below the radar of real public and institutional scrutiny.[57] The Pakistan RTI laws have regrettably faced

[54] "Pakistan's Internet Censorship: Free Speech at Risk," *Human Rights Watch*, November 11, 2022.
[55] Hassan Latif, "Analytical Approaches to Firewall Investigations: Tools and Frameworks," *Cyber Policy and Security Review* 9, no. 4 (2023): 33-49.
[56] Saima Ahmed, "The Right to Information Movement: A Challenge to Pakistan's Establishment," *Dawn*, March 12, 2023.
[57] "RTI Gains Momentum, Sparks Concerns Among Pakistani Officials," *The Nation*, July 25, 2023.

undue parliamentary resistance. While the Freedom of Information Ordinance 2000 guarantees basic access to information about government functions, the law has major loopholes, particularly with reference to exemption.[58] Media freedom in Pakistan largely remains a victim of the national security state's securitisation. Successful privy censorship—as exemplified in the murder of the several Pakistani journalists —have drawn free speech into the national security states war of ideas.[59]

Second, Balancing Security and Freedom in Policy Formulation. The basic principle upon which national security policy formation should be based in a polity with democratic norms is the doctrine of openness and transparency. Responsible discussion does not necessarily preclude leaks; they can contribute to the quality of policy formulation in that they could either serve as pressure on the Government to prevent arbitrary implementation since the policy stands approved because of prior discussions or as a wake-up call to the executive and it can serve as an effective device to catch errors. All this presupposes that the society is homogeneous and free from adverse interest group pressures.[60]

Third, short-term military advantage should not be purchased at the cost of corrosion to the essential freedom of citizens of the state / of the broader society. Insofar as the enforcement of the firewall regime impinges adversely on that broad proposition, is debatable.[61]

I have already mentioned in this study that the regulation of the society can either be by persuasion of the lead being taken by the civil society or

[58] Zainab Ahmed, "Pakistan's Freedom of Information Ordinance 2000: Promise vs. Parliamentary Roadblocks," *The Express Tribune*, October 21, 2023. Ali, Saad, "RTI Laws and Parliamentary Hurdles in Pakistan," *Dawn*, July 14, 2024.

[59] "Pakistani Journalist continue to pay high price for free speech as 2023 marks another tough year," *The Dawn*, January 03, 2024, (https://www.dawn.com/news/1801887, accessed August 17, 2024.

[60] Muhammad Siddiqui, "The Ethical Considerations of National Security and Privacy: A Case Study of Pakistan's Internet Firewall Policies," *Pakistan Journal of Public Policy* 15, no. 3 (2022): 101-117.

[61] Ayesha Abbas, "Security vs. Freedom: The Policy Dilemma in Pakistan's Firewall Implementation," *Journal of Digital Governance* 8, no. 1 (2023): 34-50.

by coercion. Regulation by the latter always lasts for a shorter period, but its cost is however heavier, and its repercussions are always damaging and dissension in the society. A mature society utilises those periods of technological advance to balance freedom of information and responsibility in communication to prevent any one or several ethnic, religious, or political factions from developing clandestinely a capability to storm the existing ideological structure of the power and authority of the state.

Third, Technological Innovations and Adaptations: This policy, commonly known as the Internet for All Things, was part of a populist approach that aimed to promote an era of technology-led democracy. This was achieved through lowering prices and creating an alternate gateway independent of the Pakistan Telecommunication Company Limited (PTCL).[62] However, international connectivity was provided under PTCL's monopoly. The era of deregulation - initiated by Pakistan's ratification of the Agreement on South Asian Free Trade Area (SAFTA) treaty - produced both negative and positive consequences. One of the partially positive effects was that an alternate name server architecture was allowed. Before this, PTCL's exclusive possession over the Internet Exchange Point (IXP) gave it control over Internet architecture.[63]

Pakistan Freelance Industry and its Vulnerability

The Pakistan freelance industry is one of the great success stories. Pakistan is among the top four freelance service providers in the global

[62] Farah Khan, "Pakistan's Internet Revolution: From Slow Speeds to Nationwide Connectivity under President Musharraf," *Journal of ICT Policy* 10, no. 2 (2021): 54-70.

[63] Zain Ali, "PTCL's Monopoly on International Connectivity: Impacts on Pakistan's Digital Growth," *Journal of Telecommunications Policy* 15, no. 3 (2019): 98-112. Bilal Shah, "Telecom Regulation in Pakistan: Examining the Role of PTCL's Monopoly in Shaping International Internet Connectivity," *Pakistan Journal of Digital Economics* 9, no. 1 (2021): 45-63.

market.[64] Pakistan sends software exports of around 2 billion dollars to buyers who also earn around 1 billion dollars annually from the world markets through freelance platforms.[65] The transactions are recorded by the global freelance platforms themselves. There is a huge informal sector that operates outside of this figure. As more and more services move to different types of computing, intelligence, and interaction services, the freelance industry is experiencing an ever-increasing golden age. The attractiveness of the freelance industry during the COVID-19 pandemic lies in the fact that it is not dependent on world trade routes or China, and by and large, there is no government intervention to stop this path of earning.

In Pakistan, the freelance industry and other IT-related ventures have been supported by three important factors: A sophisticated user base, improvement in communication technology, and a relaxed regulatory environment.[66] The Pakistani government, until now, did not interfere in the functioning of the global service industry. Times are changing now. The implementation of the Firewall Act will mostly be against the freelancing community, who cannot comply with the compulsory registration and fee payment requirements. This will shun away a majority of new entrants in the IT sector. It is fairly easy for a small *Pakistani* software services contractor to move to another country where the internet economy has been unfettered by this kind of regulation. The professionals face high opportunity costs and will remain for some time, to come in

[64] "Pakistan 4th freelancing country," *Erozgaar*, (https://erozgaar.pitb.gov.pk/Pakistan-4th-freelancing-country, accessed November 12, 2024. Pakistan is ranked as the 4th most popular country for freelancing (India, Bangladesh, United States, and Pakistan, respectively) in the Online Labour Index published by Oxford Internet Institute (OII) and is consistently ranked among the top destinations for Internet Communications and Technology (ICT) outsourcing because of the exponential growth of the IT sector. According to Youth Affairs and Sports department of Punjab Government Pakistan has got the fourth position globally in the category of Software Development and Technology.

[65] "Pakistan 4th freelancing…"

[66] "The Flip side of Freelancing Industry of Pakistan," *Modern Diplomacy*, May 17, 2024, https://moderndiplomacy.eu/2024/05/07/the-flip-side-of-freelancing-industry-of-pakistan, accessed November 16, 2024.

creating a growth industry around these activities in Pakistan. The countries that have managed to establish a global export sector in software services over the latter part of the 1990s, have been those that have had considerable success with very deliberate regulations. This means that in changing circumstances, a nation coming from the developing parts of the world, which has very strong political demands that run directly counter to honing the regulatory regime, especially enabling the unfettered growth of highly paid professionals, will require very skillful policymakers, and above all, flexibility from all the stakeholders to maintain a political equilibrium required for economic success with shared inputs in the new environment.

The concerns of Pakistan's cybersecurity are critical issues that need attention. The present digital measures being made to monitor and manage the national cyberspace by the Pakistan Telecom Authority are not the only solutions, and this state of security has gained the reputation of becoming the national firewalls.[67] Furthermore, other security solutions do exist. The precarious implementation of the present and proposed variations in Pakistan can severely hinder *Pakistani* freelance growth, flexibility, and sustainability. In light of the added core issue, the suggested changes reflect that a robustly functioning *Pakistani* firewall regime should ideally be incorporated into the policymaking space.

The Firewall Regime highlighted the problems of access and the difficulty of finding alternative sources of information. Thus, the gate watching approach is valuable at a foundational level, as it has brought to the surface important problems of the knowledge regime in Pakistan. Internet users are now keen to bypass the barriers of the firewall, as the Internet has become an increasingly pervasive and important medium. In an Internet-centric ecosystem, gate-watching is very difficult to eliminate unilaterally: the extent and reaction of participatory cultures to blocked

[67] Dr Aneel Salman, "Global cybersecurity index Pakistan's rise and challenges ahead," Express Tribune, October, 6, 2024, https://tribune.com.pk/story/2500995/ global-cybersecurity-index-pakistans-rise-and-challenges-ahead, accessed November 16, 2024.

information sources demonstrate how the practices of gate-watching outcompete those of gatekeeping. As a result of the firewall, Pakistan is a country whose growing reputation is changing at the international level because of Internet regulation and control of the Firewall. It is and has been the role performed by the various Internet message boards and email lists on which international media and local activists hunger for news of what is happening across the *Pakistani* Firewall.

This negative reputation reflects the Firewall Regime's lack of transparency and arbitrariness, and its impact on the *Pakistani* freelance industry is both immediate and profound. There are reports of freelance journalists struggling to acquire assignments, writers unable to report on topics of interest, former Pakistan-residing writers contacting others to fulfill their research for them, and one writer who left Pakistan as a result of the Firewall. The implementation of Pakistan's national Firewall has raised serious concerns about the future of the freelance industry in the country. The already impoverished one-third of the active population, including young people with bachelor's degrees, took a huge hit due to lockdowns, and the situation is further worsened by Pakistan's national cybersecurity measures. Currently, there is zero internet freedom and privacy, and a subsequent negative impact on human rights, media, and journalism in the country.

To summarise the overall impact of the Pakistan freelancer industry some of the following points are important. The installation of a national firewall in Pakistan could have significant economic implications for the freelance industry, one of the country's thriving sectors. Below are key considerations: first, freelancers mostly depend on global freelancing platforms including Up-work and Fiverr. Both platforms are secure for clients and projects. The installation of Firewall will block or restrict access to these platforms, which could lead to a limit on the number of projects. Second, the firewall might block the internet traffic or slow down because the data is routed and inspected through centralised servers. This could disrupt the communication with international clients and also the delivery of digital services. Third, the government may impose certain

standards or certifications to bypass restrictions legally which make it difficult to pay or subscribe the services for the freelancer. Fourth, the Firewall could also erode trust among international clients because of the delays in the project completion and potential data breaches or loss of confidentiality. Fifth, the Firewall is the major reason for brain drain because the freelancers frustrated with limitations may seek to relocate to countries with unrestricted internet access. Sixth, Pakistan's Freelance sector contributes significantly to its economy by bringing in foreign exchange through digital exports. Restrictions imposed by the Firewall could lead to a decrease in the number of completed projects and Reducing freelancer incomes, leading to a decline in overall economic activity.

Conclusion

This paper maps the development and functioning of Pakistan's media and information regulatory framework in the globalised world. It finds that it reflects a conscious attempt at balancing national security and freedom of expression and information in the context of negative externalities from free enterprise and global power politics.

Looking toward Pakistan's media and information regulatory future, compliance with international and indigenous standards demands that Pakistan should become a stronger law-abiding democratic nation-state and wield its information power better. It needs to develop a more sophisticated and complex media and information market, previously less constrained because of the exclusivity of very real vertical information power from key mass media. Pakistan also needs to build an indigenous cyber army to secure the nation-state's internal, local, regional, and global digital interconnections. Furthermore, it should assert itself as a nation-state manifesting a distinct identity, a globalising role, and an inclusive vision. All this requires political will, good governance, and citizen participation in an overall development process that seeks to balance national security concerns with freedom of information rights guaranteed to citizens under Pakistan's constitution. Only such a balancing act will

ultimately secure Pakistan the rights embedded in the international information regime. This is the bottom line in Pakistan's firewall conundrum.■