Journal of Engineering, Science and Technological Trends (JESTT)

Vol. 2, Issue 1, February 2025
DOI: https://doi.org/10.48112/jestt.v2i1.11

Article

Firewall Technology Testing in Pakistan: The Fine Line Between National Security and Freedom of Expression

Jalil Ahmad[1], Aftab Haider[1*] and Anisa khalid[2]

[1]Southwest University of Political Science and Law, China

[2]Aisha Public School and College, KPK, Pakistan

*Corresponding Email: aftabhaider@awkum.edu.pk (A. Haider)

Received: 02 December 2024 / Revised: 18 January 2025 / Accepted: 04 February 2025 / Published online: 28 February 2025

This is an Open Access article published under the Creative Commons Attribution 4.0 International (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0/). © Journal of Engineering, Science and Technological Trends (JESTT) published by SCOPUA (Scientific Collaborative Online Publishing Universal Academy). SCOPUA stands neutral with regard to jurisdictional claims in the published maps and institutional affiliations.

ABSTRACT

Concerns have been raised over the international trend of relying on firewall technology for cybersecurity and digital censorship, especially in Pakistan. Firewalls are important to protect critical infrastructure, but can also be used to restrict access to information as state-controlled devices. In this article, we critically examine Pakistan's firewall deployment, investigating whether it intended to promote national security or online freedom. This study applies qualitative analysis, through economic, legal, and technological assessment of firewall policies in Pakistan, especially in the light of the amendment of the Prevention of Electronic Crimes Act (PECA) in 2025, which was in the course of writing this article, and the implications of this on the economic, political and social life of the country. It also draws comparative insights from global cybersecurity models, including China and Iran, to analyze Pakistan's trajectory of digital governance. The key findings highlight that Pakistan's firewall policies have increasingly been used as a means of controlling the internet; laws are unclear and can be used to limit free speech and media. Firewall-based censorship also has hidden economic costs, which now reach $1.62 billion in 2024. Implications of this research suggest that digital rights and cybersecurity should be balanced in the policies. Key to preventing Pakistan's cybersecurity efforts from eroding democracy and economic growth is transparent firewall governance and independent judicial oversight. Without such reforms, Pakistan runs the risk of digital isolation, loss of investment, and online freedoms. The findings add to the ongoing debate about cybersecurity law, digital human rights, and technology in government.

Keywords*:* Firewall; Cybersecurity; Digital Rights; National Security; PECA 2025; Internet Censorship

1. Introduction

In past centuries, walls were constructed as shields against outside dangers, be it the Great Wall of China, which was constructed to prevent nomadic northern tribes from penetrating within, or the European castles, which were surrounded by high walls and moats to dismay robbers. The history and background of firewalls are examined to understand how they became widely deployed and how they can make organizations and household networks safer places [1]. Even the term "firewall" itself, is not very old. It originated in 1764 and was used to refer to structures that helped prevent fire from spreading to other buildings, steam-powered trains, etc. Firewalls were established as significant components of computer protection by the 1980s, even though they began as simple filtering devices on routers. In the modern world, there are advanced security systems that regulate traffic between networks according to set security standards [2]. The Next Generation Firewalls (NGFWs) have become an essential part of modern cybersecurity as they incorporate intrusion prevention, deep packet inspection, real-time threat intelligence, and cloud security [3]. This article will discuss the importance of firewall technology in Pakistan and how it is being experimented and implemented for its impacts on security and freedom of speech. It analyses the differences between cyber security and cyber censorship, evaluating whether the deployment of firewalls in Pakistan meets the country's security requirements or whether it is an attempt to regulate freedom of speech on the Internet. The key objectives that are covered in this article are as follows;

1. How firewalls protect against cyber threats, with a focus on Pakistan's digital security landscape.
2. Whether firewall testing in Pakistan is genuinely about cybersecurity or a means to restrict digital freedoms.

3. How firewall policies intersect with Pakistan's regulatory framework, including the Pakistan Electronic Crimes Act (PECA) 2016.

4. The financial and political costs of internet restrictions, and their impact on Pakistan's digital economy.

Through a thorough analysis of these objectives, this article will explore the dual role of firewalls as an important defence against cyber-attacks and a possible mechanism for the government's control over online expressions.

2. Role of Firewall in cyber security

When constructing the concept of a firewall with its historical development, it is impossible to overestimate its importance in modern cybersecurity [4]. Firewalls act as the primary barrier against cyber threats and prevent unauthorized access and unlawful activities on the network [5]. As the modes of cyber threats increase, today's firewalls have incorporated new functions like intrusion prevention, DPI, and threat intelligence in real-time. Such features not only recognize but also counteract threats that may emerge in the future. Among the new advances in the field of firewalls is the concept known as the next-generation firewall (NGFW). NGFWs enhance the features of traditional firewalls by integrating them with other security solutions such as application control, intrusion prevention, and cloud intelligence [6]. It enables the identification of threats more effectively and accurate prevention procedures that can respond to the challenges of the modern cyberspace environment flexibly.

2.1. National security perspective

From a national security perspective, firewalls perform an important function for a network as the first line of defence against cyber threats and unauthorized intrusions [7]. These are positioned as the first line of defence in a network and are constantly analyzing traffic and applying a set of pre-defined security rules to regulate the flow of incoming and outgoing traffic. Firewalls can effectively protect against complex attacks like DDoS attacks by blocking harmful traffic that tries to disrupt services [8]. They are also used to prevent such IP addresses from enjoying the loopholes in network services to gain access to sensitive configurations. Governments must protect sensitive information, like financial records, to keep taxpayers' data safe. They need to manage the risks related to information security effectively. Information security officers in the public sector face the ongoing challenge of limiting the damage from security breaches, protecting networks from threats, and ensuring the security of government systems. To meet these challenges, governments need to implement a sound logging and intrusion detection system and create network management frameworks that would secure internal and external risks. The Great Firewall of China, implemented in 2008, controls and censors the flow of data, making China one of the strictest countries in the world when it comes to internet freedom [9]. Even though it has been more than a decade and is still dynamic, the Great Firewall has been effectively preventing politically sensitive information and collective action. Nevertheless, it continues to enable the majority of Chinese Internet users to use social networks, entertainment, and some forms of news. On the other hand, the protests in Iran in the new millennium have depended a lot on the Internet for planning and information sharing. Banned Iranians have also relied on digital means to disseminate information to both international audiences as well as the internal Iranian population. However, the Iranian government knowing the dangers of the internet has come up with the National Information Network (NIN) [10]. The NIN aims to improve the interconnection and the management of communication domestically as well as internationally. It encapsulates the government's efforts to control information dissemination and still retain control over social media. North Korea has a very weak internet system, with Kwangmyong, the national intranet, available only to selected people. Nevertheless, North Korea has been actively promoting itself as a cyber-power on the level of such countries as the USA, China, Russia, Great Britain, Israel, and Iran. The country has ramped up its cyber capabilities, as seen by the Sony Pictures hack, the WannaCry attack, and the DarkSeoul attack, even though the government has denied its involvement in these incidents. Cybersecurity has been an issue of concern in the United States for many years, and cybercriminals have attacked different industries. From 2005 to 2015, the cyber security organization recorded over 12,000 cyber incidents, which included data security breaches and violations. By 2017, the U.S. Department of Defense (DoD) had to enhance its defences by using advanced firewalls to protect vital military data, this is due to the rising complexity of cyber threats [11]. In the same year, hackers targeted different systems by using different tools such as viruses, worms, Trojans, DoS, DDoS, ransomware, and SQL injection. These cyber exploits were put at $445 billion globally meaning that there is a need to step up the defence against cyber incidents [12]. Pakistan, like many other countries, has seen growth in online services and information technology in its organizations, thanks to support from higher authorities [13]. One of the leading driving forces in this regard is NADRA (National Database and Registration Authority) which is responsible for operating the centralized national identity database in Pakistan. This database is used in many sectors such as the banking sector, passport offices, the Election Commission, mobile companies, and even international agencies like the FBI. NADRA is the only organization that deals with the registration and collection of population data in the country [14]. Due to its enhanced level of technological adoption, NADRA has been named among the most efficient organizations in the world. A report by Threat Track Security (2014) revealed that NADRA is among the best organizations in terms of modern technologies for managing sensitive data. Similarly, the European countries have adopted the Security Content Automation Protocol (SCAP) algorithm for their National Vulnerability Database (NVD) [15]. This protocol makes vulnerability management, security measurement, and compliance to be automated, this is in line with the international trend of improved cybersecurity.

However, the issue of cybersecurity threats persists. Criminals have gone for the accounts, trying to steal personal details such as those belonging to institutions like NADRA. Such breaches have been witnessed by organizations such as Cybersecurity, Stanford, CA (USA) and Pro Pakistani (2013). Since NADRA holds very sensitive national data, it is possible that it could fall prey to cyber terrorism, which would aim at either incapacitating the services offered by NADRA, corrupting human confidential information, or using the data for other wrong purposes. Pakistan being a developing country is in the stage of integrating cyber services throughout different fields. With this development, the protection of information from third parties has become of paramount importance in organizations. One of the issues is the appearance of social sites as websites that allow users to freely communicate and share information with friends. However, these platforms have turned into the most vulnerable to cybercriminals who seek to get unauthorized access to users' data with their places of residence. With these platforms becoming more popular, it becomes important to keep user data safe from cyber criminals to retain consumer confidence and uphold personal privacy.

Pakistan has accepted the emerging real dangers of cybercrimes and has developed several institutional structures to support its cybersecurity programs. Among these are the Pakistan Computer Emergency Response Team (Pak CERT), the Pakistan Infor-

mation Security Association, and the Computer Emergency Response Team (PISA-CERT) [16]. These teams are part of a worldwide trend where CERTs (Computer Emergency Readiness Teams) and CSIRTs (Computer Security Incident Response Teams) are established in both the government and business to address cyber threats and manage cybersecurity. While CERTs and CSIRTs deal with cybersecurity problems, they are different in some aspects. CERT is a trademark term referring to the intelligence of cyber threats, people who identify, secure, prevent, and mitigate threats. CSIRT on the other hand is a cross-functional team that offers legal and technical remedy. CERTs are especially oriented to national threats affecting critical infrastructures, the economy, national security, and DoS attacks. Pakistan has created the 'Pakistan Research Centre' under the Senate Defense Committee's Cyber Security Task Force to improve its cybersecurity and protect its cyberspace. In the same year, May 2018 to be specific, Pakistan established the National Centre of Cyber Security (NCCS) at Air University Islamabad to improve the country's cybersecurity systems [17]. Further, to deal with technological abuse in Pakistan, the Federal Investigation Agency (FIA) framed the National Response Centre for Cyber Crime (NR3C) in 2007. NR3C provides services including network forensics, technical training, and handling of computers, videos, mobile, and many other cybercrimes [18].

Despite these efforts, NR3C still faces limitations in preventing cybercrimes and addressing cyber offences due to a lack of capacity. However, the legal framework of cybercrimes in Pakistan has been established in the Pakistan Electronic Crimes Act (PECA) 2016, and it also lacks a strategic approach towards cybersecurity and its enforcement is still in progress [13, 18]. Cyber security in Pakistan is gradually emerging as a critical problem due to rising threats of cyber-criminal activities, cyber warfare, and terrorist activities. These challenges pose a threat to national security given the fact that main infrastructures and governmental and private sectors are at high risk[4]. The weakness is caused by several factors: old hardware and software, lack of training, and unawareness of threats. To this, one can add the fact that modern terrorist organizations have started using the Internet to perform their crimes, which adds to the challenges facing the country's security forces [19]. The government has introduced several steps to counter these important issues like the formation of cybersecurity response teams and laws like the Pakistan Electronic Crimes Act (PECA). However, these efforts are still inadequate as the threats in cyberspace continue to surge. There is a high demand for a strong and effective cybersecurity system to protect national interests. The only sustainable way forward is for the public and the private sectors to work more closely together. This would ensure that resources, expertise, and intelligence could be shared effectively to deal with cyber threats. Moreover, international cooperation should be improved when it comes to creating measures that affect global cybercrimes [20, 21]. Pakistan also needs to invest in technologies that can identify and counter cyber threats before they occur. The formulation of a national cybersecurity strategy that will be on par with international standards will be a central factor in the attainment of long-term cybersecurity.

2.2. Freedom of Expression

In the past decade, predominantly in the last few years, the internet has emerged as a major source of disseminating information and fighting media restrictions imposed by the authorities. This expansion can be directly attributed to the ever-growing internet users around the world. There are over two billion unique internet users today, more than doubling in the past five years. This shows how important online communication has become. The Internet is now a major means by which people communicate, obtain information, socialize, and even transact business, and governments have sought ways and means of regulating and, in some instances, controlling this important medium [22, 23]. This shift in policy has taken many forms such as website blocking and content filtering, manipulation of content, cyber-attacks, and the harassment of bloggers many of whom have been imprisoned for their online activities.

3. Legal and Policy Framework in Pakistan

3.1. The Prevention of Electronic Crimes Act (PECA) 2016 and Its Impact on Internet Freedom in Pakistan

Most of the offline human activities have gone online due to information and communication technology, which has resulted in high usage of the internet, including Pakistan. The increasing rate of cybercrimes led Pakistan to pass the PECA 2016 to prevent malicious activities through the internet [24]. However, when compared to similar cybercrime legislation in other countries, people have pointed out that PECA has stricter penalties and contains provisions that outlaw activities that are not considered unlawful in other countries. PECA, effective from August 16, 2016, is one of the most debated laws in Pakistan, especially with freedom of speech. Many civil society groups, opposition parties, and international human rights organizations have criticized this as overly harsh, flawed, and problematic. The law has raised specific uncertainties over its effects on freedom of speech on the internet in Pakistan.

3.2. Sections 3 and 4: Vague Terminology and Due Process Issues

The new penalties are introduced in sections 3 and 4 of PECA for unauthorized access to data and information without proper permission. According to Section 3, any person who accesses data or information systems for a dishonest purpose is liable to imprisonment for a term that may extend to three months, or a fine that may extend to fifty thousand rupees or both. Section 4 also forbids copying or transmitting data without permission and prescribes imprisonment (up to 6 months) and/or a fine of up to one hundred thousand rupees [25]. However, these sections use terms like dishonest intention, information system, unauthorized access, and transmission of information, and that raises many issues about due process. That is why the law that defines crimes in rather vague terms can lead to a situation when the very right to free speech is limited. In the U.S., courts pay special attention to vague laws, especially those related to the First Amendment. The U.S. Supreme Court stated in Connally v. General Construction Co. that a law is unconstitutional if an average person cannot easily understand its meaning. Likewise, the vagueness of provisions in PECA can lead to denial of due process, which in turn affects freedom of speech and expression for civil society activists, opposition politicians, journalists, and the common person who uses social media.

3.3. Sections 11 and 37: Hate Speech and Content Removal

PECA also talks about hate speech and content removal provisions. Section 11 prescribes a maximum of seven years imprisonment and or a fine for anyone who circulates information on media that incites sectarianism, inter-faith, or racial [25]. Under section 37 of the law, access to published content can be restricted or blocked by authorities if it is necessary for the national security, public order, morality, or defence of Pakistan or if it is considered as 'offensive' under the PECA [26]. As in Sections 3 and 4, these provisions are also ambiguous, and such terms as 'dissemination of information," 'hatred' and 'public order' are vague. These sections are too broad and allow authorities to censor content without specific stipulations and engulf important concerns of censorship of

free speech. Lacking proper protection measures to prevent the elimination of the posted information, these provisions can become instruments of oppression in the hands of administrators and regulators, limiting the rights of the people to share their opinions on the Internet.

3.4. Effect on Democracy and Human Rights

The vagueness of PECA and its wide-ranging provisions are problematic for rights that form the very basis of civil liberties such as the right to free speech. Owing to the availability of ambiguous and broad terms within the law, those in support of democratic changes, free access to information, and human rights may be suppressed or punished. The law's adverse effect on freedom of speech and expression, freedom of information, and academic freedom threatens democracy and the promotion of human rights in Pakistan.

3.5. Financial Impact of Pakistan's Internet Restrictions

As Pakistan's government attempts to gain greater control over its cyber sphere through the new national internet firewall, this move is not without monetary implications. In 2024, Pakistan had the highest financial loss from internet restrictions at $1.62 billion, more than Sudan and Myanmar, which are in civil wars. Asia was the hardest-hit region, with major losses in Pakistan, Myanmar, Bangladesh, and India due to these restrictions. These four countries are among the six most affected nations in 2024 proving that internet censorship has profound economic impacts. The financial cost is a clear indication of the current and future economic implications of internet blackouts and restrictions to freedom of access to the internet.

4. Global Approaches to Regulating Online Content

Different countries have unclear definitions of illegal content, leading to various regulation approaches. The United States (US) and China can be viewed as the two extremes in terms of approach to the regulation of content shared online. While the US has relatively liberal policies that restrict freedom of speech on social media to a limited extent, China thoroughly regulates the usage of the internet. Between these two poles, there are such states and actors as India, the European Union, Great Britain, Germany, etc., each of which is designing its model of content regulation as the balance between freedom, security, and governance.

4.1. Basic Provisions of the ICCPR on Freedom of Speech

Article 19: Freedom of Expression

Article 19 affirms freedom of expression, which includes the freedom to obtain, receive, and impart information [26]. However, it also allows for restrictions, provided that:

1. Law provides such restrictions and it has to be ensured that the restriction is clear, easily understandable, and unambiguous so that it cannot be used arbitrarily against any person.
2. They aim at a legitimate interest of the state, for instance, national security, public order, public health, or morals.
3. They satisfy the necessity and proportionality test whereby the measures adopted are the least intrusive and are proportionate to the stated aims without unreasonably jeopardizing freedom of expression.

Article 20: Prohibition of Certain Forms of Expression

In contrast to Article 19, which permits certain limitations, Article 20 obligates states to prohibit specific forms of expression:

1. Promoting national, racial, or religious enmity leads to discrimination, hostility, or violence. This provision works in conjunction with Article 19 since it deals with expressions that are likely to incite violence and infringe on the dignity of individuals. However, there are still concerns about which direction the human rights protection is taking, nevertheless, the development of the rights in peace, security, and justice for all people in the world is the most powerful tool [27].

4.2 Freedom of Expression in States of Emergency (Article 4, ICCPR)

Article 4 of the ICCPR allows states to derogate from some rights, including freedom of expression, during a State of Emergency [27]. This is allowed only under specific conditions:

1. *Existence of a Public Emergency:* Some situations must indeed be about the nation's life.
2. *Strict Necessity:* This must be the case with the measures taken.
3. *Non-Discrimination:* These measures may not be based on race, colour, sex, language, religion, or social origin.
4. *Proportionality:* Derogations must be no wider in scope and no longer in duration than is necessary for the emergency.

The Siracusa principles also help to guide and ensure that derogations do not go beyond the bounds of necessity and do not become a pretext for trampling dissent and rights arbitrary.

4.2. Ensuring Balance: Safeguards and Mechanisms

Striking a balance between national security and freedom of expression requires:

1. *Legal Clarity:* Speech regulation laws must be narrowly drawn and should refer only to clear and present dangers of breach of the peace, and should not be overly broad or vague to suppress dissent.
2. *Independent Oversight:* Restrictions must be applied through mechanisms such as judicial review or independent monitoring bodies, which should ensure their application and prevent abuses.
3. *Proportionality Assessments:* Restrictions on expression must be the least intrusive means to address security concerns and proportionate to the threat posed, and states must prove that.
4. *Transparency and Accountability:* Transparency in decisions taken by governments should be provided, rationale for restrictions should be disclosed, and governments should engage with civil society to protect public trust.
5. *Regular Reviews and Sunset Clauses:* Periodic review is required of temporary restrictions, and in particular of those implemented in states of emergency, to be sure that they are proportionate and necessary. Restrictions can be sunsetted when the emergency has ended.

Guiding principles exist as to what a country would need to do when deploying surveillance technologies. The voluntary and non-legally binding principles seek to show how governments can meet their commitments to democratic values, human rights, and fundamental freedoms, as required under their international obligations and commitments. In three areas of concern, the principles are designed to guard against the misuse of surveillance technologies by governments and their agents. Still, in recent decades, technological progress has been progressing, especially due to the exponential growth of Internet connectivity, and the world has been receiving enormous benefits from it. If used responsibly and by international law, surveillance technologies are an important tool to protect national security, public safety, and critical infrastructure and facilitate criminal investigations [28, 29]. Similarly, conducting complex investigations calls for advanced technological equipment consisting of forensic software, advanced data analysis tools, and high-tech equipment [30, 31]. If a country lacks these technological resources, it may not be able to conduct investigations efficiently, which could make it less complicated for organized crime to thrive. These technologies go so far as to further ensure that people can

continue to exercise their rights and liberties. Surveillance technologies are used responsibly to improve safety and security while complying with the rule of law. As these technologies develop, governments must take steps to make sure these technologies are used lawfully and responsibly, and that they include appropriate information safeguards to regulate the collection, handling, and disclosure of information collected through their use. The effectiveness of these protections is essential to the protection of individual privacy, personal data, and human rights, and to promoting transparency, accountability, and civic participation, all while we continue to pursue legitimate objectives, including law enforcement, public safety, and national security.

The legislation defines and regulates a wide range of tools as *'surveillance technologies'*. These technologies include products or services that are used to detect, collect, exploit, intercept, monitor, preserve, process, analyze invasively observe, or retain sensitive data, personally identifiable information (including biometric data), and communications regarding individuals or [32, 33]. These technologies can, of course, be lawfully used, but the misuse of these technologies by governments remains a major concern. The guiding principles address how surveillance technologies are to be used in three particular areas of concern. It should be stressed that these principles are not to apply to activities not in these listed areas. Governments to unjustifiably interrupt freedom of expression, discourage human rights and fundamental freedoms, or enable technology-based gendered violence or discrimination, online or offline must not use surveillance technologies. They also must not perpetuate harmful or discriminatory norms or stereotypes, or undermine bodily autonomy by unlawful collection or misuse of personal health data, including reproductive and sexual data, or by the dissemination of intimate images. These guiding principles are a set of common practices and standards, with variations in implementation based on national legal frameworks and systems. Other nations may have more entrenched safeguards, indeed more robust safeguards that show even stronger commitments to these principles. In summary, it emphasizes the need for lawful and responsible use of surveillance technologies to avoid harm and uphold human rights and freedoms.

5. Critical Analysis

The recent amendment to the Prevention of Electronic Crimes Act (PECA) 2025, which was approved by the National Assembly while this article was being written, makes it even more important to analyze Pakistan's firewall technology and how it affects freedom of expression and national security. The amendment makes it a crime to share *false and fake information*, with penalties of up to three years in prison and fines. This further limits online dissent. This development strengthens the case that Pakistan's firewall policies are not only about protecting cybersecurity but also about tightening the wheels over digital spaces in the name of national security. The consideration that a crucial provision has passed without discussion from the public seems to be a most serious concern for its legitimacy and purpose. Given that it happens at a time when states are taking control of online platforms, and social media censorship, the timing of this amendment is significant. Already, Pakistan has been actively blocking websites, restricting VPNs and digital blackouts, and now, with the formation of the Social Media Regulation and Protection Authority, the state will have even greater powers to remove content at will. They limit online freedom and raise worries that Pakistan is moving toward a system of internet control like China's. The new law is so ambiguous that this means any critical voice, journalists, opposition figures, activists; or even ordinary citizens will now be tried in a criminal court for *spreading false information*. It continued in a pattern of the use of cybersecurity laws by the government to stifle political opposition rather than attack misinformation.

This amendment has implications far deeper than legal overreach. It is an attack on Pakistan's digital economy and democratic participation. Public discourse, political mobilization, and economic opportunities, especially for freelancers, startups, and online businesses, have become a space on social media platforms. The blanket bans and higher censorship measures are bad for investors in the tech sector who are pushed into a hostile environment for digital entrepreneurship and global partnerships. Even before the beginning of the current block on X (formerly Twitter) in February 2024, it has already indicated how the state will control the narratives by shutting down those platforms that allow unrestricted discussions. It is worth noting that as these restrictions had already cost Pakistan $1.62 billion in financial terms in 2024, their financial cost will only skyrocket even further, hindering the country's digital future. This amendment exposes a fundamental contradiction: Meanwhile, Pakistan says it is building its cybersecurity infrastructure, but it is simultaneously undermining digital freedoms and economic opportunities. National security laws are based on the logic that they should promote public safety with adequate respect to fundamental rights, yet PECA 2025 puts state prerogative above public empowerment. But it also lacks judicial oversight and independent accountability mechanisms, leaving the government free to regulate, block, and punish online speech arbitrarily defined as *fake information*. In addition to these repressive digital policies, a more recently proposed law the Digital Nation Pakistan Bill ensures these intrusive surveillance technologies with no human rights protections. These developments beg the question: What is Pakistan's digital future, will it be one of security or suppression? And if these trends hold, Pakistan will not be remembered for its cybersecurity progress, but rather for its cyber censorship and human rights abuses. The remedy is not in changing laws to limit freedom, but in changing cybersecurity laws to strike a balance between national security and fundamental rights. The government must immediately withdraw PECA 2025 and begin a sincere dialogue with civil society, digital rights activists, and legal experts before legislating against cyber threats turns into weapons laws against dissent. Firewall technology should be employed to counter the external cyber threat to Pakistan and not be utilized as an internal tool for silencing opposition. Continuing on this path, Pakistan will ultimately cut itself from the global digital economy, isolate its youth, and force independent thinkers into self-censored or exiled. Pakistan faces a serious risk of a controlled and stagnant digital future if action is not taken. Reform is urgently needed.

6. Conclusion

The debate surrounding firewall technology in Pakistan is no longer just about cybersecurity, it has evolved into a critical human rights and governance issue. Firewalls are important for protecting national security, blocking cyberattacks, and safeguarding sensitive data, yet the growing use of such controls as weapons of digital censorship is cause for grave concern. Pakistan's way of setting up firewalls shows a concerning trend of controlling information, where national security is used to limit online freedom. While this article was being written, the amendment to PECA 2025 further solidified these concerns by allowing the state to even more heavily police dissent under the guise of *spreading false information*, in completely ambiguous ways. The growing digital control has economic and political implications. Internet restrictions have already cost Pakistan billions and the financial cost of internet restrictions threatens Pakistan's emerging digital economy, deters foreign investment, and disrupts online businesses. Meanwhile, political censorship through firewalls and social media regulations is undermin-

ing democracy by silencing activists, journalists, and opposition voices. If these trends persist, Pakistan risks being left behind in the global digital sphere, where unrestricted access to information is a major factor in the country's economic and technological development. It is still possible for a balanced approach. If these policies are transparent, legally justified and proportional to the level of security threats, then firewall technology can be used without suppressing free speech. The firewall testing and implementation in Pakistan must be under clear regulations, independent oversight, and judicial accountability. It is also important that cybersecurity laws be reformed through a consultative process with digital rights organizations, legal experts, and civil society to avoid their misuse of political control. Ultimately, it will be Pakistan's choice between security and repression that will determine its future as a digital-free country, an economically progressive country, and a democratic stable one. An open and secure internet is not a contradiction; it is imperative for a modern, progressive Pakistan.

Reference

1. Broderick, J.S., *Firewalls–Are they enough protection for current networks?* Information Security Technical Report, 2005. **10**(4): p. 204-212.
2. Afzal, J., et al., *Review ofVarious Aspects of Digital Violence.* 2024.
3. Ahmadi, S., *Next generation ai-based firewalls: a comparative study.* International Journal of Computer (IJC), 2023. **49**(1): p. 245-262.
4. Afzal, J., *Implementation of digital law as a legal tool in the current digital Era*. 2024, Springer.
5. Vacca, J.R. and S. Ellis, *Firewalls: jumpstart for network and systems administrators*. 2004: Elsevier.
6. Sharma, H., *Next-Generation Firewall in the Cloud: Advanced Firewall Solutions to the Cloud.* ESP Journal of Engineering & Technology Advancements (ESP-JETA), 2021. **1**(1): p. 98-111.
7. Naseer, I., *Implementation of Hybrid Mesh firewall and its future impacts on Enhancement of cyber security.* 2020.
8. Chatterjee, K., *Design and development of a framework to mitigate dos/ddos attacks using iptables firewall.* International Journal of Computer Science, 2013.
9. Chandel, S., et al. *The golden shield project of china: A decade later—an in-depth study of the great firewall*. in *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*. 2019. IEEE.
10. Aryan, S., H. Aryan, and J.A. Halderman. *Internet censorship in Iran: A first look*. in *3rd USENIX Workshop on Free and Open Communications on the Internet (FOCI 13)*. 2013.
11. Logan, B.E., *A CASE FOR SOFTWARE-DEFINED NETWORKING IN THE UNITED STATES MARINE CORPS: AUTOMATING DISTRIBUTED FIREWALLS*. 2019, Monterey, CA; Naval Postgraduate School.
12. Gangwar, S. and V. Narang, *A survey on emerging cyber crimes and their impact worldwide*, in *Research Anthology on Combating Cyber-Aggression and Online Negativity*. 2022, IGI Global Scientific Publishing. p. 1583-1595.
13. Afzal, J. and C. Yongmei, *Federal and provincial legislation regarding 'Right to Information'for good governance in Pakistan.* Discover Global Society, 2023. **1**(1): p. 12.
14. Alam, S., *Successful organization change at national database and registration authority (NADRA) Pakistan: a case study.* Global Management Journal for Academic & Corporate Studies, 2013. **3**(1): p. 166-175.
15. Niemi, K., *Engaging security into product development by using baseline security configuration for operating systems.* 2024.
16. Masudi, J.A. and N. Mustafa, *Cyber security and data privacy law in Pakistan: Protecting information and privacy in the digital age.* Pakistan Journal of International Affairs, 2023. **6**(3).
17. Khan, M.F., A. Raza, and N. Naseer, *Cyber security and challenges faced by Pakistan.* Pakistan Journal of International Affairs, 2021. **4**(4).
18. Saleem, B., et al., *A survey of cybersecurity laws, regulations, and policies in technologically advanced nations: A case study of Pakistan to bridge the gap.* International Cybersecurity Law Review, 2024. **5**(4): p. 533-561.
19. Afzal, J., *An Overview of Digital Law*, in *Implementation of Digital Law as a Legal Tool in the Current Digital Era*, J. Afzal, Editor. 2024, Springer Nature Singapore: Singapore. p. 1-21.
20. Afzal, J., *Legal Challenges Regarding Digital Operations*, in *Implementation of Digital Law as a Legal Tool in the Current Digital Era*, J. Afzal, Editor. 2024, Springer Nature Singapore: Singapore. p. 23-45.
21. Haider, A., S. Raza, and B.Z. Khan, *Organized Crime and the Objectives of the Islamic Penal System.* Al-Qamar, 2023. **6**: p. 63-82.
22. Afzal, J., *Digital Law Enforcement Challenges and Improvement*, in *Implementation of Digital Law as a Legal Tool in the Current Digital Era*, J. Afzal, Editor. 2024, Springer Nature Singapore: Singapore. p. 47-78.
23. Castells, M., *The Internet galaxy: Reflections on the Internet, business, and society*. 2002: Oxford University Press.
24. Yongmei, C. and J. Afzal, *Impact of enactment of 'the prevention of electronic crimes act, 2016'as legal support in Pakistan.* Academy of Education and Social Sciences Review, 2023. **3**(2): p. 203-212.
25. Ahmad, A.A.M.D.A., *Deficiencies In peca and proposed amendments to facilitate investigating agencies, courts and prosecution; proper use of electronic devices for effective implementation of law.* International Journal for Electronic Crime Investigation, 2019. **3**(3): p. 6-6.
26. Daudpota, F., *An Examination of Unconstitutional Aspects of Pakistan's Cybercrime Law.* Available at SSRN 2860954, 2016.
27. Haider, A., I. Ahmad, and M. Yaseen, *Jus Cogens and the Right to Self-Determination: A Study of its Peremptory Status and Erga Omnes Effects.* Pakistan JL Analysis & Wisdom, 2024. **3**: p. 59.
28. Afzal, J., *Digital Evidence and Permissibility in Court of Law*, in *Implementation of Digital Law as a Legal Tool in the Current Digital Era*, J. Afzal, Editor. 2024, Springer Nature Singapore: Singapore. p. 121-137.
29. Haider, A., *Application of the United Nation Convention against Transnational Organized Crime: An Analysis.* Available at SSRN 4686710, 2024.
30. Afzal, J., *Best Practice of Digital Laws and Digital Justice*, in *Implementation of Digital Law as a Legal Tool in the Current Digital Era*, J. Afzal, Editor. 2024, Springer Nature Singapore: Singapore. p. 95-120.
31. Haider, A., A. Ali, and B. Zeb, *Broken Laws, Broken Lives: When Organized Crime Shreds Human Rights.* 2024.
32. Afzal, J., *Future of Legal Tools and Justice*, in *Implementation of Digital Law as a Legal Tool in the Current Digital Era*, J. Afzal, Editor. 2024, Springer Nature Singapore: Singapore. p. 155-177.
33. Hosein, G. and C.W. Palow, *Modern safeguards for modern surveillance: An analysis of innovations in communications surveillance techniques.* Ohio St. LJ, 2013. **74**: p. 1071.