The Lighthouse Journal of Social Sciences, Vol. 04, Issue 1, Summer 2025, pp. 85-94

Balancing Internet Freedom and National Security in Pakistan: A Case of Censorship and Cybersecurity

Shahid Akbar[1], Robina Khan[2], Zafar Abbas[3]

ABSTRACT

This article aims to examine the cybersecurity and censorship policies in Pakistan and their impact on internet freedom. It also seeks to analyse the tactics for achieving a harmonious balance between online freedom and security. The emergence of the internet has brought out several challenges for contemporary society, including the need to strike an appropriate balance between the liberties afforded by the virtual world and the risks posed by cybersecurity. The Pakistani government has enacted censorship legislation to regulate online material in order to protect against cybercrimes, promote social ethics, and ensure national security. Nevertheless, these limitations pose a potential threat to individuals' digital rights. This study concludes that achieving a delicate balance between internet freedom and national security in Pakistan is a multifaceted but important undertaking.

Keywords: *Cybersecurity, Cybercrimes, Censorship, Internet Freedom, National Security*

INTRODUCTION

The rapid advancement of digital technology has completely transformed the world. The advent of digital technology has revolutionized civilizations, facilitating seamless worldwide interactions. The internet is an essential instrument for facilitating communication and enabling self-expression. However, the internet revolution has presented several obstacles for civilized communities, such as the task of effectively managing the balance between online freedom and the hazards posed by cybersecurity (Rehmat & Alam, 2018). The concept of internet freedom in Pakistan is quite intricate. The Pakistani government has implemented censorship regulations to oversee internet content with the aim of safeguarding against cybercrimes, upholding societal decency, and ensuring national security (Jamil, 2021).

The Pakistani government claims that its censorship laws aim to protect citizens from cyber threats and harmful content. However, these rules pose a risk to the digital rights of individuals (Jamil, 2021). The surge in cybercrime is also a cause for alarm. Cybercrimes in

[1] MPhil in Political Science, Qurtuba University, Dera Ismail Khan, Khyber Pakhtunkhwa.

[2] Assistant Professor, Department of Political Science, Gomal University, Dera Ismail Khan Khyber Pakhtunkhwa. **Corresponding Author's Email: dr.robina@gu.edu.pk**

[3] Assistant Professor, Department of Political Science, Government College No.1 Dera Ismail Khan Khyber Pakhtunkhwa

Manuscript Submitted: April 10, 2025
Manuscript Accepted: June 15, 2025

Pakistan have seen a substantial increase. The offences include cyberbullying, internet fraud, and hacking, among others (Abbas & Zubair, 2020). The government argues that implementing cyber laws and censorship is essential to mitigating the hazards associated with cybercrime. Furthermore, enacting digital regulatory legislation is critical for maintaining national security. Nevertheless, it is imperative and essential to establish a harmonious balance between these measures and the potential infringement of basic digital rights.

THEORETICAL FRAMEWORK

Cyberspace is a digital reality that is borderless and timeless. Often referred to as a “consensual hallucination”, cyberspace enables individuals to share their ideas and perspectives through a global network of connections. The communication platform is considered innovative and has led to the emergence of a “network society” (Castells, 2009). In the 1990s, the word “cyberspace” became closely associated with the Internet and the World Wide Web. People sometimes refer to cyberspace in this way when discussing its potential for censorship (Peteva, 2020). Therefore, throughout our discussions, we tend to favour the phrase “Internet censorship” instead.

Over the last two decades, the concepts of "Net Utopians" regarding the Internet's resistance to censorship have evolved and proven inadequate in the face of current, more stringent measures. It is possible to examine the concept of Internet censorship within the context of the libertarianism/paternalism discourse (Jewkes & Yvonne, 2010). As Spinello (2002) points out, the beginnings of cyberspace are decidedly libertarian. They advocate for the classical liberal ideals that Mill accepted, and as a result, they promote an Internet that is free from censorship. A paternalistic approach, on the other hand, may support censorship since it seeks to avert possible damage, which in turn justifies further government interference, surveillance, and limits on free speech. The fact that the Internet is not fully immune to censorship is a truth that cannot be denied, regardless of one's point of view. This has been proved in a range of scenarios using a large number of different strategies.

National Security Concerns in Digital Age

Cybercrimes in Pakistan

The term "cybercrime" is commonly used in a broad meaning by individuals. Cybercrime refers to the commission of a criminal act using a digital device, such as a computer, and the internet. It is important to note that according to Munir and Gondal (2017), this kind of criminal activity does not need the perpetrator to be physically present at the location where the crime was committed. Using the internet, 3G/4G technology, and information and communication technologies (ICTs), Pakistan is making attempts to advance in both the public and private sectors of the economy. The fast growth of technology poses a significant danger to developing countries, as it threatens not only individuals and businesses but also the country itself from cybercrimes. This problem is especially prevalent in emerging nations. Unfortunately, Pakistan is not one of the countries that is immune to the prevalence of cybercrimes (Zahoor & Raz, 2020).

An accurate understanding of cybercrime is crucial. According to Barn and Barn (2016), the lack of comprehensive definitions and categorisation systems that may cover the many different varieties of cybercrime is one of the probable reasons for the difficulties that are encountered when attempting to estimate what constitutes cybercrime. According to Black et al. (2019), the lack of systematic and uniform cybercrime legislation across various jurisdictions worsens this problem. There has been an increase in the number of cybercrimes in Pakistan, which has created complicated problems for individuals, businesses, and government authorities. Criminals operating online are aiming their attacks against the information infrastructure. According to Abbas et al. (2023), the most common types of cybercrime are hacking, phishing, identity theft, online fraud, and cyberbullying. According to Shahzad (2023), the growing number of cybercrimes provides more evidence of the vulnerabilities that are present in Pakistan's digital infrastructure and drives home the importance of implementing comprehensive cybersecurity measures.

Cybersecurity Measure

With the advent of the digital era, the incidence of cybercrime is growing at an alarming rate (Ekwonwune et al., 2024). Given the increasing danger of cybercrime that Pakistan is now facing, the cybercrime legislation in Pakistan encompasses offenses such as cyberterrorism, online theft, and online fraud, all of which include the use of electronic devices. For the purpose of addressing cybersecurity concerns, several cyber laws have been implemented from the year 2002 and even earlier (Rehmat & Alam, 2018).

In order to successfully address cybercrimes, Pakistan has built a comprehensive regulatory framework. According to Hamdani (2014), the Electronic Transaction Ordinance (ETO) of 2002 was passed by the government of Pakistan with the purpose of recognising and simplifying the use of electronic papers, records, information, communications, and transactions. The expansion of the media sector was significantly aided by the passage of the Pakistan Electronic Media Regulatory Authority (PEMRA) Ordinance in the year 2002. In addition, the government passed a number of other laws pertaining to the media, such as the Press Council Ordinance of 2002, the Defamation Ordinance of 2002, and the Press, Newspaper, News Agencies, and Books Registration Ordinance of 2002. Additionally, the Newspaper Employees (Conditions of Service) Act of 1973 was also in force during this time period (Gul, 2017).

In Pakistan, the Electronic Crime Act (ECA)-2004 was first presented to the public by the Ministry of Information Technology in the year 2004. This law was built on the framework of the ETO-2002, but with certain alterations brought about by the legislation. Several new terminology were incorporated in the Electronic Communications Act of 2004, including "electronic theft," "unauthorised entry," "cyber-terrorism," "systems," and "data damage." In essence, the primary purpose of this Act was to provide legal protections for actions that were implemented with the intention of combatting cybercrime. The Prevention of Electronic Crimes Ordinance (PECO 2007) was enacted in Pakistan in 2007 with the purpose of addressing the problem of cybercrime (Daily Dawn, 2009). Notable is the fact that Pakistan had the aim of enacting cyber-law legislation under the name PECO-2007. This is something that should be taken into consideration. This piece of law addressed the penalties that are imposed for electronic fraud, falsification, data manipulation, cyberstalking, spoofing, and spamming. Politics was the impetus for some elements of society's criticism of this legislation, which they believed stifled debate. In November of 2009, the statement was ruled null and void as a result of the efforts of critics and members of civil society (Zafar & Ahmad, 2011).

PECA-2016, which stands for the Prevention of Electronic Crimes Act, was signed into law by the President of Pakistan on August 18, 2016. Legislation was passed that required the control, monitoring, and punishment of communications that took place on the internet. The Act covers a broad variety of offences, such as the transfer of data without authorisation, the illegal copying of data, and the unauthorised entrance into an information system. This Act provides severe penalties for any unauthorised access or manipulation of data or computer networks related with vital infrastructure. These sanctions include a wide range of punishments. In accordance with the provisions of the PECA-2016, individuals who engage in actions connected to terrorism, including as planning, recruitment, and fundraising for terrorist acts using new media, are subject to disciplinary action (LOC, 2016). Due to issues over the definition and identification of cybercrime, several aspects of the PECA-2016 legislative process were met with intense criticism from human rights groups on both the national and international levels. Concern was expressed by the United Nations Special Rapporteur on Freedom of Expression, who suggested conducting an exhaustive and all-encompassing evaluation of the Act, which should include ensuring that it adheres to international human rights standards. There have been several international human rights organisations who have voiced their disapproval of the PECA-2016 due to its excessive harshness, citing it as a breach of both freedom of speech and privacy (Privacy International, 2017).

Internet Freedom

Prior to the advent of the Internet, academics provided an explanation of the difference between good and bad freedoms provided by the Internet. Picard (1985) distinguished between two separate sorts of press freedom: negative press freedom, which refers to freedom from censorship, and positive press freedom, which relates to the public's ability to use the media. Both types of press freedom are fundamentally different from one another. There is a beneficial alignment between the conceptual framework and the human rights viewpoint on Internet freedom. The conceptual framework incorporates both positive and negative elements of Internet freedom. According to this perspective, international human rights norms are pertinent to the freedom of thought and expression that is available on the internet (Shen, 2017).

The concepts that promote the freedom of the internet are outlined in documents such as the Universal Declaration of Human Rights (UDHR), which declares the right to receive and distribute information without interference as an inherent and non-negotiable right. Platforms for social media have evolved as essential tools that enable people all over the globe to freely express themselves, participate in conversation, and share information, perspectives, and news with one another while also facilitating communication. Platforms dedicated to social media have made it easier for people to communicate with one another and organise themselves for a wide variety of causes, including political and social initiatives. A significant portion of the transmission of ideas and the gathering of information took place via traditional media platforms such as newspapers, radio, and television prior to the arrival of social media. Nevertheless, over the course of the last ten years, social media platforms have built a worldwide platform that allows users to actively seek, gather, receive, and transmit a wide variety of material. In the past, governments lacked the ability to restrict content disseminated via social media. However, they have since taken steps to regulate social media platforms and enforce censorship regulations (Tambini, 2021).

Not everyone embraces the Internet's capacity to enhance freedom of speech. Social media are subject to far stricter regulations in several nations. Nations such as China, Cuba, Iran, Syria, Turkey, and Vietnam systematically restrict access to social media platforms and suppress online content via censorship measures. In China, the government enforces strict internet censorship via the “Great Firewall of China” and keyword filtering. This leads to the online prohibition of a significant number of phrases and a severe restriction on the nation's freedom of speech.

Censorship Policies and its Effects

Access to the internet may be restricted by governments via various methods, including the banning of websites, the filtering of material, and the monitoring of online activities. The protection of national security and the limitation of access to potentially harmful content, such as pornography or hate speech, are only two of the many reasons why governments use internet censorship. Although there are a number of people who argue that internet filtering is necessary for preserving the harmony of society and protecting the well-being of individuals, there are also some who argue that it is a violation of the basic right to freedom of speech and expression. The censorship of the internet may take place in two different ways: A practice known as "top-down censorship" is one in which a government or organisation has the authority to direct service providers as to which content should be blocked. It is possible that some pieces of content might be subject to censorship if certain conditions are met. It is not possible for users to use their judgement in deciding which material to access since they do not have any autonomy in this area. The term "self-imposed censorship" refers to the practice of individuals or organisations deliberately filtering themselves by choosing which content to avoid.

Censorship of the media is a pervasive problem that has had an effect on many sources of information for a significant amount of time. It is possible that the necessity to maintain a well-organised society is the root cause of censorship. The fundamental purpose behind censorship is to prevent the general population from gaining access to information that may potentially threaten those in positions of authority. Due to the fact that the present global Internet connection makes it possible to send information across international boundaries in a short amount of time, an increasing number of people who consume media are becoming more dependent on the Internet for a wide variety of information. The Pakistani government relies on a robust Internet monitoring system to ban websites and selectively filter content, restricting access to only approved news sources (Abbasi & Al-Sharqi, 2015).

The government uses censorship to formally regulate and suppress any speech that threatens its stability. People have used censorship throughout history to oversee societal ethics, regulate public consciousness, and suppress dissent. Socrates, condemned to death in 399 BC for his recognition of unconventional deities, was among the first victims of censorship (Newth, 2010). In theory, the recent technological improvements pose significant challenges, or possibly render it unfeasible, to impose limitations on the accessibility of information for Internet users. On the other hand, the emergence of journalism on the Internet led to the development of digital censorship, which included methods such as filtering, blocking, hacking, and redirecting. In spite of this, the government of Pakistan has come into possession of cutting-edge technology that enables it to regulate the flow of information and monitor the content of the internet.

The desire to maintain a well-regulated society often motivates censorship in Pakistan. Censorship is a common occurrence worldwide. The implementation of censorship serves the purpose of preserving social order. Government organizations, like the PTA, have a crucial role in implementing censorship measures (Abbasi & Al-Sharqi, 2015). The government often restricts access to websites and internet services due to security concerns, therefore infringing upon digital rights. Several civil society organisations and human rights campaigners have expressed their worries about how filtering impedes democratic engagement and online discourse (Abbas & Zubair, 2020).

Need for Balancing National Security and Internet Freedom

Democratic governments sometimes have difficulties in achieving an adequate equilibrium between permitting freedom of expression and instituting fair restrictions. Conversely, non-democratic nations often use censorship as a tool of oppression, termed “digital authoritarianism” (Shahbaz & Funk, 2019). Bischoff (2020) asserts that North Korea ranks first in Internet censorship. The government exerts total control over the broadcast of information to the public and regulates it intensively. China's "Great Firewall" efficiently controls internet information, positioning it as the second most effective in the world. This firewall successfully prevents unauthorised material from being accessible to Chinese internet users, sometimes referred to as "netizens" (Lee & Liu, 2012). Nations such as Russia, which has enacted a "blacklist law" (BBC News, 2012), and Vietnam, whose Decree 72 criminalises dissent against the government, exemplify increasing efforts to filter information and impose stringent censorship (Schmidt & Cohen, 2014).

The extensive use of the internet in Pakistan has empowered individuals to assert their right to freedom of speech, access a plethora of information, and participate in civic discourse. However, this surge in online activity presents challenges for national security. The government recognises that distributing material online may compromise national security. The surge of misinformation, cybercrime, and the utilisation of digital platforms by terrorist organisations necessitates a deliberate approach to internet governance that safeguards both internet freedom and national security. Sensitive materials, such as several films depicting military operations and strategy, documents holding confidential economic data, or any other potentially compromising information, pose a risk to national security.

Nonetheless, there exists discord among differing views. One viewpoint contends that controlling technology infringes against international human rights standards and facilitates governmental surveillance of the masses' internet activity. Governments misuse cyber laws related to legal and political matters concerning Internet-based technology, including freedom of speech, information accessibility, privacy rights, and intellectual property rights. The internet's multi-functionality indicates the importance of implementing a balanced approach that protects individual freedoms while also addressing security issues.

Achieving balance between the principle of online freedom of expression, which allows for user anonymity, and the need of fostering a secure environment where accountable governments can detect and mitigate threats posed by dangerous persons is a formidable challenge. Policymakers are now striving to achieve two simultaneous and sometimes contradictory objectives. Promoting Internet freedom involves endorsing privacy safeguards and providing tools that enable individuals to participate in online activities anonymously. Cybersecurity pertains to the assurance of online visibility and the capacity to ascertain the origin of actions or occurrences. These two activities generate conflicts that are poorly understood and often neglected. The challenge arises mostly because talks on cybersecurity and Internet freedom rules have largely transpired independently of one other. The creation of cybersecurity policy has mostly included the national security sector, while the development of Internet freedom policies has mainly engaged the technology industry and a limited group of human rights supporters.

The primary challenge faced by the Pakistani government is to strike a delicate balance between safeguarding digital rights and upholding societal order, peace, and security. One of the primary concerns for policymakers in Pakistan is the need to balance the preservation of national security with the preservation of internet freedom. In order to safeguard against cyber threats and safeguard the country's interests, policymakers in Pakistan have a duty to enforce cybersecurity protocols that uphold basic rights, including the right to privacy, freedom of speech, and access to critical information (Abbas *et al*., 2023).

CONCLUSION

Cybercrime incidents in Pakistan are increasing, affecting both organizations and individuals. Talent shortages and insufficient resources pose significant challenges for the government to address these concerns. Investing in technology and promoting international collaboration are critical measures for enhancing cybersecurity and successfully deterring cybercrime in Pakistan. This article asserts that censorship regulations in Pakistan impede internet freedom. Pakistan may achieve a more equitable strategy that upholds people's basic rights and security by including stakeholders, improving openness, and refining legislative frameworks. Ensuring a delicate balance between the preservation of internet freedom and the maintenance of national security in Pakistan is a multifaceted but important undertaking. It necessitates the combined efforts of all sections of society, a dedication to democratic principles, and comprehension of the digital terrain. The article asserts that technical progress and the development of skills and resources are crucial for ensuring cybersecurity. The article highlights the need for precise legal definitions and transparent governmental policies concerning internet freedom. It encourages the involvement of multiple stakeholders and suggests solutions to maintain this balance. Pakistan can establish a digital ecosystem that ensures the protection of both online freedom and national security.

REFERENCES

Abbas, Z. & Zubair, M. (2020). Freedom of Expression under Censorship is a threat to Democracy. *The Dialogue,* 15(1): 18-26.

Abbas, Z; Khan, R; Khan, M.Z; & Imran, M. (2023). Cyber Laws and Media Censorship in Pakistan: An Investigation of Governmental Tactics to Curtail Freedom of Expression and Right to Privacy. *Journal of Creative Communications,* 1-14.

Abbasi, I. S & Al-Sharqi, L. (2015). Media censorship: Freedom versus responsibility. *Academic Journals, Journal of Law and Conflict Resolution, 7*(4): 21-25.

Barn, R.; Barn, B. (2016). An ontological representation of a taxonomy for cybercrime. *In Proceedings of the 24th European Conference on Information Systems* (ECIS 2016), Istanbul, Turkey, 12–15 June 2016.

BBC News (2012, January 11). Russia internet blacklist law takes effect. Retrieved from http:// www.bbc.co.uk/news/technology-20096274

Bischoff, P. (2020). Internet Censorship 2020: A Global Map of Internet Restrictions. *Comparitech* Retrieved from, https://www.comparitech.com/blog/ vpn-privacy/internet-censorship-map/>

Black, A.; Lumsden, K.; Hadlington, L. (2019). Why Don’t You Block Them? Police Officers’ Constructions of the Ideal Victim when Responding to Reports of Interpersonal Cybercrime. *In Online Othering: Exploring Violence and Discrimination on the Web; Lumsden, K., Harmer, E., Eds*.; Palgrave Macmillan: Basingstoke, UK, pp. 355–378.

Castells, M. (2009). *The Rise of the Network Society: The Information Age: Economy, Society, and Culture*. Wiley-Blackwell.

Daily Dawn. (2009, October 30). Traders term e-crime law anti-people. Retrieved from https://www.dawn.com/news/889238

Deibert, R.J. (2003). *Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace*. 32 Millennium.

Ekwonwune, E.N., Eduroha, A., Dennis, M.C., & Chigozie, U.C. (2024). Internet Censorship and its Implication on Personal Privacy. *International Journal of Research Studies in Computer Science and Engineering, 10*(2): 22-30.

Gul. A. (2017, November 14). Study: Internet Freedom Worsens in Pakistan. *Voice of America,* [Retrieved from https://www.voanews.com/a/internet-freedom-worsens-pakistan-study/4114815.html].

Hamdani, Y. (2014). Major Challenges to Fundamental Right of Freedom of Speech in Pakistan. *Media Defense*.

Jamil, S. (2021). The rise of digital authoritarianism: Evolving threats to media and Internet freedoms in Pakistan. World of Media. *Journal of Russian Media and Journalism Studies*, 3(1): 5-33.

Jewkes, Y & Yvonne, M. (2010). Introduction: the Internet, cybercrime and the challenges of the twenty-first century, [in:] Y. Jewkes, M. Yvonne (ed), *Handbook of Internet Crime.* Willan Publishing.

Lee, L & Liu, C. (2012). Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China. *Minnesota Journal of Law, Science and Technology, 13*(1): 125-135.

LOC. (2016, September 21). Pakistan: National Assembly passes a new cybercrime law. *Library of Congress*. https://www.loc.gov/item/global-legal-monitor/2016-09-21/pakistan-national-assembly-passes-newcybercrime-law/

Munir, A., & Gondal, M.T. (2017). Cyber Media and Vulnerability: A discourse on cyber laws and a probe on victimization of cybercrimes in Pakistan. *Global Media Journal: Pakistan Edition*, *10*(2).

Newth, M. (2010). The long history of censorship. Retrieved from http://www.beaconforfreedom.org/liste.html?tid=415&art_id=475

Peteva, P. (2020). The nature of censorship and regulation of the darknet in the Digital Age. PRAWO, Retrieved from https://repozytorium.uni.wroc.pl/en/dlibra/publication/129046/edition/118462/the-nature-of-censorship-and-regulation-of-the-darknet-in-the-digital-age-peteva-petya

Privacy International. (2017). *The right to privacy in Pakistan*. Privacy International: Human Rights Committee 120th Session.

Rehmat, A. & Alam, M. A. (2018). The State of Digital Rights in Pakistani Cyberspace. *Freedom Network.*

Schmidt, E.E. & Cohen, J. (2014, March 11). The Future of Internet Freedom. *The New York Times.* Retrieved from http://www.nytimes.com/2014/03/12/opinion/the-future-of-internet-freedom.html?_r=0

Shahzad, M. (2023). Emerging Cyber Crimes in Pakistan: A Case Study of Online Fraud through Digital Microloan Apps. *Global Digital & Print Media Review, 6*(2): 411-421.

Shen, F. (2017). Internet Use, Freedom Supply, and Demand for Internet Freedom: A Cross-National Study of 20 Countries. *International Journal of Communication*, 11(2): , 2093–2114.

Tambini, D. (2021). A theory of media freedom. *Journal of Media Law, 13*(2); 135-152, DOI: 10.1080/17577632.2021.1992128.

Zafar, F., & Ahmad, S. (2011). *The challenges of internet rights in Pakistan*. Global Information Society Watch. https://www.giswatch.org/en/country-report/internet-rights/challenge-internet-rights-pakistan

Zahoor, R & Raz, N. (2020). Cyber-Crimes and Cyber Laws of Pakistan: An Overview. *Progressive Research Journal of Arts and Humanitie*, 2(2): 134-143.