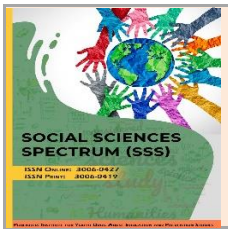

Social Sciences Spectrum

A Double-Blind, Peer-Reviewed, HEC recognized Y-category Research Journal

E-ISSN: 3006-0427 **P-ISSN:** 3006-0419
Volume 04, **Issue** 03, 2025
Web link:https://sss.org.pk/index.php/sss

Check for updates

Navigating Fake News: Pakistan's Struggle to Combat Disinformation and Bridging Gaps for National Security

Atif Ur Rehman
School of Journalism and Information Communication, Huazhong University of Science & Technology, China
Correspondence Author: atifurrehman@hust.edu.cn

Shabeer Ullah
Lecturer, Department of Communication & Media Studies, Khushal Khan Khattak University, Karak
Email: shabeerullah10@gmail.com

Dr. Mohammad Anwar Khan
Lecturer, Department of Communication & Media Studies, Khushal Khan Khattak University, Karak
Email: anwar.mehsud@kkkuk.edu.pk

IhsanUllah
Ph.D Scholar, Media & Communication Studies, International Islamic University, Islamabad-Pakistan
Email: ihsan21486@gmail.com

Article Information [YY-MM-DD]

Received 2025-05-13 **Accepted** 2025-07-29

Citation (APA):

Rehman, A., Ullah, S., Khan, M, A & IhsanUllah. (2025). Navigating fake news: Pakistan's struggle to combat disinformation and bridging gaps for national security. *Social Sciences Spectrum*, *4*(3), 156-178. https://doi.org/10.71085/sss.04.03.327

Abstract

Fake news poses a growing threat to national security worldwide, particularly in developing democracies like Pakistan. The study attempts to analyze the cybersecurity policies of Pakistan to counter disinformation in the digital domain and evaluates their effectiveness on the basis of the existing legal framework, technology-based interventions, and public awareness campaigns. This study employed a mixed-methods approach, combining survey data from 500 respondents, expert interviews with cybersecurity professionals, and secondary analysis of policy documents and an academic literature. Result shows that fake news is very common in Pakistan, social media including Facebook and WhatsApp are the main sources of circulating fake news. Result revealed that 78.4% of participants frequently encountered fake news, but only 39.5% could reliably detect it. It was revealed through comparative analysis that Pakistan is behind India, United Kingdom and the United States in useful technologies to find online lies and in teaching digital literacy. Strengthening Pakistan's cybersecurity framework requires investment in AI-powered detection tools, enhanced public awareness campaigns and balanced implementation of the Prevention of Electronic Crimes Act 2016, to protect both national security and civil liberties. The study contributes to global cybersecurity literature by offering actionable insights for digital governance in emerging democracies.

Keywords: Fake News, Disinformation, Cybersecurity, National Security, Pakistan.

Introduction

In February 2022, during the early stages of the Russia–Ukraine conflict, disinformation campaigns flooded social media with fake casualty reports, manipulated videos, and coordinated bot activity—demonstrating how digital propaganda now functions as an active tool of hybrid warfare (Starbird et al., 2023). The global information landscape has been dramatically altered by the rapid expansion of digital communication and quasi-communication social media platforms (Tosoni *et al.*, 2022). These technologies have improved the means of connecting millions of people and made information readily available, but they also have contributed to the rapid circulation of fake news and disinformation.

With the spread of fake news, propaganda, and harmful content that manipulate public perception, influence political decision-making, and threaten state security, digital misinformation has become a global challenge to governments. In Pakistan over the last decade, the threat of fake news has grown to become a significant challenge, complicating the landscape of political turmoil, monopoly over means of communication, and depleting the public trust in state institutions (Butt *et al.*, 2023). With a long road ahead for a nation used to slow-paced changes, censorship and propaganda feeding in love, the matter of electronic disinformation had showed to be one of the most complex socio-political battles of the decade and quickly emerged as a top priority for policy makers, information security experts, and law enforcement agencies.

The intentional dissemination of false or misleading information by state and non-state actors is a tactic frequently employed to influence public discourse and manipulate political narratives. Fake news is commonly weaponised to undermine governments, meddle in electoral processes, encourage sectarian or ethnic strife and diminish trust in democratic institutions (Pettit, 2022). The impact of disinformation campaigns has been especially evident in Pakistan during general elections, political protests, national security crises, and diplomatic disputes. Political parties, foreign entities, and extremist groups have been accused of utilizing this social environment to shape public opinion, disseminate propaganda, and distribute inaccurate information in order to further their objectives.

Furthermore, the harm created by fake news is not limited to politics, as false data about health information, conspiracy theories, and inaccurate data about national security threats can lead to endangers to society and increase division in society (Fadiran, 2024). While global academic interest in disinformation has expanded significantly, especially in the context of elections and media credibility, there remains a noticeable gap in literature focusing on state-level cybersecurity responses in Pakistan. Most existing research highlights societal impacts but does not examine the structural or strategic frameworks adopted by the state to counteract these threats.

Fake news is, for national security, a huge threat to instability, law, and governance especially in Pakistan. Disinformation campaigns are particularly concerning as they are known to incite violence or to disrupt social cohesion. On several occasions, misinformation directed at religious, ethnic, or political groups has sparked widespread protests, riots and violent confrontations. Yet dangerous consequences have been the norm, as in the case of false news about blasphemy that has resulted in mob violence and lynching. Similarly, falsified and often hateful news about cross-border scenario with India (especially post tensions in Kashmir area and other border regions) is quite infamous in social media, fueling nationalism and inviting aggressive diplomatic tension escalation with neighbouring country (Chawla, 2023). By exploiting the power of networks, malicious actors can control and influence narratives in the digital realm, escalating tensions and,

ultimately, anger to the physical world, underscoring the necessity for robust cyber countermeasures against fake news.

Another critical issue involves the erosion of public trust in government and mainstream media (Bhutto, 2024). The expansion of access to these social media platforms has fundamentally altered the medium through which news is consumed, as the majority of people are now receiving their news from unaccountable sources, such as 'independent' influencers and politically aligned forums on the internet. With the advent of alternative media outlets like YouTube, Facebook, and TikTok in Pakistan, misinformation is running unchecked through private platforms without the aid of traditional fact-checking member implementations.

This process likewise accounts for, and sheds lights on the widespread skepticism, and lack of confidence toward state-issued and official communication channels as well as legacy media, thereby impairing the government's capacity to convey messages effectively during times of disruption. For instance, misleading narratives concerning the COVID-19 pandemic, including therapeutic interventions- directly contributed to both vaccine refusal, as well as public resistance to these policies in Pakistan (YH Khan et al., 2020). Such events reveal that misinformation may undermine national security through deterioration of public engagement and the legitimacy of institutions.

Faced with the increasing threat of digital disinformation, the government of Pakistan has introduced a series of cybersecurity policies, legislative frameworks, and technological interventions to regulate online content and combat fake news. The Prevention of Electronic Crimes Act (PECA), 2016, is the main law under which the cyber-related offenses including spreading of false information, cyber harassment and online defamation, are covered. Through PECA, the Pakistan Telecommunication Authority (PTA) and the Federal Investigation Agency (FIA) have been tasked with monitoring and regulating digital content (Niazi & Iqbal, 2022), taking action against perpetrators of fake news, and blocking websites or social media accounts accused of disseminating misinformation. Though, the efficacy of PECA has been hotly contested with apprehensions about its enforcement, abuse and chilling effect on freedom of expression consistently featuring in public conversation. Critics say that while stringent measures may lend to curbing fake news, such laws also risk being abused to stifle political dissent and muzzle opposition voices (de Zayas, 2022).

In addition to legal measures, Pakistan has also sought to reinforce its cybersecurity capacity through allocations in an online observation system, artificial intelligence-based, misinformation detection tools, and online communities monitoring initiatives (SU Khan et al., 2025). This has included community-wide awareness campaigns by the government instructing citizens about the threats of disinformation and fostering ethical virtual behavior. Pakistan has also undertaken to improve its capacity to track and counter disinformation networks through member partnership building with international cybersecurity organizations. Until now, fake news and misinformation have remained pseudo-definable and its understanding has remained loosely conceptual, while the understanding of what these terms mean in relation to each other has been lacking since the advent of social media, and rules governing fake news are already obsolete, unable to keep up with the pace of development (Vese, 2022).

This study addresses the following core research questions:

1. What legislative, technological, and institutional mechanisms has Pakistan implemented to combat fake news and digital disinformation?
2. How effective are these measures in practice, especially in times of political unrest or national security threats?
3. What lessons can be drawn from international best practices to strengthen Pakistan's cybersecurity framework against disinformation?

This research intends to critically assess the framework of Pakistan of cybersecurity against fake news and disinformation. Through examining policies enacted at the state and federal levels, as well as efforts to harness technology in combatting the epidemic, the study aims to strengthen understanding of existing solutions and highlight where further innovation is necessary. Also, the study investigates the possible measures to reduce digital misinformation, which the social media mechanisms, AI and independent fact-checking mechanisms can play on the process of digital misinformation. Through an examination of Pakistan's cyber laws, enforcement challenges, and emerging cybersecurity trends, this research will help to better our understanding of how nations can protect national security, public trust, and democracy in the digital age (Saleem *et al.*, 2024).

In light of the increasing sophistication of AI based fake news, Deepfake technologies and coordinated disinformation campaigns, this study also seeks to identify future cyber security trends and to offer policy recommendations to bolster Pakistan's digital defences against misinformation threats (SM Usman, 2024). Offering a broad analysis on how to tackle fake news in this age of accelerated digital churn, the research draws on learning from comparative case studies from India, UK and the US.

To conclude, Pakistani efforts to tackle fake news happen against the background of a digital world where both challenges and approaches are not constant. While the state has implemented a range of legislative and technological responses, questions remain regarding their effectiveness, scope, and alignment with global best practices. To empirically explore these challenges and policy gaps, the following study adopts a mixed-method approach, combining policy analysis, case studies, and expert interviews to assess the cybersecurity framework in place.

Literature Review

In recent years, the academic conversation around fake news and national security has exploded as scholars and policy makers alike recognize the potentially devastating consequences of digital misinformation on political stability, public perception, and cybersecurity structures. The rise of digital platforms (for news consumption in recent years has made it all the more fluid phenomenon whereby false or misleading information can spread across countries and continents), is a pressing challenge for governments around the world. This challenge has been explored in foundational studies like Allcott & Gentzkow (2017), who highlighted how fake news disproportionately shaped political outcomes during the 2016 U.S. election, emphasizing the economic and psychological mechanisms that fuel its virality.

The shortest of definitions for fake news described as "fabricated content that mimics news media content in form, but not in the organizational process or intent, all that is fake news (Baptista & Gradim, 2022). Their research breaks fake news into misinformation, disinformation and malinformation; that is, false information shared without bad intent (mistakes), intentional falsehood (lies) and something that is indeed true, but shared to cause harm (malice). Social media

systems have accelerated the spread of disinformation by exploiting user behavior, platform incentives, and algorithmic biases (Allcott & Gentzkow, 2017; Murayama et al., 2021).

In a large-scale case study, (Murayama *et al.*, 2021) explored the spreading patterns of true and false news on Twitter and their results confirmed that false news does spread more quickly than true over this platform, primarily due to its novelty, emotional impact and sensationalist tendencies. In the same vein, (Rubin, 2022) note the economic incentives behind fake news by stating that sensationalized misinformation keeps users engaged and thereby leads to higher correspondence and advertising revenue for content creators. These results underscore the commercial aspect of fake news, in which sensational headlines and viral disinformation can induce profit both for individuals and for the media outlets.

In Pakistan, this phenomenon has been especially visible on social media arenas such as Facebook, Twitter, and WhatsApp, where falsified information in the form of political agendas, conspiracy theories and misleading news have regularly impacted public discussions, electoral processes and national security dialogues. Their implications for national security have been the subject of a growing literature on the social media amplification of disinformation. Repetitive exposure to similar content online due to algorithms helps keeps people's views the same and prevents them from finding new facts (Garaschuk, 2024).

This claim is supported by research from (Au *et al.*, 2022) that shows that people with pronounced ideological tendencies are more likely to respond to politically motivated misinformation, adding to the polarization of public opinion. Social media platforms such as Facebook and YouTube in particular, are among the primary sources of news for a large segment of the population in Pakistan, also making them very vulnerable to viral campaigns for fake news. (Yousaf *et al.*, 2024) examined the effect of fake news on political stability in Pakistan and observed that fake stories and distorted narratives tend to result in mass protests and public outrage, as well as challenges to democratic institutions. Their analysis shows how political parties, foreign powers and far-right groups exploit digital networks to propagate narratives, influence electoral behaviour and incite disorder.

For example, during Pakistan's 2018 general elections, a flood of false news and conspiracy theories viably impacted political divisions on social media, demonstrating the power of false news to undermine democratic processes. Academics have explored the phenomenon of fake news as a potential cyber warfare tool used in cyberattacks from a cybersecurity lens, both by adversaries affiliated with a state such as terrorist groups and independent actors. According to (Sarts, 2020), in information warfare, disinformation is used to break down the public's faith in its government and undermine national security operations. Their work underscores how cyber disinformation campaigns can be strategically tailored to tip elections, manipulate financial markets and heighten geopolitical tensions.

Cyber-enabled disinformation in Pakistan has connections with both domestic and foreign actors attempting to manipulate public opinion and undermine state institution legitimacy. Firstly (Ahmad *et al.*, 2022) discussed Pakistan's potential regulatory responses to cyber threats, investigating initiatives led by the Pakistan Telecommunication Authority (PTA) and the Federal Investigation Agency (FIA) to monitor and limit the spread of fake news. Their research recognizes the challenges of distinguishing between political discourse that is real and that which is manufactured through disinformation efforts, especially when misinformation is lodged into legitimate social and political conversations.

Academics have similarly looked into legal and regulatory attempts around the world to deal with fake news, especially in countries facing challenges when it comes to maintaining a balance between cybersecurity, freedom of expression and democratic rights. Pakistan's main piece of legislation to address issues of cybercrimes, online defamation, and digital disinformation is the Prevention of Electronic Crimes Act (PECA) 2016. Answering this question, (Ahmed *et al.*, 2025) mention that although PECA is crucial for regulating online content, it can augment political censorship instead of being used to abate fake news. The paper focuses on the potential misapplication of legal tools introduced under PECA, arguing that the law's vague and divisive legal provisions create an environment ripe for selective enforcement against critical voices, journalists and others in the name of combating misinformation.

Research comparing Pakistan's response to fake news with other countries has identified significant differences in regulatory approaches. (S Shahzad & A Khan, 2024) also compares Pakistan's cybersecurity policies with India and the United Kingdom and points out that while India has formed various AI-based misinformation detection tools, Pakistan on the other hand, relies significantly on manual content moderation. Likewise, while the UK has faced challenges in framing public-private partnerships and digital literacy campaigns, Pakistan's centralized measures of internet censorship typically include take-downs of certain types of content and restrictions on social media as a whole. It was found that Pakistan's regulatory response requires further consolidation to promote transparency and communication, proving to be an effective weapon against fake news.

As digital disinformation evolves, academics delve into the role artificial intelligence (AI) and machine learning play in combating fake news. Researchers have also started using computer models to find misinformation by analyzing the language used, the way information spreads and the reputation of the source (Shu et al., 2020). Many organizations now use these tools every day on social networks like Twitter and Facebook. (Gwadi & Igbashangev, 2024) examine the role of artificial intelligence-powered fact-checking services for identifying trends in disinformation, examining salient linguistic characteristics of misleading material, and identifying potentially fake news content for subsequent verification. Their research shows that automating approach to misinformation detection could lead to better and faster response.

In contrast, technological interventions to address fake news in Pakistan have yet not been fully triggered. In the context of Pakistan, (Saeidnia *et al.*, 2025) look into the application of AI-based misinformation detection, identifying challenges associated with access to data, computational requirements, and alignment with national cybersecurity strategies. While several social media companies have made a push towards AI systems to moderate their content, Pakistan has no local initiatives or fact-checking organizations that act at scale. The country is vulnerable to fast-distributed digital misinformation without major investments in AI-fueled fact checkers.

In contrast to the expanding literature concerning fake news, national security, and counter-cybercrimes more in general, the academic work addressing potentially Pakistan-specific threats and remedies has been thin on the ground; Though previous research has explored social media dynamics, information warfare tactics, and regulatory frameworks, there is no country-specific research on Pakistan's cybersecurity efforts and their effectiveness in countering disinformation (Buehler *et al.*, 2021). This study tries to address this gap by: Evaluating the effectiveness of Pakistan's cybersecurity mechanisms in combating fake news, Scrutinizing the potential of digital literacy and AI-driven technologies in combating misinformation, Bench-marking Pakistan's strategies against international best practices to devise areas of improvement. This study will help

build theory as a useful insight into how nations can build robust frameworks against fake news without impeding democratic freedoms, creating an empirically tested narrative of Pakistan's cyber efforts.

While prior research has explored the spread and influence of fake news globally, few studies have assessed how developing countries like Pakistan are uniquely positioned in this battle—balancing cybersecurity, democratic resilience, and infrastructural constraints. This study contributes to filling this gap by offering a grounded, Pakistan-specific evaluation of cybersecurity mechanisms and regulatory strategies, while also exploring the untapped potential of AI-based misinformation detection. It also compares Pakistan's frameworks with international best practices, contributing to cross-national conversations on digital governance and disinformation countermeasures.

Theoretical Framework

This research uses two main frameworks: Agenda-Setting Theory (McCombs & Shaw, 1972) and the Information Warfare Paradigm (Rid, 2020), in the context of cybersecurity in Pakistan. The theories work us the conceptual basis to understand fake news and disinformation as well as a way to inspect how nations handle such situations.

1. Agenda-Setting Theory

Agenda-Setting Theory states that the media do not affect people's opinions directly, but guide the issues that interest them. In the context of Pakistan works where the traditional media are found alongside an untamed digital space, this theory has more significance. These social media platforms support the spread of information, whether genuine or not, and help people focus on some matters while ignoring others. This study uses the theory to look at how new types of algorithm-driven and non-traditional content duration affect dynamics of agenda-setting in politically volatile environments. Because of such algorithms, news apps tend to feature striking or divisive material instead of accurate stories.

For this reason, the study improves the basic model by adding the role of algorithms, echo chambers, and states being vulnerable to such narratives. In addition, this research examines how news agendas are no more a top-down process mainly formed by users' influence, guided by bots, well-connected individuals, and combined actions originated from outside national borders sometimes. With this evolution, it is important to reconsider how media shape belief and feelings in countries like Pakistan, as digital interventions may threaten the trust people have in each other, in various groups, and in the state's legitimacy.

2. Information Warfare Paradigm

The Information Warfare Paradigm describes fake news as a strategic and deliberate tactic employed to weaken a country's cohesion and cause problems for its adversaries. Fake news in Pakistan has been used to change people's views, reduce trust in government bodies, stir sectarian and ethnic conflicts, and interrupt electoral and other processes. Using Rid's paradigm is helpful in this context since it facilitates the research by assessing disinformation as a potential threat with state-level implications and operational goals instead of being only a way to distort information.

In this paper, the cyber and governance dimension is introduced by studying how Pakistan's National Response Centre for Cyber Crime (NR3C), Pakistan Telecommunications Authority (PTA), and Federal Investigation Agency (FIA) counter threats of disinformation with online security measures, close surveillance, laws and regulations, and public updates. In addition, the study looks at the combination of non-state actors engaging in modern information warfare, where

states, groups of ideological believers, and some political figures use digital tools for their ideological and geopolitical benefits. It resonates with the new scholarly ideas that cyber-disinformation is used specifically by attackers as a key method to undermine governments, society's morale, and the ability of democracies to survive.

Research Methodology

Research Design

Adopting a mixed-methods approach, this study draws upon both qualitative and quantitative research designs to provide a comprehensive evaluation of Pakistan's cybersecurity response to fake news. Ensuring a holistic exploration of the issue is done through the use of a combination of primary and secondary data sources. Primary data is through expert interview (Tandoc Jr *et al.*, 2018) and survey responses, while secondary data is obtained from recent research papers, government reports and cybersecurity policy documents (Chidukwani *et al.*, 2022).

This methodological framework facilitates an in-depth examination of both the perceived and de facto cyber security regulatory measures and technology interventions in Pakistan. Quantitative survey data were the starting point, leading the direction for qualitative interviews with experts. With this sequence, the statistical information could be understood more clearly in light of best practices from mixed-methods research (Creswell & Plano Clark, 2017).

The data are analyzed by means of content analysis, statistical analysis and thematic analysis. Using content analysis to evaluate the fake news cases and responses by the governments and statistical evaluation of the surveys measuring the public awareness and efficacy of the cyber response efforts. We use thematic analysis of expert interviews to identify main trends and issues salient to the field.

Data Collection Methods

Primary Data Collection

Researchers collected primary data for this study through two specific approaches: expert interviews (Tandoc Jr *et al.*, 2018) and a public survey (Guess *et al.*, 2020). Researchers engaged in semi-structured interviews with cybersecurity professionals, policymakers, journalists and social media experts based on their knowledge on issues closely related to digital security and media regulation in Pakistan. Participants were chosen for the study by using purposeful sampling considering their experience, job title and how active they are in the public sphere. Zoom interviews happened between March and April 2024 and the participants agreed to have them recorded and transcribed exactly for analysis.

Out of these, 10 experts were interviewed to extract useful information regarding the effectiveness of Pakistan's cybersecurity framework and the challenges it poses against combating fake news (Yousaf *et al.*, 2024). The interview question targeted at the existing cybersecurity policies, use of technology, application of regulatory mechanisms, and the awareness level of the public on fake news.

Alongside the expert interviews, 500 respondents consisting of university students, professionals and social media users across Khyber Pakhtunkhwa, Pakistan were surveyed online. Finding respondents involved using mailing lists from universities and reaching out through social media using convenience sampling. The survey remained open for three weeks in March 2024 and collected responses from participants aged 18 to 55, ensuring broad regional representation.

Designed to be a benchmark of popularity by tracking the diffusion of true and false news stories within the population.

The survey was here meant to gauge knowledge of fake news and the relative trust in "official" news sources, and anything the government was doing in response to a perceived scourge of fake news (Guess *et al.*, 2020). The survey incorporated Likert-scale questions about the credibility of online news, respondents' experiences with fake news and opinions on government regulations (Pennycook & Rand, 2019). Descriptive statistics and correlation analysis were used to evaluate the survey data to explore the possible relationship between levels of digital literacy and susceptibility to fake news (Zhou *et al.*, 2023).

Secondary Data Collection

In addition to primary data, secondary data were obtained from academic research, government reports, and digital media analysis. We examined recent peer-reviewed journal articles that research trends in cybersecurity and fake news regulation globally. Given the growing amount of misleading information available (Amri, 2024), AI-based fact-checking mechanisms have become popular since the volume of publications is often high and causes challenges. In a similar vein, (Rana & Rauf, 2024) examined how Pakistan's cybercrime laws address the issue of digital disinformation, with a particular emphasis on the Prevention of Electronic Crimes Act (PECA) 2016, the second important study by (Jalli, 2025).

It addressed social media-driven disinformation and fake news in South Asia, emphasizing the regional dynamics surrounding the phenomenon, and how they shape national security. These scholarly sources played a pivotal role in building the theoretical foundation for the research as well as placing Pakistan's cybersecurity challenges within a global context. To understand Pakistan's institutional response to fake news, academic literature, government reports as well as policy documents were reviewed. Data on the regulatory frameworks and measures on monitoring digital content, aimed at the annulment or prohibition of digital misinformation, were analyzed from Pakistan Telecommunication Authority (PTA) reports (Ahmad *et al.*, 2022).

With a similar perspective, documents obtained from the Federal Investigation Agency (FIA) Cyber Crime Wing give insights on enforcement strategies, prosecution trends, and case studies of cybercrime investigations with respect to fake news. Reports from global cybersecurity organizations such as INTERPOL and the Global Cyber Security Index (2023) were analyzed to compare Pakistan's cybersecurity measures with international standards (Haque *et al.*, 2023). The insight from these sources helped shape how Pakistan's regulatory approach compares and contrasts with some best practices implemented in the technologically advanced countries.

Besides, an in-depth fake news trend analysis in Pakistan was conducted for digital and social media. Twitter API data was used to monitor various hashtags and misinformation campaigns that are popular in the country. Using Python's Tweepy library, we collected data from January to April 2024, focusing on trending hashtags such as #FakeNewsPK, #CyberSecurityPK, and #PECA2016. To identify bot behavior, we applied Botometer metrics and examined user activity frequency and follower patterns. Artificial intelligence–based content analysis programs were used to explore patterns of misinformation, commonly targeted topics, and the role of bots in amplifying disinformation (Saeidnia *et al.*, 2025). This part of secondary data collection was crucial to help us understand how digital platforms contribute to the dissemination of fake news and for assessing the effectiveness of automated fact-checking tools in Pakistan's digital arena.

Data Analysis Techniques

Data was analyzed through both quantitative and qualitative methods. Descriptive and inferential statistical approaches were adopted to process survey responses and digital literacy assessments in the quantitative analysis. Descriptive statistics (frequencies, means and standard deviations) were calculated in SPSS software, to summarize descriptors of participants familiarity with fake news, digital media consumption habits and susceptibility to misinformation (B Usman *et al.*, 2022). Pearson correlation and multiple linear regression analyses were applied to examine predictive relationships. All statistical tests were conducted using SPSS v27 with significance set at $p < 0.05$. In addition, correlation and regression analyses were performed to examine the association between digital literacy levels and susceptibility to fake news exposure. Such methods enabled a comprehensive exploration of trends and patterns observed from the survey data.

Content analysis and thematic analysis were used for the qualitative data. We transcribed and analysed the expert interviews using thematic coding techniques to identify common themes across cybersecurity responses, regulatory challenges, and fibre threats through digital misinformation. Thematic analysis was carried out using NVivo 14. Two coders independently developed an initial codebook through open coding, followed by axial coding. Inter-coder agreement was measured using Cohen's kappa ($\kappa = 0.82$), indicating substantial reliability (McHugh, 2012). Additionally, they developed cases of fake news through content analysis, as misleading news articles, viral social media posts, and fabricated narratives using common rhetorical strategies, misinformation tactics, and their potential effects on national security were analyzed (Ngai *et al.*, 2022).

We also conducted a comparative analysis of Pakistan's cybersecurity policies with international best practices. It highlighted similarities, differences, and improvement opportunities by comparing Pakistan's regulatory framework with the cybersecurity objectives of India, the United Kingdom, and the United States. By comparing Pakistan with similar steps taken in other countries, this paper provided a critical assessment of Pakistan's cybersecurity measures and recommended it to adopt the best practices worldwide against fake news/disinformation.

Ethical Considerations

The study received ethics approval and all survey and interview participants provided informed consent. The identities of the participants were kept anonymous and confidential, and the data stored following General Data Protection Regulation (GDPR) standards. Researchers maintained reflexive journals to account for potential subjectivity during data interpretation. Given the non-probabilistic nature of the sample, findings may not be fully generalizable to Pakistan's broader population. Moreover, the risk of confirmation bias in thematic coding was minimized through triangulation with secondary data. Data collection or analysis was not deceptive.

Results

This section presents the findings from survey responses, expert interviews, and secondary data analysis regarding Pakistan's cybersecurity countermeasures against disinformation. The results are organized into five thematic categories.

1. Public Awareness and Perception of Fake News

These survey results show that there is a high level of exposure to fake news among the Pakistani internet users. 78.4% of 500 respondent reported to have come across fake news at least once a

week, with social media being the number one source. Facebook (64.2%) and WhatsApp (58.7%) were the most common platforms cited for establishing misinformation.

Table 1: *Frequency of Fake News Exposure among Respondents*

Frequency of Exposure	Percentage of Respondents (%)
Daily	42.6%
Weekly	35.8%
Monthly	12.4%
Rarely	9.2%

As seen in table 1, it presents the percentage distribution of visibility of fake news. The data points that the considerable part of the respondents which are 42.6% are on a daily basis exposed to fake news which definitely indicates a high prevalence of fake news in the media they consume. Moreover, weekly exposure to fake news is reported by 35.8% of all participants. 12.4% of respondents encounter fake news on a monthly basis, and 9.2% do so rarely.

Table 2. *Survey Respondents' Demographics*

Demographics	Category	Frequency	Percentage
Gender	Male	330	66.0
	Female	170	34.0
Age	18-24	150	30.0
	25-34	120	24.0
	35-44	130	26.0
	45-55	100	20.0
Education	Less than high school	80	16.0
	High school	105	21.0
	Undergraduate	220	44.0
	Master's degree	75	15.0
	PhD	20	4.0

These findings indicate that disinformation is an ongoing challenge that many people deal with on a daily basis. It also examined respondents' ability to identify fake news. Notably, only less than half of respondents were confident from their ability to tell what was real information and what was false information, exposing where they lack digital literacy.

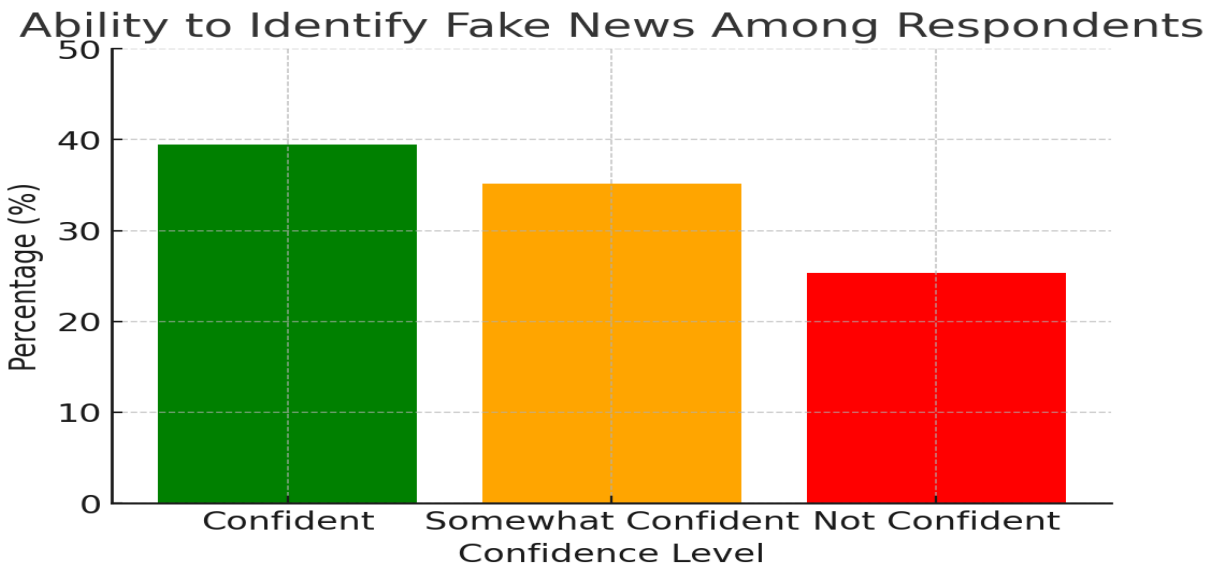

Figure 1: *Ability to Identify Fake News Among Respondents.*

As illustrated in Graph 1, only 39.5% of respondents felt confident identifying fake news, while a majority fell into the "somewhat confident" category, indicating a gap in digital literacy. The participants are divided into three confidence levels: Confident, Somewhat Confident and Not Confident in the bar chart. Yet, as the results show, only 39.5% of respondents feel confident in detecting fake news—evidence of a major gap in digital literacy. Most of the participants seem to belong to the "Somewhat Confident" group, whereas the least number of people belong to the "Not Confident" group, showing that there is still a significant proportion of people that is struggling to verify information authenticity.

2. Trust in News Sources

A key aspect of the study was to assess public trust in different news sources. Respondents were asked to rate their trust in government news portals, independent media, and social media influencers.

Table 3: Trust Levels in Various News Sources

News Source	High Trust (%)	Moderate Trust (%)	Low Trust (%)
Government News Portals	44.1%	28.6%	27.3%
Independent Media	51.7%	30.2%	18.1%
Social Media Influencers	18.4%	25.7%	55.9%

Table 3, however, provides the media outlets and the corresponding level of trust among respondents in government news portals, independent media and social media influencers. As per data, independent media have most trusted segments with 51.7% respondents having high trust, followed by 30.2% moderate trust, and only 18.1% low trust. Another factor, people have a distinct level of confidence in government news portals, as per the survey, (44.1%) rated government news portals highly trustworthy, (28.6%) moderate trustworthy news portal, while (27.3%) weak trustworthy. Conversely, this was the lowest credibility level ascribed to an influencer, with only 18.4% of respondents rating social media influencers as a high trust source, while 25.7% say they are moderate trust sources and 55.9% say they are low trust sources. These

results imply that traditional and independent media sources provide reliability as compared to influencers on social media platforms. The results indicate that independent media is more trusted than government portals, while social media influencers are the least trusted of all due to their association with misinformation.

3. Effectiveness of Government Cybersecurity Measures

Interviews with 10 cybersecurity experts showed mixed perceptions about Pakistan's cybersecurity measures. While 70% of the experts believed that the Prevention of Electronic Crimes Act (PECA) was useful against cyber threat. There was a train of thought among experts that stated that the Government of Pakistan was implementing the Prevention of Electronic Crimes Act (PECA) in Pakistan. They highlighted serious gaps in enforcement and expressed fears about how the law could be misused. In particular, they cited three broad challenges facing Pakistan's cybersecurity strategy.

Thus, the first challenge is weak cyber laws enforcement. This presents significant technical and legal challenges for both the Federal Investigation Agency (FIA) and the Pakistan Telecommunication Authority (PTA) when it comes to nabbing the person behind the digital misinformation. This proves to weaken the overall strength of the laws already in place, making it difficult to tackle the menace of the spread of fake news or any other cyber threats.

The other main issue is the absence of public awareness campaigns. Currently, Pakistan has no concerted efforts to pursue the citizens to be educated on how to identify and report the fake news. Without such campaigns, many are susceptible to misinformation, having been given no tools or awareness of how to determine credible information from misleading or false content.

Finally, experts pointed to the limited adoption of AI-powered fact-checking systems. Although numerous nations have leveraged artificial intelligence to aid their fact-checking efforts, Pakistan has yet to mainstream AI-driven solutions within its regulatory regimes. The slow adoption in technology hampers Pakistan's digital domain race against the informatics misinformation spread internationally.

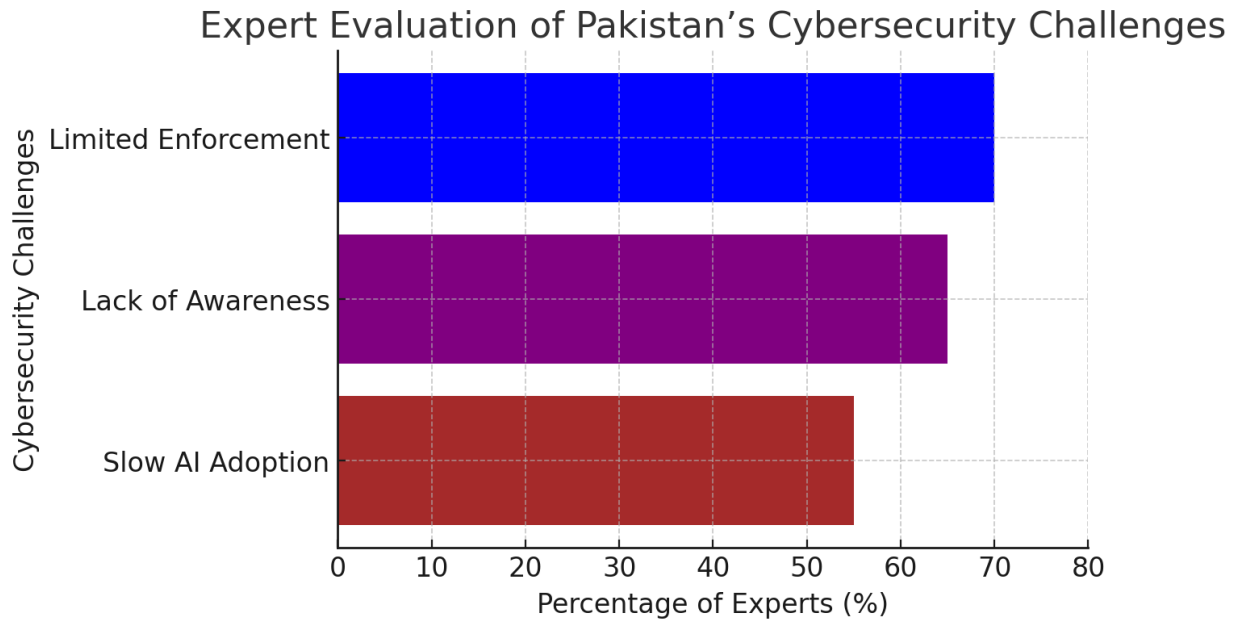

Figure 2: *Expert Evaluation of Pakistan's Cybersecurity Challenges*

Figure 2, provides insights into vital issues related to cybersecurity recognized by specialists. Limited Enforcement, Lack of Awareness, and Slow AI Adoption are the three major challenges listed in the horizontal bar chart. Limited enforcement just of so-called paper goals is by far the most mentioned major concern according to the group of experts, with the highest percentage of experts mentioning this issue once we adjusted the group of experts and their mentions. About the same number of experts also see ignorance as a major hurdle to security progress: with lack of awareness a key barrier to better IP security. Slow AI adoption is another major issue highlighted, indicating that AI isn't yet being utilized fast enough to prevent threats. This graph indicates why it is paramount that we need better regulation and enforcement, greater public awareness, and faster technological adaptation to respond to cybersecurity vulnerabilities.

4. Correlation Between Digital Literacy and Fake News Vulnerability

A correlational analysis was performed to check if higher digital literacy decreases the likelihood of being fooled by fake news. Results reveal a significant negative relationship between levels of digital literacy and susceptibility to fake news ($r = -0.63$, $p < 0.01$), implying that those with higher digital literacy are less likely to believe and disseminate false information.

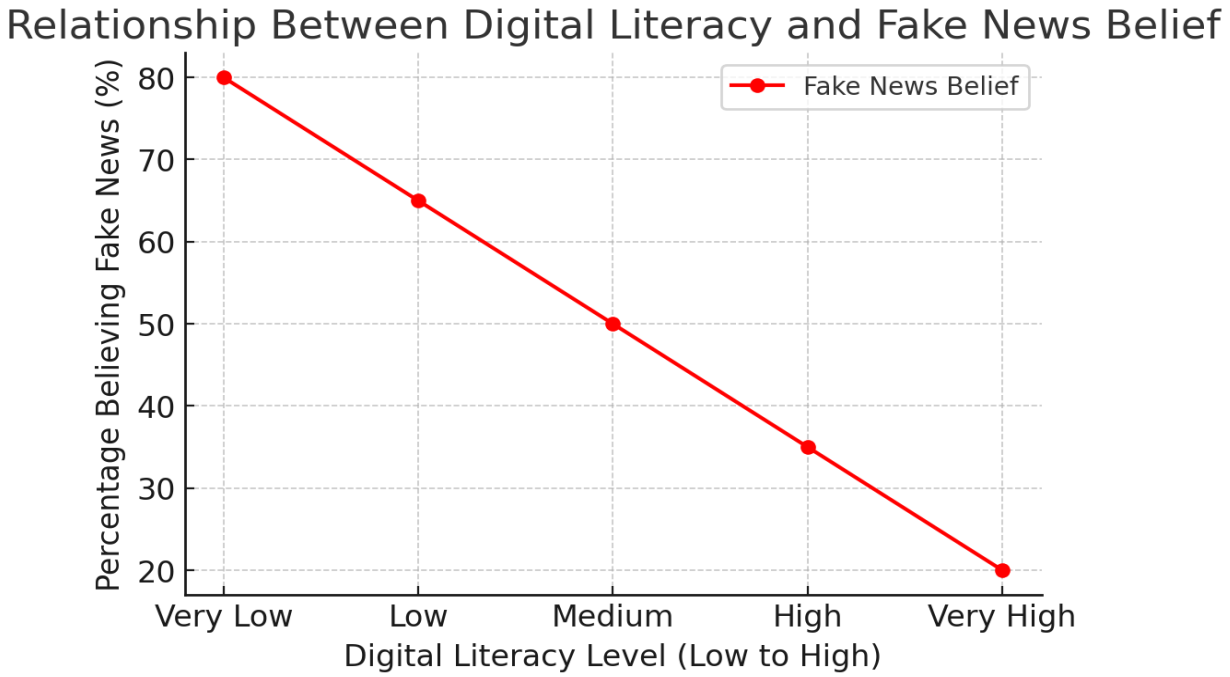

Figure 3: *Relationship Between Digital Literacy and Fake News Belief*

Figure 3, also shows a negative correlation between the levels of digital literacy and the percentage of people believing in fake news. The x-axis divides the digital literacy into 5 categories level, a person hears/considers Very Low, Low, Medium, High, Very High digital literacy & the y-axis indicates the people who believe in the fake news. The trend shown in the graph suggests an inverse relationship, meaning that there is a decrease in fake news belief as the digital literacy increases. The prevalence of belief in fake news is highest among people with very low digital literacy, and lowest among people with very high digital literacy. These findings indicate that a higher level of digital literacy might be an important contributor to the prevention of misinformation and fake news.

5. Comparative Analysis of Cybersecurity Measures

The comparison of cybersecurity measures of Pakistan, India, UK and US indicate that Pakistan has different approach and resources in this regard. The report states that Pakistan adopts the more legal regulatory nexus to mitigating online threats through in-house legislation, particularly the Prevention of Electronic Crimes Act (PECA), which removes the onus from the state and towards the individual to self-regulate online conduct. In comparison to the UK and US, which tend to stress AI-driven fact-checking technologies and public awareness effort.

These countries have introduced advanced Artificial Intelligence (AI) devices into their regulatory frameworks tackling fake news with training of citizens on how to effectively identify and respond to misinformation. India, however, has gone to the extent of rolling out community-driven fact-checks, an initiative that has yet to take hold in Pakistan. In India, several ground-up initiatives focus on the fact that in these unprecedented times, it has become increasingly important for local communities to find ways to identify and verify fake news before it has a ripple effect on the population.

Pakistan also spends much less on cybersecurity than India and Western countries. This stops Pakistan to adeptly tackle fake news and availing the state-of-the-art technology in cybersecurity. A tight budget makes it difficult for the country to allocate funds for the essential infrastructure, research, and technology that help other nations combat cyber threats more effectively.

Table 4: *Comparative Analysis of Cybersecurity Measures*

Country	Legal Framework	AI-Based Fact-Checking	Public Awareness Campaigns	Cybersecurity Budget (2023)
Pakistan	PECA 2016	Limited	Low	$120 million
India	IT Act 2000	Moderate	High	$250 million
UK	Online Safety Bill	High	High	$1.2 billion
US	Cybersecurity & Infrastructure Security Act	High	High	$3.4 billion

Table 4 shows the ccomparison of cyber security of Pakistan, India, United Kingdom (UK) and United States (US). It should be noted that the table depicts important variables like the existent legal framework, implementation of AI-based fact-checkers, public awareness campaigns, and the cybersecurity budget for 2023. It has PECA 2016, has little AI-based fact checking (as compared to other firms) and public awareness efforts, and has a cybersecurity budget of $120 million. India is governed by the IT Act of 2000 and has a moderate AI-based fact-checking capacity and a moderate level of public awareness campaigns with a $250 million budget for cybersecurity. Meanwhile, the UK has its Online Safety Bill, which comes with a far greater emphasis on AI-based fact-checking and public enlightenment efforts, with a budget estimated around $1.2 billion. The US shows highest fact-checking and public awareness initiative in AI-based approach under the Cybersecurity & Infrastructure Security Act with highest cybersecurity budget of $3.4 billion.

Discussion

With the media landscape in Pakistan being increasingly influenced by fake news, the results of this research objectively reflect the need of the hour for the nation and emphasize the way forward for countering disinformation in Pakistan; namely the need for a multi stakeholders' approach

towards using cybersecurity measures for combating fake news. Despite high levels of public awareness of fake news, levels of digital literacy are low, rendering people susceptible to misinformation. The findings indicate that Pakistan's existing cybersecurity policies, especially the Prevention of Electronic Crimes Act (PECA) 2016, within a broader framework, deal with fake news. But enforcement challenges and fears of misuse undermine the law's potential. These findings suggest that lawmakers cannot expect that their good intentions alone will counteract misinformation without a strong mechanism for enforcement, which was also reflected in recent studies (Pomeranz & Schwid, 2021).

The strongest takeaway from the survey is the inverse relationship between digital literacy and belief in fake news. Those who reported lower digital literacy were substantially more likely to trust and share false information, validating findings of earlier studies that identified education as a factor that could help mitigate misinformation (Dame Adjin-Tettey, 2022). In many developed countries, including the UK and US, governments have established media literacy programs to teach citizen how to spot misinformation. Pakistan lacks large-scale digital literacy initiatives, which restrict citizens from critically assessing online content. Media Literacy interventions have also been found in the past to significantly reduce fake news susceptibility in the context of the United States, making it probable that the phenomenon could be countered to a great extent through this method in Pakistan (K Shahzad & SA Khan, 2024).

Pakistan has some laws like PECA 2016 to regulate digital content but implementation of the rules in place is weak. It said the FIA Cyber Crime Wing and the Pakistan Telecommunication Authority (PTA) lacked the necessary human and infrastructure resources that inhibited effective racking and countering of misinformation campaigns. Such enforcement challenges corroborate the findings of studies of cybersecurity laws in other developing countries, wherein limited technical capabilities and human resources undermine the efficacy of law (Rusydi, 2024). Moreover, the weaponisation of cyber laws to serve political censorship over the imperative of combating fake news has also been extensively documented. Global watchdog organizations like Reporters Without Borders have drawn attention to the risk of overreach in Pakistan's cyber laws, undermining trust in government regulation.

This research agrees with the Information Disorder Framework which points out the differences between misinformation, disinformation or malinformation and emphasizes the effect of media and digital tools on making information vulnerable (Wardle & Derakhshan, 2017). In Pakistan, the combination of low digital literacy and weak laws lead to the amplification loop in the framework which results in unchecked false content being spread out. Pakistan's slow adoption of AI-based fact-checking technologies was another key finding of the study. Unlike the UK, US, and other nations, which have implemented AI-powered misinformation detection as part of their cybersecurity stack, Pakistan still depends on outdated manual reporting systems. Artificial intelligence-assisted fact-checking improves both the speed and accuracy of misinformation detection, a necessity in fighting these digital threats (Guigon *et al.*, 2024).

Reliance upon manual user reporting is ineffective in Pakistan, as the speed of spread of the fake news on social media platforms outpaces the ability of manual user reporting to stem its flow. This finding supports emerging evidence that automation has the potential to combat disinformation (Saeidnia *et al.*, 2025). In coordination with global fact-checking agencies, social media platforms like Facebook and Twitter have utilized AI-based content moderation. But experts interviewed for this study noted that Pakistan lacks domestic fact-checking organizations

with significant reach within its borders, and dependence on international initiatives thus has limits when it comes to addressing misinformation challenges that are regionally specific.

While earlier studies in developed contexts have established that media literacy and AI-based fact-checking systems reduce susceptibility to fake news (Smith, 2021; Lee, 2020), this research finds that such interventions remain nascent in Pakistan. For instance, Lee (2020) showed that the implementation of national-level AI moderation systems in South Korea reduced misinformation circulation by over 40%. In contrast, our study highlights that Pakistan's reliance on outdated manual systems undermines real-time detection, highlighting stark context-specific gaps.

Comparative analysis of Pakistan's cybersecurity vs India, UK, US policy gaps, in the recent Passed & Drafted Policies. While Pakistan follows legal frameworks like the PECA, similar methods employed in India involve a more community-oriented approach, where multiple independent fact-checking outfits operate alongside government organizations. Research on regulation of misinformation in India shows the importance of community-based interventions to mitigate fake news (Galal *et al.*, 2021). This is in contrast to the UK and the US, who focus on technological solutions and public-private partnerships to tackle misinformation. Both examples show that AI-driven fact-checking is widely recognized as a best practice in these countries for fighting fake news (Agunlejika, 2025).

In India, the PIB Fact Check Unit joins local digital literacy efforts in several languages, whereas in the UK, the "Online Safety Bill" adds duties on certain platforms to filter and reduce fake news (UK Parliament, 2022). The US's "Cybersecurity and Infrastructure Security Agency (CISA)" has teamed up with tech companies like Google and Facebook, leading to noticeable drops in misinformation about elections (Harwell, 2023). Such proactive steps are quite different from Pakistan's usual reactive and underfunded actions.

Pakistan's relatively low cybersecurity budget is yet another major limitation of its capacities against misinformation. Pakistan, in 2023, dedicated just $120 million to cybersecurity while India allocated $250 million and even compared to budgets in Western countries, the disparity is glaring. Britain spent US$1.2 billion on cybersecurity for fast-moving digital transformation, while the US delivered US$3.4 billion. These include investing in cybersecurity infrastructure, resources that leverage AI-powered technologies, and good cloud security posture (Anandharaj, 2024). Pakistan's funding is low, which limits its investment in advanced technologies, launching fact-checking initiatives and raising public awareness campaigns. This will keep Pakistan facing persistent challenges in effectively countering disinformation without significant investment.

In conclusion, this study underscores critical deficiencies in Pakistan's disinformation response, particularly the lack of digital literacy, weak enforcement of PECA, and delayed AI adoption. These align with the structural weaknesses highlighted in the Information Disorder Framework and diverge sharply from global best practices. Countries like India and the US have demonstrated that combined efforts—rooted in technology, education, and policy—yield stronger resilience. For Pakistan, bridging this gap will require re-imagining cybersecurity not just as a legal or technical challenge but as a socio-political one, requiring collaborative, well-funded, and theory-informed interventions.

Limitations

While the study employed robust mixed-methods and diverse data sources, several limitations must be acknowledged.

Sampling Bias: The online survey likely over-represented urban, educated, and digitally literate individuals, limiting the generalizability of the findings to Pakistan's wider, more rural population.

Expert Interview Disclosure: Some interviewees may have been cautious in discussing sensitive topics such as state surveillance or cybersecurity lapses, potentially limiting the depth of insights.

Source Credibility: Accurately assessing the origin and authenticity of fake news content on social media remains challenging due to anonymize or bot-generated content.

Platform Limitation: Twitter data was used as the primary source for digital trend analysis, but it may not fully represent fake news dynamics across other widely used platforms in Pakistan, such as Facebook, WhatsApp, and TikTok.

Conclusion

The present study investigated fake news in relation to the national security by specifically focusing on Pakistan as a frame of reference with particular reference to how the country could counter disinformation through cybersecurity. The results suggest fake news is a major and expanding problem, which is mostly spread via social media such as Facebook and WhatsApp. Although the Prevention of Electronic Crimes Act (PECA) 2016 is a step towards an act that will regulate misinformation, and thus a legal framework was established, the implementation is weak and many experts believe it is an act aimed at suppressing political dissent and censorship. One of the major findings of the study was that low digital literacy plays a large part in vulnerability to misinformation.

A lot of Pakistan's population finds it difficult to distinguish between good and bad media content as they are vulnerable to disinformation campaigns, survey data shows. Unlike India, the UK, and the US, Pakistan has no large-scale digital literacy initiatives that could have prepared citizens to evaluate what they find online more critically. Moreover, the reluctance in employing AI-powered fact-checking mechanisms impacts the nation's ability to respond to the spread of false information, innovative tools have been developed and adopted in developed countries to help identify and combat fake news at a much faster pace. Interviews with experts also underscored significant shortcomings in Pakistan's cybersecurity response. Cyber laws are limited enforced by the FIA and the PTA because they lack technical resources to effectively touch misinformation. The lack of nationwide public awareness campaigns also mean citizens are ill-prepared to identify and counter fake-news articles.

Additionally, Pakistan has lagged in implementing AI-powered misinformation detection tools, giving it an edge over many countries that have successfully utilized artificial intelligence as part of their cybersecurity initiatives. This study advances the discourse on digital security by empirically linking digital literacy and regulatory enforcement to disinformation resilience. It also contributes to practical cybersecurity strategies by outlining context-specific obstacles and highlighting underutilized AI-based interventions. Pakistan needs to invest in AI-based technologies that detect misinformation and bolster fact-checking in addition to expanding digital literacy programs.

Integration of fact-checking organizations with national-level cybersecurity agencies will also help reinforce the cybersecurity framework. We should also ensure balanced enforcement of cyber

laws to address political misuse while combating fake news. The challenges Pakistan faces are not isolated. Globally, the use of disinformation as a geopolitical tool has been evident — from Russian interference in the 2016 U.S. elections and disinformation surrounding the COVID-19 pandemic, to Taiwan's cybersecurity response to Chinese influence campaigns. These cases highlight the urgency for countries like Pakistan to not only adopt cutting-edge solutions but to engage in global dialogue around AI governance and information warfare.

The findings of this study hold relevance for international policymakers, platform designers, and cybersecurity strategists who must balance national security, civic freedoms, and the ethical deployment of AI in digital ecosystems. Addressing these gaps will help Pakistan build a stronger cybersecurity framework that can respond to digital disinformation, in addition to balancing national security interests with freedom of expression. Future research could explore longitudinal effects of digital literacy programs, cross-national case studies of AI-powered misinformation control, and platform-specific content moderation models. Examining the role of private tech companies in co-governing disinformation would also offer deeper insight into shared global responsibilities.

Conflict of Interest

The authors showed no conflict of interest.

Funding

The authors did not mention any funding for this research.

References

Agunlejika, T. (2025). AI-Driven Fact-Checking in Journalism: Enhancing Information Veracity and Combating Misinformation: A Systematic Review. *Available at SSRN 5122225*.

Ahmad, W., Khan, A. K., Baloch, R. N., Asif, W. Z. A., Wazir, S., & ul Islam, M. (2022). Critical Analysis of the Recent Legislation and Initiatives to Curb Fake News and Disinformation in Pakistan: Challenges and Way Forward.

Ahmed, F. A., Zafar, S., & Gul, S. (2025). Analyzing PECA Amendments: Press Freedom, Democratic Values, and Digital Regulation in Pakistan. *Traditional Journal of Law and Social Sciences, 4*(01), 41-51.

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. Journal of Economic Perspectives, 31(2), 211–236. DOI: 10.1257/jep.31.2.211

Amri, S. (2024). FACTS-ON: Fighting Against Counterfeit Truths in Online Social Networks: fake news, misinformation and disinformation.

Anandharaj, N. (2024). AI-Powered Cloud Security: A Study on the Integration of Artificial Intelligence and Machine Learning for Improved Threat Detection and Prevention. *J. Recent Trends Comput. Sci. Eng. (JRTCSE), 12*, 21-30.

Au, C. H., Ho, K. K., & Chiu, D. K. (2022). The role of online misinformation and fake news in ideological polarization: barriers, catalysts, and implications. *Information Systems Frontiers*, 1-24.

Baptista, J. P., & Gradim, A. (2022). A working definition of fake news. *Encyclopedia, 2*(1).

Bhutto, F. (2024). Trust in Public Institutions: Causes of Decline and Ways to Restore It. *Research Consortium Archive, 2*(3), 123-131.

Buehler, M., Schatz, E., Ali, S. M., Greene, C., & Sombatpoonsiri, J. (2021). How information disorder affirms authoritarianism and destabilizes democracy: Evidence, trends, and actionable mitigation strategies from Asia and the Pacific. *US Agency for International Development*. http://dx.doi.org/10.2139/ssrn.3996805

Butt, M. N., Riaz, M., & Rabbani, A. W. (2023). Countering Fake News in Pakistan: Challenges Faced by Newsrooms and Regulators. *Mairaj, 2*(2), 79-87. DOI: https://doi.org/10.58760/mairaj.v2i2.31

Chawla, S. (2023). India's Neighbourhood: Challenges and Opportunities.

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. *Ieee Access, 10*, 85701-85719. DOI: 10.1109/ACCESS.2022.3197899

Creswell, J. W., & Plano Clark, V. L. (2017). Designing and Conducting Mixed Methods Research.

Dame Adjin-Tettey, T. (2022). Combating fake news, disinformation, and misinformation: Experimental evidence for media literacy education. *Cogent Arts & Humanities, 9*(1), 2037229.

de Zayas, A. (2022). *Countering Mainstream Narratives: Fake News, Fake Law, Fake Freedom*: SCB Distributors.

Fadiran, O. A. (2024). Fake News On Social Media and its Implication on National Security.

Galal, S., Nagy, N., & El-Sharkawi, M. E. (2021). Cnmf: A community-based fake news mitigation framework. *Information, 12*(9), 376. https://doi.org/10.3390/info12090376

Garaschuk, D. (2024). Digital Echo Chambers: Amplifying Populist Rhetoric in the Age of Social Media. *Current Problems of Philosophy and Sociology* (46), 152-157. DOI https://doi.org/10.32782/apfs.v046.2024.26

Guess, A. M., Nyhan, B., & Reifler, J. (2020). Exposure to untrustworthy websites in the 2016 US election. *Nature human behaviour*, *4*(5), 472-480.

Guigon, V., Villeval, M. C., & Dreher, J.-C. (2024). Metacognition biases information seeking in assessing ambiguous news. *Communications Psychology*, *2*(1), 122.

Gwadi, I. W., & Igbashangev, P. A. (2024). Evaluating the Impact of Artificial Intelligence on Fact-Checking Social Media Content in Nigeria: An Analysis of Tools and Strategies for Combating Misinformation during Elections. *Available at Ssrn 5015986*. http://dx.doi.org/10.2139/ssrn.5015986

Haque, E. U., Abbasi, W., Murugesan, S., Anwar, M. S., Khan, F., & Lee, Y. (2023). Cyber forensic investigation infrastructure of Pakistan: an analysis of the cyber threat landscape and readiness. *Ieee Access, 11*, 40049-40063. DOI: 10.1109/ACCESS.2023.3268529

Harwell, D. (2023). CISA and Tech Giants Combat Election Disinformation. Washington Cyber Policy Weekly.

Jalli, N. (2025). Viral Justice: TikTok Activism, Misinformation, and the Fight for Social Change in Southeast Asia. *Social Media+ Society*, *11*(1), 20563051251318122.

Khan, S. U., Shah, I. U., Shah, K., & Iqbal, M. J. (2025). The Role of China-Pakistan Relations in the Global Tech Competition, Especially in Areas like 5G, AI, and Cybersecurity. *Review of Education, Administration & Law*, *8*(1), 73-85. DOI: https://doi.org/10.47067/real.v8i1.404

Khan, Y. H., Mallhi, T. H., Alotaibi, N. H., Alzarea, A. I., Alanazi, A. S., Tanveer, N., & Hashmi, F. K. (2020). Threat of Covid-19 vaccine hesitancy in Pakistan: the need for measures to neutralize misleading narratives. *The American journal of tropical medicine and hygiene*, *103*(2), 603. DOI: https://doi.org/10.4269/ajtmh.20-0654

Lee, H. (2020). Digital Literacy Campaigns and Disinformation Control: Lessons from South Korea. Media Studies Review, *14*(3), 221–239.

McCombs, M. E., & Shaw, D. L. (1972). The agenda-setting function of mass media. Public Opinion Quarterly, *36*(2), 176–187. https://doi.org/10.1086/267990

McHugh, M. L. (2012). Interrater reliability: the kappa statistic. Biochemia Medica, *22*(3), 276–282. DOI: 10.11613/BM.2012.031

Murayama, T., Wakamiya, S., Aramaki, E., & Kobayashi, R. (2021). Modeling the spread of fake news on Twitter. *Plos one*, *16*(4), e0250419.

Ngai, C. S. B., Singh, R. G., & Yao, L. (2022). Impact of Covid-19 vaccine misinformation on social media virality: content analysis of message themes and writing strategies. *Journal of medical Internet research*, *24*(7), e37806. doi: 10.2196/37806

Niazi, B. K. N. B. K., & Iqbal, J. (2022). Exploring and Critically Analyzing Cybercrime Legislation and Digital Rights in Pakistan: Challenges and Prospects. *Indus Journal of Law and Social Sciences, 1*(1), 1-8.

Pennycook, G., & Rand, D. G. (2019). Fighting misinformation on social media using crowdsourced judgments of news source quality. *Proceedings of the National Academy of Sciences, 116*(7), 2521-2526. https://doi.org/10.1073/pnas.180678111

Pettit, J. E. (2022). *Political sectarianism, disinformation, and cyber threats.* Iowa State University,

Pomeranz, J. L., & Schwid, A. R. (2021). Governmental actions to address Covid-19 misinformation. *Journal of public health policy, 42*(2), 201.

Rana, J. I., & Rauf, S. (2024). Cybersecurity Legislation and Global Standards: A Comparative Analysis of Pakistan's Peca 2016 and Un Guidelines On Disinformation. *Sociology & Cultural Research Review, 2*(4), 489-507.

Rid, T. (2020). Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux.

Rubin, V. L. (2022). Manipulation in marketing, Advertising, propaganda, and public relations. In *Misinformation and disinformation: Detecting Fakes with the eye and AI* (pp. 157-205): Springer.

Rusydi, M. T. (2024). Evaluating Global Cybersecurity Laws: Efectiveness of Legal Frameworks and Enforcement Mecanism in the Digital Age. *Walisongo Law Review (Walrev), 6*(1), 71-83.

Saeidnia, H. R., Hosseini, E., Lund, B., Tehrani, M. A., Zaker, S., & Molaei, S. (2025). Artificial intelligence in the battle against disinformation and misinformation: a systematic review of challenges and approaches. *Knowledge and Information Systems*, 1-20.

Saleem, B., Ahmed, M., Zahra, M., Hassan, F., Iqbal, M. A., & Muhammad, Z. (2024). 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, 5*(4), 533-561.

Sarts, J. (2020). Disinformation as a threat to national security. In *Disinformation and fake news* (pp. 23-33): Springer.

Shahzad, K., & Khan, S. A. (2024). Relationship between new media literacy (NML) and web-based fake news epidemic control: a systematic literature review. *Global Knowledge, Memory and Communication, 73*(6/7), 956-983. https://doi.org/10.1108/GKMC-08-2022-0197

Shahzad, S., & Khan, A. (2024). Adoption of AI in Warfare: Comparative Study of India and Pakistan. *International" Journal of Academic Research for Humanities", 4*(2), 70-85.

Shu, K., Sliva, A., Wang, S., Tang, J., & Liu, H. (2020). Fake news detection on social media: A data mining perspective. Acm Sigkdd Explorations Newsletter, *19*(1), 22–36. https://doi.org/10.1145/3137597.3137600

Smith, A. (2021). AI Moderation and the Future of Digital Misinformation. *Journal of Cyber Policy*, *6*(2), 110–125.

Tandoc Jr, E. C., Lim, Z. W., & Ling, R. (2018). Defining “fake news” A typology of scholarly definitions. *Digital journalism, 6*(2), 137-153.

Tosoni, S., Mascheroni, G., & Colombo, F. (2022). 4. A Media-Studies Take on Social Robots as Media-Machines. *Humane Robotics*, 265.

UK Parliament. (2022). Online Safety Bill: Parliamentary Report.

Usman, B., Eric Msughter, A., & Olaitan Ridwanullah, A. (2022). Social media literacy: fake news consumption and perception of Covid-19 in Nigeria. *Cogent Arts & Humanities, 9*(1), 2138011.

Usman, S. M. (2024). Pakistan in the Crosshairs and the Rising Stakes of Strategic Information Warfare. *Journal of Research in Social Sciences, 12*(1), 1-23.

Vese, D. (2022). Governing fake news: the regulation of social media and the right to freedom of expression in the era of emergency. *European Journal of Risk Regulation, 13*(3), 477-513. DOI: https://doi.org/10.1017/err.2021.48

Wardle, C., & Derakhshan, H. (2017). Information Disorder: Toward an interdisciplinary framework for research and policymaking. Council of Europe.

Yousaf, M. N., Shah, M. A., & Khalid, M. (2024). Combating fake news and propaganda: policy approaches for safeguarding media integrity and public trust in Pakistan. *Assaj, 2*(4), 524-533.

Zhou, Q., Li, B., Scheibenzuber, C., & Li, H. (2023). Fake news land? Exploring the impact of social media affordances on user behavioural responses: A mixed-methods research. *Computers in Human Behaviour, 148*, 107889. https://doi.org/10.1016/j.chb.2023.107889