JOURNAL FOR SOCIAL SCIENCE STUDIES
An International Peer-Reviewed Open Access Journal

ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4 • Issue 5 • September 2026

PAKISTAN'S GROWING CYBERSECURITY CRISIS: EMERGING THREATS, CHALLENGES, AND POLICY RESPONSES

Dr. Tehzeeb-ul-Hassan[1], Muhammad Ismail[*2]

[1]SDPO Headquarter City Skardu / Former Visiting Assistant Professor Department of Sociology and Anthropology, Karakoram International University
*[*2]PhD Scholar, Department of Political Science, University of Karachi, Pakistan*

[1]drtehzeebulhassan@gmail.com, [*2]ismail.hamza@ymail,com

DOI: https://doi.org/10.5281/zenodo.23014217

Keywords
Cybercrime, Cybersecurity, Digital Vulnerabilities, Gilgit-Baltistan, Pakistan

Article History
Received: 21 June 2026
Accepted: 12 September 2026
Published: 28 September 2026

Copyright @Author
Corresponding Author: *
Muhammad Ismail

Abstract
The rapid growth of digital technology and internet usage in Pakistan has increased the risk of cybercrime, creating serious challenges for national security, economic stability, and individual privacy. Cybercrimes such as hacking, online fraud, identity theft, cyber harassment, phishing, and social media misuse are becoming increasingly common. This study examines the rise of cybercrime in Pakistan with special reference to Gilgit-Baltistan, a region experiencing growing digital connectivity but limited cybersecurity infrastructure. The research highlights emerging threats, digital vulnerabilities, and security challenges faced by individuals and institutions in the region. Poor digital literacy, weak law enforcement capacity, and limited cyber awareness increase the exposure of citizens to online crimes. Using a qualitative research methodology, the study analyzes secondary data from academic literature, government reports, and media sources. The study concludes that stronger cybersecurity policies, digital awareness programs, and institutional reforms are necessary to reduce cyber threats and improve digital security in Pakistan, particularly in Gilgit-Baltistan.

Introduction

Cybercrime has emerged as one of the fastest-growing security challenges in Pakistan due to the rapid expansion of digital technologies, internet penetration, mobile banking, and social media usage. The increasing dependence on digital communication has created new opportunities for economic growth and connectivity, but it has also exposed individuals, institutions, and governments to cyber threats such as hacking, online fraud, identity theft, cyber harassment, and financial scams. In recent years, Pakistan has witnessed a sharp increase in cybercrime complaints, reflecting the growing vulnerability of its digital environment. According to official reports, thousands of cybercrime complaints are registered annually, with digital fraud and social media hacking becoming major concerns nationwide. The establishment of legal and institutional frameworks such as the Prevention of Electronic Crimes Act (PECA) 2016 and the role of the Federal Investigation Agency Cyber Crime Wing demonstrate Pakistan's efforts to address cyber threats. However, the rapid evolution of technology has made cybercrime more sophisticated than the country's existing cybersecurity mechanisms. Weak law enforcement capacity, limited digital literacy, lack of cybersecurity awareness, and insufficient technical infrastructure continue to create gaps in cybercrime prevention and investigation.

JOURNAL FOR SOCIAL SCIENCE STUDIES
An International Peer-Reviewed Open Access Journal

ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4 • Issue 5 • September 2026

Reports indicate that only a limited number of complaints are converted into formal investigations and convictions, highlighting institutional weaknesses in cyber governance (Haque, et, al,2023).

Gilgit-Baltistan has become increasingly vulnerable to cybercrime due to expanding internet access, tourism-related digital activities, mobile banking, and social media usage. Although the region is geographically remote, technological connectivity has integrated it into Pakistan's broader digital landscape. At the same time, limited cybersecurity infrastructure, poor digital awareness, weak internet systems, and inadequate cyber policing have increased the risks of online fraud, SIM misuse, fake social media accounts, and digital financial crimes in the region. Local authorities have recently conducted operations against illegal SIM sales and mobile IMEI cloning in Gilgit, reflecting the seriousness of emerging cyber threats in the area. The unique geographical and strategic importance of Gilgit-Baltistan further increases cybersecurity concerns. The region borders China, Afghanistan, and India, making it sensitive from both national security and geopolitical perspectives. Cyber vulnerabilities in such strategically important areas can contribute to illegal surveillance, financial crimes, misinformation campaigns, and transnational digital threats. Weak digital infrastructure and unreliable internet services in remote districts also create challenges for implementing effective cybersecurity systems and digital governance.

The rise of cybercrime in Pakistan with special reference to Gilgit-Baltistan by analyzing emerging threats, digital vulnerabilities, and security challenges. It explores the major forms of cybercrime affecting the region, the institutional and legal response mechanisms, and the broader implications for national and regional security. The research also highlights the importance of cybersecurity awareness, technological capacity-building, and policy reforms in strengthening Pakistan's digital security framework.

Emerging Threats of Cybercrime in Pakistan

Pakistan is facing multiple forms of cyber threats including online financial fraud, identity theft, cyber harassment, ransomware attacks, social media manipulation, and hacking of digital accounts. WhatsApp hacking, phishing scams, and mobile banking fraud have become increasingly common across the country. Recent reports show that cybercrime incidents increased significantly in Pakistan, largely due to low digital literacy and the misuse of personal data by cybercriminals. Another growing concern is the illegal sale of foreign SIM cards, IMEI tampering, and cloned mobile phones, which enable anonymous communication and criminal activities. In Gilgit, law enforcement agencies have conducted several raids against illegal mobile cloning networks and unauthorized SIM distribution. These activities are often linked to financial fraud, extortion, and organized criminal operations. Cyber harassment and online blackmail have also emerged as serious social issues, particularly affecting women and young people. Social media platforms are frequently used for fake accounts, data theft, and cyberbullying. The misuse of digital platforms has increased psychological insecurity and social vulnerability among internet users in Pakistan (Farrukh, 2025).

Cyber Crime in Gilgit-Baltistan

Cybercrime in Gilgit-Baltistan has emerged as a growing security and social challenge due to the rapid expansion of internet access, mobile phone usage, social media platforms, and digital financial services. Although Gilgit-Baltistan is geographically remote, technological development and increasing digital connectivity have integrated the region into Pakistan's broader cyber environment. The use of smartphones, online banking, e-commerce, and tourism-related digital services has increased significantly in cities such as Gilgit, Skardu, and Hunza, creating both opportunities and risks in the digital sphere. The rise of cybercrime in the region includes activities such as online fraud, hacking of social media accounts, cyber harassment, fake online advertisements, identity

ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4 • Issue 5 • September 2026

theft, financial scams, and misuse of mobile SIM cards. Many people in Gilgit-Baltistan have limited awareness regarding cybersecurity and safe internet practices, making them vulnerable to cybercriminals. Young people, students, and social media users are particularly exposed to online scams, fake profiles, and cyberbullying. One major challenge in Gilgit-Baltistan is the lack of strong digital infrastructure and cybersecurity institutions. Internet services in many districts remain slow and unstable, while specialized cybercrime investigation units and trained cybersecurity experts are limited. Most cybercrime cases depend on federal institutions such as the Federal Investigation Agency (FIA), which creates delays in investigation and legal action. The shortage of digital literacy programs and cybersecurity education further weakens the region's capacity to respond effectively to cyber threats (Kashif, et, al, 2025).

The tourism industry and growing online business activities have also increased cybersecurity concerns in Gilgit-Baltistan. Hotels, travel agencies, and local businesses increasingly rely on digital payment systems and social media marketing, which expose them to online fraud and hacking risks. Similarly, the misuse of social media platforms for spreading misinformation, blackmail, and fake news has become an emerging social problem in the region. The Gilgit-Baltistan's strategic location near international borders also increases the importance of cybersecurity from a national security perspective. The region is connected to the China-Pakistan Economic Corridor (CPEC), making digital security and communication protection important for both economic and strategic stability. Cyber threats targeting digital infrastructure, communication systems, or financial networks can therefore have broader implications for regional security and development. Cybercrime in Gilgit-Baltistan is becoming an important issue that requires immediate attention from government institutions, law enforcement agencies, educational organizations, and civil society. Strengthening cybersecurity awareness, improving internet infrastructure, establishing regional cybercrime response centers, and promoting digital education are essential steps for protecting citizens and ensuring a secure digital environment in Gilgit-Baltistan. The Several cybercrime cases have recently emerged in Gilgit-Baltistan, highlighting the region's growing digital security challenges. One major case involved raids conducted by the Pakistan Telecommunication Authority (PTA) and the National Cyber Crime Investigation Agency (NCCIA) against mobile repair shops in Gilgit and Hunza for illegal IMEI tampering and cloned mobile phone sales. Authorities seized laptops, software, and digital equipment used for altering mobile identities, while suspects were arrested for facilitating cybercrime and financial fraud another important cyber-related case involved the illegal sale of foreign SIM cards in Danyore, Gilgit. FIA Cyber Crime Wing officials arrested suspects accused of using international SIMs for online fraud, blackmail, fake schemes, and extortion activities through social media platforms (Amin, et, al, 2025).

The Cases of digital fraud have also increased in Gilgit-Baltistan through fake investment schemes and online scams. Reports indicate that residents from Hunza and Baltistan lost millions of rupees in fraudulent online trading and Ponzi-style schemes operating through digital applications and social media platforms. Cyber harassment and online violence against women have become another serious concern in Gilgit-Baltistan. Experts and civil society organizations have warned about rising incidents of cyberstalking, fake social media accounts, deep fake content, and non-consensual sharing of personal information targeting women and girls in the region. Additionally, digital identity misuse and fake documentation have emerged as cybersecurity issues. A recent verification drive in Gilgit-Baltistan uncovered over 310,000 fake CNIC entries linked to subsidy schemes, revealing weaknesses in digital record management and identity verification systems. These cases demonstrate that Gilgit-Baltistan is increasingly vulnerable to cyber threats due to weak cybersecurity infrastructure, low digital literacy, limited internet regulation, and inadequate cybercrime response mechanisms. Strengthening digital awareness, law

ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4 • Issue 5 • September 2026

enforcement capacity, and cybersecurity regulations is therefore essential for protecting citizens and institutions in the region (Majid, et, al, 2025).

Theoretical Framework

This study will use the Cyber Security Theory and Routine Activity Theory as analytical frameworks. The Routine Activity Theory explains that cybercrime occurs when a motivated offender targets a vulnerable digital user in the absence of effective cyber protection. The theory is relevant because many cybercrimes in Pakistan and Gilgit-Baltistan occur due to weak digital awareness and inadequate cyber security mechanisms. The Cyber Security Theory focuses on protecting digital infrastructure, networks, and information systems from cyber threats. The theory is suitable because the study examines cyber vulnerabilities, security risks, and institutional responses in Pakistan and Gilgit-Baltistan.

Cyber Crime in Pakistan

Cybercrime has become one of the most significant non-traditional security threats in Pakistan due to the rapid expansion of digital technologies, internet usage, online banking, and social media platforms. The growing dependence on digital communication has transformed economic, educational, and social activities, but it has also increased the risks of online fraud, hacking, cyber harassment, identity theft, and financial crimes. Pakistan has experienced a considerable rise in cybercrime cases in recent years, reflecting weaknesses in cybersecurity awareness, digital governance, and institutional capacity. The introduction of smartphones and affordable internet services has accelerated digital connectivity across urban and remote regions alike. Gilgit-Baltistan, despite its mountainous geography and limited infrastructure, has also become increasingly connected through mobile networks and internet services. The rise of tourism, online businesses, digital banking, and social media usage in Gilgit-Baltistan has created new opportunities for economic growth and communication. However, these developments have simultaneously exposed the region to various cyber threats and digital vulnerabilities. Cybercriminal activities in Pakistan include phishing scams, social media hacking, fake online investment schemes, cyberbullying, online blackmail, SIM card misuse, and digital financial fraud. Gilgit-Baltistan faces additional challenges due to weak cyber infrastructure, low digital literacy, limited law enforcement capacity, and unreliable internet systems. The absence of specialized cybersecurity institutions in the region further increases the vulnerability of citizens and businesses to online crimes. The strategic importance of Gilgit-Baltistan also raises national security concerns regarding cybersecurity. The region shares borders with China, India, and Afghanistan and is linked to major projects such as the China-Pakistan Economic Corridor (CPEC). Cyber threats targeting communication systems, digital infrastructure, or financial networks in the region can therefore have broader economic and geopolitical implications (Sultan, et, al, 2025).

This study examines the growing problem of cybercrime in Pakistan with special reference to Gilgit-Baltistan. It highlights emerging cyber threats, digital vulnerabilities, institutional weaknesses, and security challenges while exploring the need for effective cybersecurity policies, public awareness, and technological reforms to strengthen digital security in the region and the country as a whole.

Digital Vulnerabilities in Gilgit-Baltistan

The digital vulnerabilities of Gilgit-Baltistan are closely linked to weak technological infrastructure, limited cybersecurity awareness, and inadequate internet connectivity. Many districts in the region experience unstable internet services, which affect both communication security and digital governance. Local discussions frequently highlight the poor quality of internet access in districts such as Ghizer, where residents face severe connectivity problems despite increasing reliance on digital communication. Tourism growth and digital business activities in Hunza, Gilgit, and Skardu have increased the region's exposure to cyber risks. Hotels, travel services, and small

JOURNAL FOR SOCIAL SCIENCE STUDIES
An International Peer-Reviewed Open Access Journal
ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4 • Issue 5 • September 2026

businesses increasingly rely on online payment systems and digital marketing, making them vulnerable to hacking, fraud, and data breaches. The introduction of surveillance software and cybersecurity regulations in tourism-related businesses reflects growing concerns about digital security in the region. The lack of specialized cybercrime units and trained cybersecurity professionals in Gilgit-Baltistan further weakens the region's ability to respond effectively to cyber threats. Most cybercrime investigations depend on federal institutions located outside the region, which creates delays in reporting, investigation, and prosecution (Khattak, et, al, 2025).

Security Challenges and National Implications

Cybercrime poses serious security challenges for Pakistan because it threatens economic stability, public trust, and national security. Financial fraud and online scams undermine confidence in digital banking and e-commerce systems, while cyberattacks on government institutions can disrupt critical infrastructure and public administration. The Gilgit-Baltistan's strategic location makes cybersecurity particularly important. The region is connected to major projects such as the China-Pakistan Economic Corridor, which relies heavily on digital communication and technological systems. Cyber threats targeting communication networks, financial systems, or infrastructure projects could have broader geopolitical and economic consequences. Cross-border cyber threats also remain a major concern. Pakistan has experienced incidents involving hacking of institutional websites and cyber propaganda campaigns, demonstrating the growing role of cyberspace in regional conflicts and information warfare. Furthermore, the low conviction rate in cybercrime cases reflects institutional weaknesses in Pakistan's cybersecurity governance. Although complaints continue to increase, limited technical expertise, outdated investigative tools, and legal complications reduce the effectiveness of cybercrime enforcement mechanisms (Iftikhar, 2023).

Pakistan's Growing Cybersecurity Crisis

Challenges

Policy Responses

Pakistan's growing cybersecurity challenges require a comprehensive policy response that combines legal reform, institutional strengthening, technological modernization, human-resource development, public awareness, and international cooperation. Although Pakistan has introduced important initiatives such as the National Cyber Security Policy 2021, CERT Rules 2023, National CERT, and the Pakistan Information Security Framework 2026, effective cybersecurity depends on translating these frameworks into consistent institutional practice. The following policy responses are particularly relevant.

Strengthening National CERT

Pakistan should further strengthen the National Cyber Emergency Response Team (National CERT) as a central institution for national cyber incident coordination. Its capabilities should include continuous threat monitoring, vulnerability assessment, incident response, malware analysis, threat intelligence, and coordination among government and private-sector organizations. A stronger National CERT can improve the country's ability to detect cyber incidents at an early stage and coordinate rapid responses.

Protection of Critical Information Infrastructure

Critical information infrastructure—including banking, telecommunications, energy, healthcare, transportation, and government systems—requires specialized cybersecurity protection. Government should establish sector-specific security standards, mandatory risk assessments, regular security audits, vulnerability assessments, and incident-response plans. Organizations operating critical infrastructure should also conduct periodic cybersecurity exercises to test their preparedness.

JOURNAL FOR SOCIAL SCIENCE STUDIES
An International Peer-Reviewed Open Access Journal
ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4 • Issue 5 • September 2026

Development of Cybersecurity Human Resources

A shortage of specialized cybersecurity professionals remains an important challenge. Pakistan should expand university programmes and professional training in cybersecurity, digital forensics, cryptography, network security, artificial intelligence security, cloud security, and cybercrime investigation. Greater collaboration between universities, government institutions, and technology companies could provide students with practical experience and improve the supply of qualified cybersecurity professionals.

Strengthening Cybercrime Investigation

Law-enforcement agencies require greater technical capacity to investigate cybercrime. Specialized cybercrime units should be equipped with modern digital-forensics laboratories, trained investigators, forensic software, secure evidence-management systems, and appropriate technical resources. Cooperation between law-enforcement agencies, National CERT, telecommunications companies, banks, and technology firms can improve the investigation and prosecution of cybercrime.

Improving Cybersecurity Awareness

Cybersecurity awareness should become a national priority. Government institutions, universities, schools, businesses, and civil-society organizations should conduct regular awareness programmes addressing phishing, password security, social engineering, identity theft, online financial fraud, malicious links, and privacy protection. Employees working with sensitive information should receive periodic cybersecurity training rather than relying on one-time awareness sessions.

Pakistan's cybersecurity policy should therefore move toward a proactive, preventive, intelligence-driven, and resilience-oriented model. The National Cyber Security Policy 2021 provides an important foundation, while National CERT and subsequent institutional developments provide mechanisms for implementation. The major policy task is to strengthen coordination, technical capacity, human resources, critical-infrastructure protection, cybersecurity awareness, and continuous monitoring so that policy commitments translate into operational cyber resilience.

Inspector General of Police Gilgit-Baltistan Cybersecurity

The Dr. Akbar Nasir Khan is the current Inspector General of Police, Gilgit-Baltistan, having assumed office in February 2026. He also has previous experience as the founding COO of the Punjab Safe Cities Authority and has emphasized technology-oriented policing and safe-city approaches.

Smart-City Policing and Cybersecurity in Gilgit and Skardu

The current leadership of Gilgit-Baltistan Police under IGP Dr. Akbar Nasir Khan provides an important opportunity to integrate smart-city technologies with cybersecurity in District Gilgit and District Skardu**.** Dr. Akbar Nasir Khan's previous experience as the founding Chief Operating Officer of the Punjab Safe Cities Authority is particularly relevant because safe-city systems depend on integrated command-and-control centers, digital communications, surveillance technologies, data management, and technology-driven policing. In Gilgit and Skardu, the development of smart-city policing could involve CCTV networks, automated monitoring, emergency-response systems, digital crime reporting, traffic-management technologies, and interconnected police databases. However, these systems should be designed with cybersecurity safeguards from the beginning because the concentration of surveillance, citizen, and law-enforcement data can create significant risks if systems are compromised.

Cybersecurity should therefore constitute a central component of any smart-city initiative in Gilgit and Skardu. Connected CCTV cameras, sensors, communication networks, police databases, command centers, and digital evidence-management systems can become potential targets for unauthorized access, ransomware, data theft, or disruption. A smart-

JOURNAL FOR SOCIAL SCIENCE STUDIES
An International Peer-Reviewed Open Access Journal
ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4 • Issue 5 • September 2026

city system should consequently employ encryption, multi-factor authentication, network segmentation, continuous monitoring, secure cloud infrastructure, regular vulnerability assessments, and clearly defined access controls. The experience and policy orientation of Dr. Akbar Nasir Khan toward technology-oriented policing can provide a basis for developing a more integrated approach in which public safety and cybersecurity are treated as interconnected dimensions of modern policing. His earlier public work has also addressed the relationship between surveillance, security, privacy, and safe-city systems.

For District Gilgit and District Skardu, a smart-city cybersecurity strategy could further establish dedicated cyber-security and digital-forensics capabilities within the police structure, supported by National CERT, relevant government agencies, universities, and private technology providers. Police personnel should receive specialized training in cybercrime investigation, digital evidence preservation, cyber threat detection, and incident response. Regular cybersecurity audits and simulated cyber incidents could be conducted to test the resilience of smart-city infrastructure. Such an approach would allow smart-city technologies to support crime prevention and emergency response while also protecting citizens' privacy and sensitive law-enforcement information. The broader security environment in Gilgit-Baltistan already requires coordination among institutions, as reflected in the August 2026 Apex Committee meeting chaired by the Chief Minister, where the overall security situation and protection of major development projects were reviewed.

Conclusion

The rise of cybercrime in Pakistan represents a major challenge to national security, economic stability, and social protection in the digital age. Gilgit-Baltistan, despite its remote geography, has become increasingly exposed to cyber threats due to expanding digital connectivity, tourism development, and growing online activities. Emerging threats such as online fraud, SIM misuse, IMEI cloning, cyber harassment, and digital financial crimes highlight the urgent need for stronger cybersecurity measures in the region. Pakistan must strengthen its cybersecurity framework through improved digital literacy, institutional reforms, technological modernization, and effective law enforcement mechanisms. In Gilgit-Baltistan, special attention should be given to expanding secure internet infrastructure, establishing regional cybercrime response units, and promoting cybersecurity awareness among citizens and businesses. A coordinated approach involving government institutions, law enforcement agencies, educational institutions, and civil society is essential for building a secure and resilient digital environment in Pakistan.

The rise of cybercrime in Pakistan has become one of the most serious challenges of the digital age. The increasing use of smartphones, internet services, social media platforms, and online banking has created new opportunities for communication and economic growth, but it has also increased exposure to cyber threats. Cybercrimes such as hacking, phishing, identity theft, cyber harassment, online fraud, and data breaches are growing rapidly across the country. These challenges highlight the urgent need for stronger cybersecurity measures and effective digital governance.

Gilgit-Baltistan, despite its geographical remoteness, is also experiencing the impact of digital transformation. The expansion of internet connectivity and digital communication in the region has increased access to online services and educational opportunities. However, the region lacks sufficient cybersecurity infrastructure, technical expertise, and institutional capacity to address emerging cyber threats effectively. This has made local communities increasingly vulnerable to cybercrime and digital exploitation. One major finding of this study is that low digital literacy remains a significant factor contributing to cyber vulnerability in Pakistan and Gilgit-Baltistan. Many internet users are unaware of online safety practices, making them easy targets for cybercriminals. Fake links, phishing scams, social media fraud, and online financial deception continue to affect individuals who

ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4 • Issue 5 • September 2026

lack awareness regarding digital security and privacy protection.

The study also finds that cyber harassment and online abuse have become growing social issues, particularly for women and young internet users. Social media misuse, fake accounts, blackmail, and privacy violations have created psychological and social challenges for victims. In conservative and remote areas such as Gilgit-Baltistan, these incidents are often underreported due to social stigma, lack of awareness, and limited legal support systems. Another important conclusion is that Pakistan's legal and institutional mechanisms for combating cybercrime still face significant limitations. Although the Prevention of Electronic Crimes Act (PECA) 2016 provides a legal framework to address cyber offenses, weak implementation, limited investigative resources, and slow judicial processes reduce its overall effectiveness. Law enforcement agencies often struggle with technical expertise and modern cyber forensic capabilities. that technological advancements have increased both opportunities and risks in cyberspace. Artificial intelligence, encrypted communication, digital financial systems, and social media algorithms have transformed the nature of cyber threats. Cybercriminals are using sophisticated methods to target individuals, businesses, and institutions, making cybercrime more complex and difficult to control.

The strategic importance of Gilgit-Baltistan also adds another dimension to cybersecurity concerns. As the region gains importance through tourism, trade routes, and digital connectivity projects, cyber threats may increasingly affect communication systems, local businesses, and public institutions. Protecting digital infrastructure in sensitive and strategically significant regions is therefore becoming a national security priority for Pakistan. The study concludes that public awareness and cybersecurity education are essential for reducing digital vulnerabilities. Schools, universities, government institutions, and media organizations must promote cyber awareness programs to educate citizens about safe internet usage, online privacy, and digital ethics. Increasing public understanding of cyber risks can significantly reduce the success of online scams and cyber exploitation.

Furthermore, institutional coordination between government agencies, telecommunication authorities, educational institutions, and cybersecurity organizations is necessary to develop a comprehensive cyber defense strategy. Investment in cyber forensic laboratories, trained cybersecurity professionals, secure digital systems, and modern investigative technologies can strengthen Pakistan's ability to respond effectively to cyber threats. The cybercrime in Pakistan, particularly in Gilgit-Baltistan, represents a growing challenge that requires immediate policy attention and long-term strategic planning. Strengthening cybersecurity laws, improving digital literacy, enhancing institutional capacity, and developing secure technological infrastructure are critical for ensuring digital safety and national security. A coordinated and proactive approach can help Pakistan minimize cyber threats and create a safer and more resilient digital environment for future generations.

REFERENCES:

Ehsan, S., Ismail, M., Ali, H., Ali, R., & Hussain, A. (2025). Evolving Challenges Of Climate Change: Exploring Non-Traditional Security Risks In Gilgit-Baltistan. *International Journal of Social Sciences Bulletin*, *3*(1), 57-64.

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.

Farrukh, T. (2025). A Critical Analysis of the Prevention of Electronic Crimes Act (PECA): Legislative Gaps and Enforcement Challenges in Pakistan. *Pakistan Journal of Social Science Review*, *4*(4), 1439-1448.

ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4 • Issue 5 • September 2026

Kashif, M., Shah, S. Z. A., & Ahmad, M. (2025). Impact of transnational criminal organizations on political, economic and social perspectives of Pakistan. *Bulletin of Business and Economics (BBE)*, *14*(1), 30-38.

Amin, F., Ali, S. A., & Hussain, S. (2025). Cyber Politics in South Asia: Navigating the Digital Battleground. *Journal of Regional Studies Review*, *4*(2), 26-37.

Majid, H., Mustafa, M., & Nazar, M. (2025). Digital access and women's work in Pakistan: Constraints, use patterns, and policy directions. *Development Policy Review*, *43*(6), e70042.

Sultan, S., & Ahmad, I. (2025). CPEC and Data Sovereignty: Legal and Cybersecurity Implications of Chinese Digital Infrastructure Projects. *Pakistan Journal of Social Science Review*, *4*(4), 906-920.

Khattak, T., & Asghar, R. J. (2024). Strategic Counter Measures to Terrorism and Extremism in Pakistan and Insights from Home Land Security: A Need for the Enactment of Pakistan's National Counter Terrorism Department. *Inverge Journal of Social Sciences*, *3*(1), 61-74.

Iftikhar, B. (2023). Digital Crime Scenes: Protecting Children from Sexual Exploitation in Pakistan. *Available at SSRN 5007631*.

Sattar, Z., Riaz, S., & Mian, A. U. (2018, November). Challenges of cybercrimes to implementation of legal framework. In *2018 14th International Conference on Emerging Technologies (ICET)* (pp. 1-5). IEEE.

Hussain, A. (2019). *Transport infrastructure development, tourism and livelihood strategies: An analysis of isolated communities of Gilgit-Baltistan, Pakistan* (Doctoral dissertation, Lincoln University).

Pakistan Telecommunication Authority. (2025, June 5). *PTA raids mobile repair shop tampering IMEIs and selling cloned phones in Gilgit*. ProPakistani. https://propakistani.pk/2025/06/05/pta-raids-mobile-repair-shop-tampering-imeis-and-selling-cloned-phones-in-gilgit/

Pakistan Telecommunication Authority & FIA. (2025, March 12). *PTA, FIA conduct raids against illegal pre-active foreign SIM sellers in Gilgit*. ProPakistani. https://propakistani.pk/2025/03/12/pta-fia-conduct-raids-against-illegal-pre-active-foreign-sim-sellers-in-gilgit/

Pamir Times. (2025, May 8). *Over 310,000 fake CNICs uncovered in Gilgit-Baltistan wheat subsidy scheme*. https://pamirtimes.net/2025/05/08/over-310000-fake-cnics-uncovered-in-gilgit-baltistan-wheat-subsidy-scheme/

Pamir Times. (2025, December 2). *Experts call for stronger cyber protection measures to end digital violence against women and girls*. https://pamirtimes.net/2025/12/02/experts-call-for-stronger-cyber-protection-measures-to-end-digital-violence-against-women-and-girls/

Reddit Community Discussion. (2025). *Online fraud and financial scam cases in Gilgit-Baltistan*. Reddit. https://www.reddit.com/r/GilgitBaltistan/comments/1jaezz0/

Reddit Community Discussion. (2025). *Internet security and cyber vulnerability issues in Gilgit-Baltistan*. Reddit. https://www.reddit.com/r/GilgitBaltistan/comments/1k3qb53/