ADVANCE SOCIAL SCIENCE ARCHIVE JOURNAL
Available Online: https://assajournal.com
Vol. 04 No. 01. July-September 2025.Page#.1358-1366
Print ISSN: 3006-2497 Online ISSN: 3006-2500
https://doi.org/10.55966/assaj.2025.4.1.080
Platform & Workflow by: Open Journal Systems

Cyber Crime in Pakistan: Trends, Challenges, and Legal Responses

Asad U Allah Khan
Advocate High Court
asadattorney2255@gmail.com

ABSTRACT

Cybercrime in Pakistan has emerged as a critical challenge, threatening economic stability, social harmony, and national security. This article examines the current trends, key challenges, and legal responses to cyber threats in Pakistan, offering a comprehensive analysis of the evolving digital landscape. The study highlights prevalent cybercrimes, including financial fraud, identity theft, cyber harassment, and data breaches, alongside emerging threats like ransomware, deepfake technology, and cyberterrorism. Despite legislative measures such as the Prevention of Electronic Crimes Act (PECA) 2016, systemic gaps in enforcement, technological infrastructure, and public awareness persist. The article identifies three major challenges: technical limitations (outdated cybersecurity systems, low digital literacy), institutional weaknesses (slow judicial processes, jurisdictional hurdles), and socio-cultural barriers (underreporting due to stigma, lack of victim support). Case studies of high-profile cyber incidents, such as banking fraud and social media blackmail, illustrate the real-world consequences of these vulnerabilities. The analysis concludes with actionable recommendations, emphasizing the need for government-led initiatives (strengthening law enforcement, fostering public-private partnerships), corporate and individual responsibility (adopting cybersecurity best practices, improving reporting mechanisms), and legal reforms (updating PECA, expediting cybercrime trials). Ultimately, this research underscores the urgency of treating cybersecurity as a national priority. By implementing a multi-stakeholder approach combining policy upgrades, technological investments, and public awareness campaigns Pakistan can mitigate cyber risks and secure its digital future. The findings advocate for immediate action to bridge existing gaps and build a resilient cyber ecosystem.

Keywords: *Cybercrime, Pakistan, PECA 2016, Cybersecurity, Financial Fraud, Cyber Harassment, Ransomware, Deepfake, Cyberterrorism, Legal Reforms, Digital Literacy, Public-Private Partnerships.*

Introduction

Cybercrime has become one of the most powerful obstacles of the digital era, which puts individuals, businesses and governments at risk on a worldwide level. It is also noted that cyber threats have become one of the five most significant risks globally and that the current projected financial losses are estimated to reach over ten trillion dollars by 2025 (WEF, 2023). This is a shocking number that highlights how ubiquitous digital threats have become in a world that is getting more and more interconnected. Pakistan is especially vulnerable in this environment; its digital transition was too quick to enable the establishment of well-developed cybersecurity systems. The country has experienced a surge in digital connectivity in an unprecedented scale

with internet penetration hitting 125 million users in 2024 (PTA, 2024), yet it has come along with equally stunning opportunities as well as serious vulnerabilities. The growth of mobile banking, e commerce platforms and social media networks has transformed the way Pakistanis engage with technology, however it has also given new opportunities to cybercriminals to exploit. Financial frauds, data breaches and identity theft are cases that have become more advanced and are not just nuisances, but they are systemic and require prompt legal, technical and social solutions.

The digital environment in Pakistan is a paradox of the progressive development of technology and the obvious security breach. On the one hand, the nation is experiencing a tremendous progress in the digital infrastructure, where the 5G experiments are being conducted, and the fintech adoption rate is skyrocketing (State Bank of Pakistan, 2024). The developments make Pakistan a potential participant in the digital world economy. Nonetheless, such developments are threatened by ineffective regulatory systems and a rather alarming ignorance of the masses regarding the existence of a cyber threat. According to the 2023 Kaspersky Lab cybersecurity report, Pakistan has experienced more than 500,000 cyberattacks in one year, and the most widespread type of threat is phishing schemes, ransomware attacks, and identity theft cases (Kaspersky Lab, 2023). The Federal Investigation Agency (FIA) documented a shocking rise in the number of complaints of cybercrime by 70 percent between the year 2022 and 2024, indicating a frightening trend of an increase in cybercrimes (FIA Cyber Crime Wing, 2024). The available enforcement mechanisms are still pathetically weak, not only due to legal uncertainties but also because of understaffed cybercrime units and a judiciary without special expertise in digital forensics and cyber law. This enforcement loophole gives the victims little legal options and gives the cybercriminals a free pass to do whatever they want to do, which is a vicious cycle that continues to increase digital insecurity.

The consequences of the unregulated cybercrime in Pakistan are far-reaching and highly detrimental to the economy of the country, national security, and social structure. The Pakistan Telecommunication Authority (PTA) has cautioned that the ongoing cybersecurity weakness might scare off foreign investment and the success of key digital governance projects such as the vision of a digital Pakistan (PTA, 2024). This is an economic risk that is extremely worrying because the nation is trying to become the technological and innovative centre of the region. The effects of cybercrime in society are also alarming, especially the explosion of online bullying against women and minorities. According to the report released by the Digital Rights Foundation in 2023, there was a 40 percent rise in the number of online gender-based violence, indicating how digital spaces are now being used as the means of suppression and harassment (DRF, 2023). These patterns also highlight the necessity of effective strategies that would integrate more robust laws with improved public-private cooperation and national awareness programs. With Pakistan still in the process of digital transformation, it is at a crossroads: either the nation focuses on cybersecurity as the essential component of its digital landscape or it will lose its economic and social development prospects. It is the time to act, because the price of not doing that in terms of financial losses, loss of trust in digital systems, and human pain are just too high to be neglected.

Current Trends of Cybercrime in Pakistan

Cybercrime in Pakistan has developed at a high pace with the reflection of global trends, but with the local challenges as well. Financial fraud is one of the most common threats, especially scammers using online banking and false investment opportunities. The State Bank of Pakistan (2024) stated that instances of digital banking fraud have increased by 62 percent in 2023 as

criminals use low-level authentication and social engineering strategies. Likewise, identity theft and phishing have become prevalent with the Pakistan Cybersecurity Council (PCC, 2023) observing that more than 45 percent of internet users in Pakistan have experienced phishing attacks that are sometimes presented as official messages in the form of government offices and banks. These offenses do not only result in losses of money but also decrease confidence in digital financial systems, which prevents the process of achieving a cashless economy in the country. The other current danger is cyber bullying, such as blackmail and false profiles, which are disproportionately affecting women and vulnerable groups. According to a 2023 study conducted by the Digital Rights Foundation (DRF), 65 percent of victims of online harassment in Pakistan had not reported them because they feared being stigmatized or because no legal action could be taken, showing the importance of tighter protective measures.

Besides these typical cyber crimes, there have been cases of hacking and data breaches that have hit both the private and the public institutions revealing sensitive information. According to the FIA Cyber Crime Wing (2024), the number of corporate information breaches increased by 30 percent in comparison with 2022, and the attackers frequently use outdated security measures. Meanwhile, fake news and misinformation have increased social and political tensions especially during times of elections and other crises. In 2023, at least 12 large scale instances of violence were realized in real life as a result of false narratives on platforms such as WhatsApp and Facebook (Media Matters for Democracy 2024). These trends indicate the complexity of cyber threats in Pakistan, and how the rate of technological development has exceeded the rate of regulatory and social preparedness.

Pakistan is already facing cybersecurity issues, but the new threat is combining with the already widespread ancient cybercrimes. The case of ransomware attacks is one such area, and the National Response Centre for Cyber Crimes (NR3C, 2024) has reported an increase of 90 percent in the number of ransomware attacks that target hospitals, educational institutions and SMEs. Cybercriminals usually cipher the most vital information and require the payment of cryptocurrency, and the victims have little opportunity to recover the information. The other expanding issue is the inappropriate use of deepfake technology, which has been politically weaponized, used to create revenge porn, and commit financial crimes. In a report published in 2024 by the Pakistan Institute of Development Economics (PIDE), it was advised that AI-based deepfakes would destabilize the trust of citizens in any media and government, with the example of fake videos of politicians that had been spread before elections. It is necessary to state that these processes demonstrate the importance of developing high-quality detection tools and awareness campaigns to fight with digital manipulation.

The threat that seems to be the most threatening to emerge is that of cyber-terrorism which threatens national security a lot. According to the Pakistan Electronic Media Regulatory Authority (PEMRA, 2024) state sponsored hacking groups have grown to target critical infrastructure, such as power grids and military communications. Moreover, the 2023 Global Crime Report by interpol also labeled Pakistan as a hub of the cybercriminal network in the South Asian region, where hackers use the vulnerable cybersecurity of the country to attack foreign destinations. These patterns indicate that cybercrime in Pakistan is no longer a matter of law enforcement but rather a national security priority that requires the integration of governmental and outsider firms, as well as foreign allies.

Challenges in Combating Cybercrime in Pakistan

The war on cybercrime in Pakistan is challenged by a lot of technical, legal and socio-cultural issues which are overall a weakness to the digital security system of the country. The combination of these intertwined barriers forms an ideal storm that enables the cybercriminals to act with impunity which requires serious and holistic measures to curb this situation.

The technical issues in the cybersecurity environment in Pakistan are not simple and complex. The country has a very weak cybersecurity system despite having more than 125 million internet users (PTA, 2024). The report created by the Pakistan Cybersecurity Council (PCC) in 2024 paints an alarming image, according to which over 60 percent of Pakistani companies do not implement even the most fundamental cybersecurity measures like encryption and multi-factor authentication. This weakness is worrying especially when we see a quick digitization of financial services, and government activities. As an example, the number of digital fraud cases in the banking industry has increased by 62 percent (State Bank of Pakistan, 2024), revealing significant vulnerabilities in the authentication system and transaction security systems. Adding insult to injury is the extreme digital literacy crisis. According to the 2023 survey conducted by the Digital Rights Foundation (DRF), 28 percent of Pakistani users of the internet would be able to reliably detect phishing attempts, with the majority still exposed to the threat of increasingly sophisticated social engineering attacks. Such knowledge gap is worsened by little investment on cybersecurity education at institutional and individual scales. The current digital safety education in schools and universities can hardly be considered thorough, and even corporate cybersecurity training programmes are more of an exception than a rule. The aftermath is dramatic - a world where people are getting more dependent on online services and are not capable of addressing risks, providing cybercriminals with fertile ground.

Although the theoretical framework of combating cybercrime in Pakistan is comprehensive, it is fatally impaired in terms of implementation. The Pakistan Prevention of Electronic Crimes Act (PECA) 2016, the backbone of the Pakistani cyber laws, has been found insufficiently effective against the modern risks as it has limitations in terms of its design as well as implementation. According to the Federal Investigation Agency (FIA) Cyber Crime Wing (2024), the conviction rate of cybercrime crimes is pathetic with only 15 per cent success rate, reflecting the failure of the justice system. These are due to several things: the obsolete digital forensics capabilities, the lack of dedicated cybercrime prosecutors and the lack of technical expertise of judicial officers. Cybercrime is transnational which poses other jurisdictional challenges. It is estimated that about 40% of cyberattacks on Pakistani organizations are launched by unknown addresses abroad, which leads to complicated legal issues in the investigation and prosecution process (PIDE, 2023). The MLAT (Mutual Legal Assistance Treaty) procedures are tedious and slow, and this trend tends to give the offenders a way out. Also, the absence of standardized mechanisms of cross-border data requests and evidence gathering often creates critical investigative dead-ends.

The worst evil perhaps is the socio-cultural drivers of cybercrime in Pakistan. According to the 2024 research conducted by the Aurat Foundation, more than 70 percent of victims of cyber harassment do not report the cases because of the fear of being stigmatized or facing retaliation, especially those women and marginalized communities. This underreporting crisis makes a vicious circle - the low rates of reporting contribute to the underestimation of the problem that subsequently leads to the inefficient allocation of resources to providing support to the victims and law enforcement potential. The level of awareness of the legal protection among people is appalling. According to a 2023 Gallup Pakistan survey, 35 percent of respondents had heard of the

provisions of PECA, which means that the majority of the citizens are not aware of their rights and the opportunity of recourse in cases of cybercrime. This knowledge divide is worst in rural settings and with less educated communities, which leads to a digital protection gap. The cultural response to victims of cybercrime, particularly online harassment or financial fraud, tends to further traumatize victims by victim-blaming instead of being supportive.

These related issues will have to be dealt with using a multi-faceted approach that will reinforce technical, legal, and social awareness simultaneously. In the technical area, short-term priorities involve obligatory cybersecurity requirements of business, increased digital literacy courses, and major investments in the national cybersecurity of countries. The legal changes are to be oriented at updating PECA, creating special cyber courts, and increasing the possibilities of international cooperation. The change of social attitudes should also be equally important, and it can be achieved by conducting the awareness campaigns nationwide, assisting victims, and educating the population on the principles of digital citizenship. The Pakistani government should only focus on all three aspects (technical, legal, and socio-cultural) to achieve a robust digital ecosystem that can resist the cyber threats in the 21 st century. The price of doing nothing - in terms of monetary loss, deferred trust in digital systems and human misery - is entirely too high to overlook.

Case Studies

Pakistan has experienced various high-level cybercrime cases that signify the increasing maturity of online crimes, and the drastic impacts of the same. A recent case is the 2023 Bank of Punjab data breach in which hackers accessed customer databases and stole sensitive financial data of more than 500,000 account users (State Bank of Pakistan, 2024). This involved exploitation of the third party payment systems that the bank used; the attackers used it to drain PKR 2.3 billion in the unauthorized transactions before the breach was identified. This event revealed severe flaws in the financial cybersecurity system of Pakistan and caused mass panic among consumers, resulting in a 15 percent decrease in the digital banking operations in the next quarter (Pakistan Banking Association, 2024). The case highlighted the necessity of more intensive regulatory control and the necessity of the obligatory cybersecurity audit within the financial institutions.

The other shocking incident showed blackmailing rings in the social media running in big cities that became evident after a FIA crackdown in 2023. Criminal groups were identified to lure victims, especially women, into compromising positions through false social media accounts, and blackmail them with money in exchange of threats to publish their personal materials (Digital Rights Foundation, 2024). An especially bad one in Lahore had more than 1,200 victims before it was taken apart, and investigators found that the bad guys had been using VPNs and paying in cryptocurrencies to avoid getting noticed (FIA Cyber Crime Wing, 2024). The uproar against these disclosures compelled social media providers to work more closely with Pakistani government and this led to the creation of a specific cyber harassment reporting portal under PECA. Nevertheless, the case also unveiled serious problems in society as most victims were victims of their communities as opposed to victims in need of support (Aurat Foundation, 2023).

The cases warn of important lessons in cybersecurity policy and awareness. The episode with banking fraud showed that excessive reliance on the outdated systems and insufficient training of employees regarding cybersecurity might result in disastrous outcomes, which is why the State Bank has made the use of biometric verification in all online transactions mandatory as of 2024 (State Bank of Pakistan, 2024). The social media blackmail incidents demonstrated the effectiveness of a well-coordinated effort by law enforcement agencies, as well as the necessity

of digital literacy education, especially among the vulnerable populations. The people have reacted inconsistently to these events - as the calls to provide better cyber security are increasing, a 2024 Gallup Pakistan poll indicated that two out of three citizens do not have confidence that the government could stop these crimes. All these examples underline the necessity of upgrading technology, changing the laws, and the attitudes of the society to make the digital world safer.

Recommendations for Strengthening Cybersecurity in Pakistan

The increasing threats to cyber security in Pakistan require collective, multi-stakeholder efforts to establish a robust digital environment. To the government, the ability to enforce the law should be the first priority. National Cyber Security Policy 2023 has set lofty targets yet, it will need a lot of funding at the moment, Pakistan is investing less than 0.1 percent of its IT budget in cybersecurity (Ministry of IT, 2024). Response time could be improved greatly by setting up special cybercrime investigation teams in each district with up to date forensic equipment. The Cyber Crime Wing of the FIA should triple the number of personnel with the training (there are 500 now, and it should increase to 1500) and create 24/7 monitoring centers, similarly to the Cyber Security Agency of Singapore (FIA, 2024). Also important is the concept of public-private partnerships that the government ought to enforce, where the financial institutions and telecoms share information on threats in real-time to a central repository to be maintained by the Pakistan Cybersecurity Council. The effectiveness of collaboration models such as the one practiced by MyCERT in Malaysia has cut down the time it takes to respond to attacks by 40% (PCC, 2024). Such collaborations can be speeded up by tax breaks on private companies investing in a cybersecurity infrastructure.

Basic cyber hygiene is the last defense in the business and personal setting. By 2025, the State Bank ought to require all financial institutions to adopt ISO 27001 standards, and the implementation should be audited at least four times a year (SBP, 2024). The 85 percent of enterprises in Pakistan are small businesses (SMEDA, 2024) that need to be provided with access to cybersecurity solutions at subsidized prices, which would be best achieved as a voucher program that gives out 50,000 free licenses to endpoint protection each year, effectively cutting down vulnerabilities by a dramatic margin. On a personal level, it is recommended that the PTA liaise with telecom companies to issue monthly cyber security awareness SMS to all cell phone users with an emphasis on phishing detection and password maintenance. Victims require efficient reporting processes a suggested unified cybercrime portal with chatbot services and case monitoring may raise the reporting levels to 40 percent in two years (DRF, 2024) up to the current 12 percent. Cyber harassment victims should be provided with trauma counseling services through the integration with the already existing helplines such as 1234 by PEMRA, and it would take care of the psychological aspect that is not covered by technical solutions.

The role of law reforms should be able to keep up with the technological changes. The Prevention of Electronic Crimes Act (PECA) 2016 needs to be amended urgently to cover AI-generated deepfakes, the risk of cryptojacking, and IoT-based attacks, all of which were not in existence when the law was written. An Amendment Bill to the PECA 2024 ought to bring in the tougher data localization provisions that will force social media firms to keep user data of Pakistani customers within the country just like PDP Bill in India (PIDE, 2024). The court system must be equipped with technologically trained judge pilot programs in Karachi, Lahore, and Islamabad could solve cases within 6 months as opposed to an average of 2 years (Law & Justice Commission, 2024). The implementation of evidence preservation via blockchain would eliminate the possibility of

manipulating digital evidence, whereas standardized sentencing instructions would eliminate the existing discrepancies, according to which similar crimes are punished by vastly different penalties. They are also important in implementation roadmap and monitoring mechanisms. A National Cybersecurity Implementation Committee comprising of military, civil, and private representations should be formed to monitor the progress that will publish bi-annual public scorecards (Cabinet Division, 2024). By 2025, the Higher Education Commission should institute compulsory cybersecurity training in all undergraduate degree programs, which will produce a pool of competent graduates. Knowledge transfer would be achieved with the help of international cooperation via the Cybercrime Directorate of Interpol and the cybersecurity program of ASEAN. Although these steps are expensive to undertake, the promised savings of up to 2.8 billion dollars (1.2 percentage of GDP) per year due to averting cybercrimes (PBC, 2024) make the investment worthwhile. Finally, the future of Pakistan in the digital world lies in ensuring that cybersecurity is not seen as an IT problem, but rather a national security concern that requires the whole of society approach.

Conclusion

The state of cybercrime in Pakistan has become a sophisticated and multidimensional issue that endangers economic stability, social harmony, and national security of the country. The increased level of financial fraud, data breach, cyber bullying and new forms of threats, such as ransomware and deepfake technologies, proves that there is an urgent need to take a comprehensive approach to countering them. Although the country has advanced with laws such as PECA 2016 and creating cybercrime departments, there are still major loopholes in enforcement, awareness, and infrastructure on technology. The case studies of the most high-profile cyber incidents show how sophisticated cyber threats are, as well as the outcomes of a lack of preparation, which is a sharp reminder that the reactive approaches are not effective anymore in a more digital world.

The response to the cybersecurity crisis in Pakistan needs to be integrated and multi-faceted, as well as involving all stakeholders. The government needs to focus on capacity building of law enforcement, invest in modern systems of cyber defense and develop closer international partnerships to fight cross-border cybercrime. At the same time, companies must implement strong security measures, and citizens must have more access to digital literacy courses that allow them to identify and report malicious activities on the Internet. The legal strategies have to change with the times and are required to be in line with the technological changes so that the law such as PECA may be able to deal effectively with the current issues like AI-powered crimes, and cryptocurrency-based frauds. Such systemic changes should be complemented by the de-stigmatization of cybercrime reporting, especially among highly vulnerable populations, who tend to experience the problem silently because of societal stigma.

The future of Pakistan is critical and with a proactive approach to cybersecurity infrastructure development and education, huge returns can be achieved in the long run. By displaying cybersecurity as a national issue, not only a technical problem, Pakistan will not only be able to reduce the existing threat, but also become a safer and more desirable digital innovation and investment destination. The way ahead needs a long-term dedication, proper resource investment, and, above all, a shared understanding that in the age of globalization, cyber resilience is not a choice it is a part of nation development. That is why it is time to act, so that the increasing number and complexity of cyber threats do not become more than the country can handle.

References

Aurat Foundation. (2023). *The Social Impact of Cyber Blackmail in Pakistan*. Islamabad: Aurat Foundation.

Aurat Foundation. (2024). *Cyber Harassment and Gender-Based Violence in Pakistan*. Islamabad: Aurat Foundation.

Cabinet Division. (2024). *Framework for National Cybersecurity Governance*. Islamabad: Government of Pakistan.

Digital Rights Foundation (DRF). (2023). *Digital Literacy and Online Safety in Pakistan*. Lahore: DRF.

Digital Rights Foundation (DRF). (2023). *Online Harassment and Gender-Based Violence in Pakistan*. Lahore: DRF.

Digital Rights Foundation (DRF). (2024). *Improving Cybercrime Reporting Mechanisms*. Lahore: DRF.

Digital Rights Foundation (DRF). (2024). *Social Media-Facilitated Blackmail: Trends and Countermeasures*. Lahore: DRF.

Federal Investigation Agency (FIA). (2024). *Annual Cybercrime Trends Report 2023-24*. Islamabad: FIA Cyber Crime Wing.

Federal Investigation Agency (FIA). (2024). *Capacity Building Requirements for Cybercrime Units*. Islamabad: FIA.

Federal Investigation Agency (FIA). (2024). *Cybercrime Conviction Rates and Challenges*. Islamabad: FIA Cyber Crime Wing.

Federal Investigation Agency (FIA). (2024). *Operation Against Social Media Blackmail Networks*. Islamabad: FIA Cyber Crime Wing.

Gallup Pakistan. (2023). *Public Awareness of Cyber Laws in Pakistan*. Islamabad: Gallup.

Gallup Pakistan. (2024). *Public Trust in Cybersecurity Measures Survey*. Islamabad: Gallup.

Interpol. (2023). *Global Cybercrime Report 2023*. Lyon: Interpol.

Kaspersky Lab. (2023). *Cybersecurity Threats in South Asia*. Moscow: Kaspersky.

Law & Justice Commission. (2024). *Reforming Cybercrime Adjudication*. Islamabad: LJCP.

Media Matters for Democracy (MMfD). (2024). *Misinformation and Social Unrest in Pakistan*. Islamabad: MMfD.

Ministry of IT. (2024). *National Cybersecurity Budget Analysis*. Islamabad: MoITT.

National Response Centre for Cyber Crimes (NR3C). (2024). *Ransomware Threat Assessment Report*. Islamabad: NR3C.

Pakistan Banking Association (PBA). (2024). *Impact of Cybersecurity Breaches on Digital Banking*. Karachi: PBA.

Pakistan Business Council (PBC). (2024). *Economic Impact of Cybercrime in Pakistan*. Karachi: PBC.

Pakistan Cybersecurity Council (PCC). (2023). *Phishing and Identity Theft in Pakistan*. Karachi: PCC.

Pakistan Cybersecurity Council (PCC). (2024). *Public-Private Partnership Models for Cybersecurity*. Karachi: PCC.

Pakistan Cybersecurity Council (PCC). (2024). *State of Cybersecurity in Pakistani Businesses*. Karachi: PCC.

Pakistan Electronic Media Regulatory Authority (PEMRA). (2024). *Cyberterrorism and National Security Threats*. Islamabad: PEMRA.

Pakistan Institute of Development Economics (PIDE). (2023). *Cross-Border Cybercrime and Jurisdictional Challenges*. Islamabad: PIDE.

Pakistan Institute of Development Economics (PIDE). (2024). *Comparative Analysis of Cyber Laws in Asia*. Islamabad: PIDE.
Pakistan Institute of Development Economics (PIDE). (2024). *The Impact of Deepfake Technology on Society*. Islamabad: PIDE.
Pakistan Telecommunication Authority (PTA). (2024). *Internet Usage Statistics 2024*. Islamabad: PTA.
Small and Medium Enterprises Development Authority (SMEDA). (2024). *Cybersecurity Needs Assessment for SMEs*. Lahore: SMEDA.
State Bank of Pakistan (SBP). (2024). *Digital Fraud and Financial Cybersecurity Report*. Karachi: SBP.
State Bank of Pakistan (SBP). (2024). *Financial Sector Cybersecurity Standards*. Karachi: SBP.
State Bank of Pakistan (SBP). (2024). *New Biometric Verification Protocols for Digital Transactions*. Karachi: SBP.
World Economic Forum (WEF). (2023). *Global Cybersecurity Outlook 2023*. Geneva: WEF