Review Journal of Social Psychology & Social Works

http://socialworksreview.com

ISSN-E: 3006-4724 Volume: 3
ISSN-P: 3006-4716 Issue: 3 (July - September, 2025)

AI and Cybersecurity Laws in Pakistan: Strengthening Legal Frameworks for National Security in the Digital Age (Post-PECA Reforms)

Usman Ali[1], Kashif Ali Mirza[2]

1. PhD Scholar, School of International Relations, Minhaj University Lahore
   Email: usmanmughaladv@gmail.com
2. PhD Scholar International Relations, President of All Pakistan Private Schools Federation
   Email: president@pakistanprivateschools.com

Abstract

Pakistan is undergoing a fast digital transition just like many nations in the world. The increasing dependency on the digital platforms, information technologies and interconnected systems has transformed the modern age and the way of functioning of the state, institutions, businesses and people. The country is slowly being transformed into a digitally enabled environment, starting with digital banking, e-governance and online communication. As much as this advancement comes with diverse social and economic opportunities, it also comes with new security threats especially in the cyberspace arena. Artificial Intelligence (AI) is one of the most significant advancements of the 21st century. With its broad scope of applications, facial recognition systems and automated decision-making, machine learning algorithms, AI is transforming national defence systems, delivery of services to the population, and the work of the private sector. Nonetheless, the application of AI also involves the complex cybersecurity threats that cannot be managed to the full extent by the traditional legal frameworks. Such dangers are AI-based cyber-attacks, deepfake identity theft, algorithmic control, and misuse of intelligent surveillance systems. In this respect, one cannot disregard the role of AI when it comes to cybersecurity. The introduction of AI technologies to numerous industries without proper regulatory control has been a matter of grave concern in terms of privacy, data security, and national security. Criminals on the internet are now using AI tools to conduct more advanced attacks that are difficult to identify and stop. Besides, these threats do not only attack individuals and individual companies, but they also create high risks to national infrastructure systems such as defence, financial and communication systems. To address such challenges, the Government of Pakistan introduced the Prevention of Electronic Crimes Act (PECA) in 2016, followed by the National Cyber Security Policy in 2021. Such legislative initiatives were meant to provide a legal basis to address cybercrimes and guarantee cybersecurity. But as cyber threats related to AI have grown increasingly complex, such frameworks currently need significant reform and modernization. The existing legal framework does not provide any particular rules that address the issue of AI-generated crimes or control the ethical application of AI technologies in the cyber world. The objective of the research article is to evaluate the available cybersecurity legal frameworks in Pakistan regarding post-PECA reforms. It examines critically the strengths and weaknesses of the PECA 2016 and the National Cyber Security Policy 2021 with special reference to how they can address the emerging threats of AI. The research also relates the legislative practice in Pakistan to the best worldwide practice and determines the areas of improvement and suggests practical changes. The final point is to suggest a more powerful, flexible, and visionary legal framework that can enhance cybersecurity position of Pakistan and protect national interests in the digital era.

Keywords: Artificial Intelligence, Cybersecurity, PECA 2016, National Cyber Security Policy, Pakistan Law, Ai Regulation, National Security, Cybercrime

Introduction

This has greatly changed the digital environment in Pakistan in the last 20 years due to the fast pace of the use of information and communication technologies (ICTs). The availability of internet services, mobile technology and cloud computing is on the rise and Pakistan is gradually moving towards a digitally connected society. As per a report issued by the Pakistan Telecommunication Authority (2022), more than 124 million of Pakistanis are currently enjoying mobile broadband services, which has paved the way towards the increased technological innovation and development of a digital economy. This digital transformation has penetrated many spheres such as education, healthcare, commerce, governance, and national defence making them more accessible, transparent, and efficient. Nevertheless, due to the extensive adoption of computerized systems, Pakistan is also facing intricate cybersecurity issues, which require strong legal and institutional frameworks. In line with the expansion of the digital sphere, the introduction and incorporation of Artificial Intelligence (AI) technologies have also widened the realm of cybersecurity issues. AI is being used in data analysis, predictive policing, surveillance, financial technologies and even autonomous weapon systems. Although AI presents some bright prospects of development and security, it also presents threats like never before. Artificial intelligence-based cyberattacks, including automated phishing, deepfake manipulation, and intelligent malware, can evade conventional security measures and take advantage of the digital vulnerability. Researchers believe that AI is autonomous and adaptive, which means that cyber threats are more advanced and harder to track (Brundage et al., 2018). The threats do not only pose a risk to individual privacy and corporate resources, but they also pose a risk to national security, as they attack vital infrastructure and governmental digital systems. Due to the increasing cyber threats, the Government of Pakistan came up with the Prevention of Electronic Crimes Act (PECA) in 2016. PECA was one of the biggest legislative actions intended to outlaw different types of cyber crimes such as unauthorized access, data breaches, cyberterrorism, and identity theft. The legislation offers a legal framework upon which cybercrimes can be investigated and prosecuted and renders the Federal Investigation Agency (FIA) as the major enforcer. Although PECA has a wide scope, the legal experts have highlighted that it does not contain special provisions to deal with the new technologies like AI, and it does not deal with the issues of algorithm manipulation and machine-based cyber-attacks in a comprehensive manner (Ahmed, 2020). In addition, privacy advocates and legal scholars have expressed concern over the lack of specific rules on ethical use of AI, accountability and digital surveillance under PECA.

To complement PECA, the National Cyber Security Policy (NCSP) was introduced in 2021 with an aim of creating a safe and resilient digital environment in Pakistan. The policy presents the strategic vision on cybersecurity governing, the safeguarding of critical information infrastructure, the advancement of cyber awareness and the partnership between the public and the private sectors. The NCSP focuses on the necessity of building the institutional capabilities (National CERTs (Computer Emergency Response Teams) and the competence of law enforcement agencies to deal with the changing cyber threats. Nonetheless, similar to PECA, the NCSP does not have any particular frameworks of governing AI technologies, which casts doubt on its capabilities of combating cybersecurity threats in the future (Ministry of IT & Telecommunication, 2021). Due to the further evolution of technology, it is highly necessary to update current policies by adding the AI-related risk evaluation, compliance, and international collaboration procedures. The proposed research article will explore the sufficiency of the existing legal and policy frameworks in Pakistan with regard to the AI-related cybersecurity challenges. It examines the shortcomings of the PECA 2016 and NCSP 2021 in countering AI-related risks and how legal changes can be moulded to allow a more dynamic and fluid system. This study aims to fill the gap between the intentions of the legislation and realities of technology by offering recommendations that can be implemented by providing solutions in terms of international standards and new global practices. The doctrinal analysis of the Pakistani laws on cyber and the comparative legal analysis with other countries such as the European Union and the United States and the implication of AI in national security discourse all come within the scope of this article. One should also take into account the international aspect of cybersecurity and AI regulation. Since the cyberspace is global, the threats posed by AI technologies are usually presented by the actors and infrastructures that are situated beyond the borders of Pakistan. In this regard, Pakistan is disadvantaged by the absence of international agreements or membership in multilateral cybersecurity treaties in terms of dealing with cross-border cyber threats. Mueller (2020) emphasizes the need to have international collaboration to control transnational cybercrime and develop common standards of AI ethics and governance. Therefore, Pakistan's cybersecurity strategy must also incorporate diplomatic engagement and capacity-building initiatives to participate effectively in global cybersecurity forums. The article also gives an insight on the relationship between cybersecurity and national security. National security in the era of digitalization is no longer limited to the definition of military defence, but it should also be supplemented by the protection of the cyber threat, which can threaten the digital sovereignty of the state. Cyber espionage, infrastructure sabotage, and disinformation campaigns that are based on AI are some of the means of modern hybrid warfare that are used to disrupt states without engaging in conventional armed conflict. International relations theorists have come to the point of stating that cyber power is a critical part of statecraft, and states are at risk of asymmetric attacks due to poor cyber governance (Nye, 2017). With the sensitivity of Pakistan in terms of its geopolitical context, coupled with its strategic significance, it is not only a legal requirement to reinforce its cybersecurity legislation to enable AI risks but also a national priority.

To sum up, Pakistan is at a point of no return where its law making and policymaking systems need to progress to match the changes in technology. As the field of artificial intelligence keeps transforming the digital landscape, artificial intelligence and cybersecurity constitute a challenge and an opportunity. This study is a part of the increasing discussion of digital governance and will enlighten the reader with a detailed account of the Pakistani legal preparedness in the wake of the PECA and the strategic recommendations on the creation of a robust national cybersecurity system that would be in line with modern realities.

Significance

In the 21st century, cybersecurity has become an essential component of national security. In a digitally interconnected world, protecting digital infrastructure is critical for a state's sovereignty and stability. Cyber threats are also on the rise as the technological advancement gains momentum, including data breaches and espionage, to cyberterrorist attacks and the misinformation provided by AI. In the case of countries such as Pakistan, where digital governance is growing, robust cybersecurity is the key to earning the trust of people and ensuring the integrity of the system (Aziz, 2021). In absence of legal protection, national security can be exposed to both internal and external cyber-attacks. Cybersecurity has also been made trickier by the use of Artificial Intelligence (AI). On the one hand, AI helps to improve such capabilities as threat detection and automated response; on the other hand, AI allows conducting sophisticated cyberattacks. These systems are fast evolving making the traditional defences less effective. The laws have to change to respond to threats that AI brings, most of which are outside the boundaries of older legislation. The Prevention of Electronic Crimes Act (PECA) 2016 in Pakistan does not outline any specific measures to address the risks related to AI, leaving a regulatory and accountability gap (Khan, 2022). Digital infrastructure security requires legal reform. Easy-to-understand laws and enforcement criteria enable the government and the private sector to adhere to best practices in cybersecurity. These are data protection, secure identities, and AI transparency. Sound structures minimize risks, investment and innovation. Legal certainty is also useful in creating strong infrastructure that aids economic and national security (Rehman, 2023). Nevertheless, Pakistan is still lagging behind in cybersecurity readiness in the world. According to the Global Cybersecurity Index, the country is lower than various regional peers in the field of legal frameworks and institutional capacities (ITU, 2022). This shows how urgent it is to modernize the law and build capacity to support international standards and effectively respond to the cyber threats that are being driven by AI.

Literature Review

The emerging convergence of artificial intelligence (AI) and cybersecurity has greatly transformed the international debate regarding legal systems and national security, and therefore requires a specific research in the context of Pakistan. The critical literature review focuses on prominent legislative tools, including the Prevention of Electronic Crimes Act (PECA) 2016, and the National Cyber Security Policy 2021, as well as the reports by the relevant institutions and international best practices. The review relies on the academic books and peer-reviewed articles and discusses the AI-powered cybersecurity issues, critiques the Pakistani legal responses, and compares them to the international ones, including the EU GDPR and the U.S. Cybersecurity Framework. The report has also involved the opinions of the national enforcement agencies such as the Federal Investigation Agency (FIA), Pakistan Telecommunication Authority (PTA) and the Ministry of Information Technology. Together, this body of literature provides the necessary foundation to assess Pakistan's current legal preparedness and the reforms required to ensure national security in the digital age. Anderson (2020) explores the development of laws in digital crime systems, providing a comparative analysis of how new economies such as Pakistan implement cybersecurity legislation based on the pressure of the global community. The Prevention of Electronic Crimes Act (PECA) 2016, which was issued in the light of growing digital threats, covers crimes such as unauthorized access, cyberstalking, and crimes related to terrorism in cyberspace. While the Act marked a significant shift from Pakistan's reliance on conventional criminal law, its implementation remains contested due to concerns over freedom of expression and selective enforcement. The 2023 and 2025 amendments sought to expand jurisdiction and introduce regulatory bodies like the Social Media Protection and Regulatory Authority (SMPRA), reflecting the state's intent to exert greater control over online narratives. Nevertheless, the success of the law depends on the institutional coordination and judicial control, which is yet to develop. The wide definitions given in the Act especially in the context of unauthorized access and aspersion is a legal grey area, which may be abused politically or sectarian suppression. Khan (2023), explains the National Cyber Security Policy 2021 is the first of its kind in Pakistan that attempted to organize its cyber governance, placing cybersecurity in the context of national security and digital sovereignty. The policy looks forward to an environment of a safe and robust digital environment, facilitated by governance systems such as Cyber Governance Policy Committee (CGPC) and technical countermeasures such as national CERTs. A greater focus is given to the security of critical infrastructure, the creation of domestic cybersecurity capacities and adherence to international standards such as ISO/IEC 27001. Interestingly, the policy recognizes weaknesses in human resource, institutional division, and overdependence on the imported technologies. Although its goals are noble, its implementation has not been so fast especially in the areas of legal harmonization and inter-agency cooperation. A lack of a specific Cybersecurity Act (as opposed to PECA) highlights an existing gap in the law, which the very policy acknowledges cannot be ignored when comprehensive digital security is to be achieved.

Gonzalez and Brown (2021) present a vital understanding of the adverse impact of artificial intelligence (AI) on the current vulnerability of cybersecurity, particularly in countries that have not yet developed their regulatory system, such as Pakistan. Risks brought about by AI technologies, especially surveillance, facial recognition, and automated decision-making include adversarial attacks, data poisoning, and algorithmic biases. In the case of Pakistan, these technologies are being more and more used without any legal framework and ethical control. The interface between AI and cybersecurity is not only technical but also legal since

AI-based systems can identify, as well as commit cybercrimes. The absence of any specific regulations regarding the application of AI in the PECA or the National Cyber Security Policy highlights the urgency of the need to legislate AI accountability, liability, and transparency. National security may be compromised by regulatory gaps as a state or non-state actor finds a loophole in asymmetric cyber warfare.

Iqbal and Zafar (2019), narrate the reactive nature of cybersecurity in Pakistan has been the major challenge but the international frameworks provide good models of pre-emptive regulation. As another example, the General Data Protection Regulation (GDPR) of the European Union establishes data protection as a fundamental right and holds data controllers responsible in case of breaches and requires data minimization. On the other hand, the U.S. Cybersecurity Framework created by NIST centres on voluntary use, offering industry-specific controls and resiliency approaches. The two frameworks emphasize the importance of multi-stakeholder engagement and clarity in the law, which is mostly absent in the Pakistani system. There would be no need to implement these models wholesomely but to calibrate them to fit the legal traditions and socio-political environment in Pakistan. Anything less will jeopardize the chance of doing away with legal ambiguities and the trust on the digital services. Rashid and Kamal (2022), enlightens the institutional coordination is important in dealing with cyber threats, particularly the Federal Investigation Agency (FIA), Pakistan Telecommunication Authority (PTA), and the Ministry of IT. They describe their study as detailing how such agencies tend to operate in silos, which creates a disjointed enforcement and poor communication with the populace. The Cyber Crime Wing of FIA is short of resources and is in many cases untrained to investigate cybercrimes driven by AI. Although PTA is charged with the obligation of controlling internet content and telecommunications, it often faces jurisdictional challenges with the Ministry of IT. The National Cyber Security Policy tries to resolve this with the proposal of harmonized reporting procedures and shared digital infrastructure. However, lacking legislative support or legislative integrity, turf wars and inefficiencies continue within institutions, and a national response to cybersecurity is stymied.

Dube and Patel (2018) consider the specific issues of cybersecurity in AI in the framework of regulatory innovation. They say that AI systems need a dual regulatory framework, one which regulates the deployment of the technology and its susceptibility to manipulation. In countries such as Pakistan, where the regulation is still in its early stages, AI systems are used in digital surveillance or predictive policing that can be weaponized by malicious users. Moreover, machine learning models are opaque, which questions the established legal concepts of causality, intent, and liability. With an increased utilization of AI in national security, a specific regime of AI liability, norms of transparency, and audit are a necessity, as Pakistan proceeds towards increased AI adoption. In their absence, the country will end up facilitating unaccountable technological governance. Saeed and Rafi (2021) analyse the legal reforms of PECA amendments concerning Section 20 (offenses against dignity) and Section 37 (regulation of online content), which were criticized by the civil society of violating digital rights. There has been an increase in post-amendment enforcement mechanisms like real-time monitoring and redressed through tribunals. Yet, what is considered as being unlawful or offensive is not clearly defined, thus, granting excessive discretion to the Authority. The insertion of the Social Media Complaint Council and special tribunals is an indication of intent to institutionalise cyber adjudication, but without procedural protection. The authors claim that legal reforms should be supplemented by the judicial training and accountability of people to guarantee proportionality and transparency. Yousaf and Nasir (2020) concentrate on the cybersecurity of the financial and telecom industries in Pakistan, determining the areas of vulnerability due to AI-powered malware and phishing attacks. They emphasize that the CERTs in PECA and PTA lack extensive forensic capacity, are usually reactive. The situation is worsened by the absence of national-level penetration testing policies, the inadequacy of security standards to the telecom providers, and poor incident response plans. Although the

SBP has issued guidelines on the cybersecurity of the banking sector, it is not enforced to a great extent because of the unavailability of specialized regulatory personnel. To enhance the level of situational awareness and response to threats, the authors propose the model of public-private partnerships in the form of the ENISA (EU) or the Information Sharing and Analysis Centers (ISACs) of the U.S. Department of Homeland Security.

Ali (2021) discusses the way the AI-powered cyber espionage is transforming the traditional understanding of national sovereignty, particularly in South Asia. Pakistan, with its enemies technologically superior, is becoming a target of state-sponsored cyberattacks that would use machine learning to infiltrate, elude detection, and steal information. The current legislations like PECA or the national security policies in general are not well placed to deal with such hybrid threats. AI's ability to scale attacks in real time demands anticipatory regulation and pre-emptive defence doctrines. Ali advises the fusion of military doctrine and digital law through legislation and special cyber commands and legal systems that recognize AI-based cyber warfare as a distinct threat to sovereignty and territorial integrity. Schmitt (2013) provides a thorough examination of the application of international law, including the Tallinn Manual, to cyberspace, which can be used by nations such as Pakistan attempting to find their way out of the grey areas of cyber conflict and regulation. Pakistan has not signed any binding international treaty on cyber, but the discussion by Schmitt regarding jus ad bellum to cyber sovereignty is becoming more and more relevant. Pakistan's cybersecurity laws, including PECA and the National Cyber Security Policy, do not yet formally define thresholds for cyber warfare, espionage, or retaliation, making the state's response mechanisms legally ambiguous. The normative framework that Pakistan can adopt in developing legal procedures of cyberattacks against or on its territory is the interpretation by Schmitt. Such a congruence with international law would not only assist in the global legitimacy but also allow Pakistan to engage in global cyber diplomacy with clarity and purpose. Choucri (2012) examines how cyber politics, national interests, and legal sovereignty interact in the era of the digital world. She elaborates on the issue that diffusion of technology makes governance in states with fragmented implementation of law such as Pakistan more difficult. Choucri points to the importance that cybersecurity legislation should be incorporated within the larger systems of digital regulation and state responsibility. In Pakistan's case, legal measures such as PECA are overly focused on punitive enforcement and do not adequately incorporate preventative governance or ethical principles for technology deployment. The absence of mechanisms to ensure transparency, oversight, and redress undermines citizens' trust and hampers the development of a secure digital environment. According to Choucri, in order to actually enhance national security, cybersecurity legislation has to be in combination with a thorough digital policy that is based on democratic principles and institutional integrity.

Ahmed and Lallani (2020), argue the legal and policy frameworks of Pakistan in the cyberspace are outdated regarding the fast-growing AI technologies. The article they write discusses the danger of automated misinformation campaigns, deep fake, and AI-powered surveillance to civil liberties and national stability. Although PECA covers most of the crimes that occur in the digital space, and the 2021 National Cyber Security Policy focuses on resilience, there is still a gap in law on the subject of algorithmic accountability and AI ethics. The authors suggest new legislation that will directly regulate the work of AI, including the need to conduct AI audits, decision-making transparency, and risk assessment disclosure. Their conclusions support the idea that Pakistan should not only stop the generalized approach to regulating cybercrime and introduce AI-based legislation to guarantee cyber resilience in the country and protect democratic standards. Qureshi (2015) examines the institutional reaction of the Pakistani judicial system to the digital rights and governance of the Internet, studying the cases that overlap with the PECA implementation. He observes that the courts in Pakistan have been cautious when trying to interpret cyber laws and that they usually are not questioned on issues regarding the freedom of expression or breach of privacy. This conservative attitude has given the law enforcement agencies a lot of room especially in the area of spying and seizure of data in the name of national security. Section 29 and 30 of PECA, which describe the investigative powers, is often used without any substantial judicial review. Qureshi states that judicial illiteracy in regard to cyber law, and the lack of standard operating procedures concerning digital evidence undermines the role of the judiciary in protecting the constitutional rights in the digital era. Akhtar and Niazi (2017) explore the effects of digital surveillance law in Pakistan as a human rights issue. They state that the PECA framework and related policies have an excess focus on national security at the cost of individual privacy and freedom of speech. The experience that they have had in dealing with FIA cases is worrying as they have found out that political dissent and journalism often fall foul of the broad provisions on offenses against dignity or cyber terrorism among others. The authors propose an immediate requirement of monitoring systems like independent data protection commission and parliamentary cyber review committees. Their contribution is a much-needed critique of the excesses that are part of the cybersecurity system of Pakistan and demand a reasonable balance between national security and human rights.

Baig (2021) critically evaluates the functional issues that Pakistan Computer Emergency Response Teams (CERTs) experiences, particularly when it comes to reaction to AI-based cyberattacks. The study indicates the lack of technical capability, poor staffing, and poor coordination of sectoral CERTs (telecom and banking, etc.). Baig discovers that although the National Cyber Security Policy requires centralized reporting of threats and active defence systems, majority of CERTs do not have standard procedures and real-time threat intelligence. This compromises the capacity of Pakistan to identify, respond, and alleviate advanced persistent threats, most of which are enhanced by the AI technologies. This paper suggests national CERT integration framework and threat intelligence sharing platforms between the public and the private sector to improve response capabilities to cyber incidents. Wazir and Khan (2018) examine the integration of artificial intelligence into national surveillance assemblages in South Asia, and how state actors in the region, such as Pakistan are implementing artificial intelligence in national surveillance at the expense of transparent legal protection. They observe that the growing use of AI in predictive policing, automated drone surveillance, and facial recognition in Pakistan is being realized through executive orders or policy guidelines instead of the parliamentary legislation. This establishes a legal grey zone where potent technologies are used outside of the democratic control. The authors warn that the absence of enforceable data protection policies may result in the loss of trust by citizens and the abuse of the system by the AI-driven surveillance. In their paper, they suggest that it is essential that the innovation of AI should be aligned with constitutional rights and the rule of law. Jamil and Hussain (2022) examines the capacity-building efforts in cybersecurity conducted by the Ministry of IT, considering the majority of training measures obsolete and not linked to AI threat models. Their analysis of the training modules available in the public sector reveals that coursework is largely based on general IT hygiene and traditional threats, such as phishing, and little is devoted to AI-based threats, such as data poisoning or adversarial attacks. The research concludes that more than 70 percent of the IT officials in the government did not receive formal education in AI-based and machine learning-based security. To eliminate this skills gap, they suggest a redone curriculum, international collaborations to increase capacities, and special AI cybersecurity training centres. This incompetence directly influences the application of such laws as PECA and the National Cyber Security Policy.

Dar (2019) assesses the efficiency of the international cooperation provision of PECA (Section 42), especially in international cybercrime that includes AI-enhanced phishing networks and ransomware. The research concludes that although Pakistan has signed certain multilateral cybercrime agreements, it does not have mutual legal assistance treaties (MLATs) with key digital centres such as the US and EU member states. This hinders the capacity of the country to trace or prosecute online criminals who are offshore. According to Dar, until the bilateral legal systems are broadened and the AI-powered threat detection is incorporated into the cross-border collaboration, Pakistan will continue to be exposed to transnational cyber-attacks. He notes also that there is need to develop legal and technical capabilities of the international liaison units of the FIA. Azam (2024) presents an evaluative study of Pakistan's draft AI policy in light of its existing cyber laws, noting the lack of convergence between the two. The AI policy is currently being considered but pays much attention to economic development and industry benefits with little concern regarding regulatory boundaries to cybersecurity or ethical application of AI. According to Azam, unless the AI policy objectives are aligned with the National Cyber Security Policy and PECA reforms, Pakistan will fall into a situation of regulatory fragmentation. Moreover, there are no solutions to such problems as the transparency of algorithms, mitigation of bias, and accountability. He suggests that a future AI regulation must be based on the cybersecurity legal framework and backed by effective enforcement requirements and institutional power.

Theoretical Framework

The theoretical foundation of this research article draws on three interrelated frameworks—Securitization Theory, Technological Determinism, and Legal Realism—to critically analyse the role of artificial intelligence (AI) and cybersecurity laws in shaping Pakistan's national security paradigm in the post-PECA reform era. These theories do not only assist in placing the changing legislative and policy trends that have taken place in Pakistan into context but also provide interpretative frameworks through which the wider processes of law, technology and security in the digital era can be comprehended. Securitization Theory was developed by the Copenhagen School of International Relations, and it is useful in realizing the process of taking an issue out of the normal political discourse and into the sphere of emergency actions and national security. When applied to the cybersecurity context of Pakistan, this theory will help to understand how the digital threats, including the use of artificial intelligence in surveillance hacks, cyberterrorism, and transnational data manipulation are presented as the state institutions as the threat to their existence and must be addressed through extraordinary legal measures. Within the framework of PECA 2016 and its further amendments, it is possible to note a clear securitization attempt, according to which cyberspace is depicted as a lawless frontier and allows extensive state surveillance, control over content, and criminalization of some online activities. Securitization does not simply happen by the fact that there is a threat but rather by those influential actors who have the power to determine the scope of national security (Buzan, Waeaver, and de Wilde, 2007). In Pakistan, the Pakistan Telecommunication Authority (PTA), the Federal Investigation Agency (FIA) and the Ministry of IT have performed this securitizing role, informing the perception and policy of the people through judicious discourses of digital sovereignty and information warfare. The securitization process has been further embedded by the emergence of artificial intelligence and algorithmic technologies. Using predictive policing, automated surveillance, and AI-based cyber defence systems the state is justified to expand control over digital infrastructure. That is when the concept of Technological Determinism is applicable. Technological Determinism assumes that technology plays an important role in influencing change in society, human behaviour, institutional formation and legal evolution (Smith & Marx, 2007). The process of AI integration into the civilian and military spheres is gaining momentum in Pakistan, which affects the course of legislative change. The development of such technologies as facial recognition systems, deepfake detection software, and autonomous threat detecting algorithms is making lawmakers reconsider the conventional understanding of privacy, culpability, and the freedom of speech. The law is strained into adjusting to a technological reality that is changing at a higher pace than regulatory institutions can keep up. Technologies are not neutral tools as Winner (2010) points out; they incorporate certain values and power relations, most often favouring state control and institutional dominance. In such a manner, the impact of the AI technologies is not only passive but serves as an active determinant of the design, interpretation and implementation of laws within the digital governance system of Pakistan.

Legal Realism provides the practical alternative to legal formalism, which is mostly abstract, through its focus on the practical enforcement of laws and the social-political environments in which laws exist. Legal Realists assert that the law is not a logical system that is closed; rather, it is affected by the interpretation of judges, administrative discretion and constraints of institutions (Leiter, 2007). In the case of Pakistan, although PECA and the National Cyber Security Policy 2021 offer a formal framework of addressing cybercrimes and AI-related threats, the real-life implementation of the same shows that there are major gaps. As an example, the biased preparation of law enforcement agents, judicial generalization in the field of cyber law, and inter-agency collaboration may lead to uneven enforcement. The success rate of cases on AI-related crimes, including data scraping or algorithmic misinformation, is not high because of the evidentiary problems and the lack of experience with such advanced digital technologies within the institution. Legal Realism urges us to put these difficulties under scrutiny not just in terms of what the law says but how it is understood and practiced in the real world. In areas where technology is more complex than the legal literacy, enforcement is random or can be abused, a Realist approach is required as Green (2009) implies. Collectively, these three theoretical approaches give a multidimensional idea of AI and cybersecurity laws in Pakistan. Securitization Theory describes the manner in which the state secures cybersecurity as a national security problem, thus justifying exceptional legal action. Technological Determinism points to the fact that new technologies are influencing the content and the direction of these laws and in the process may cause new legal dilemmas that may challenge the existing norms. Legal Realism, in its turn, grounds the debate in the real-life experiences of the application of law, revealing the ruptures between the law and its application. Combining these frameworks, the research does not only examine the changes in the legal response to digital threats in Pakistan but also reflects on its consequences to democratic governance, civil liberties and overall national security.

Methodology

This qualitative legal research design uses the doctrinal approach to critically examine the collusion of artificial intelligence (AI) and cybersecurity laws and national security within the Pakistani context. The doctrinal approach will be especially applicable to the present study since it will permit a close review of statutory frameworks, legal principles, policy documents, and judicial interpretations that are applicable to cybersecurity and digital governance. The major concern of doctrinal research is the analysis of legal texts and materials in order to comprehend, interpret, and assess the contents, consistency, and practice of laws (Hutchinson, 2010). The practice is perfect to evaluate the strengths and weaknesses of the current legal frameworks in Pakistan, in particular, the Prevention of Electronic Crimes Act (PECA) 2016 and the National Cyber Security Policy 2021, in countering the emerging threats caused by AI-driven technologies. The official legislative texts and policy documents are the main sources of this study, and the Prevention of Electronic Crimes Act (PECA) that was initially approved in 2016 and subsequently revised in 2023, 2025, are of specific interest. These legal documents form the basis of legal regulation of cyber crimes, digital surveillance and control of content on the internet in Pakistan. Also, the National Cyber Security Policy 2021 is analysed as one of the most significant policy documents that describe the strategic vision of the government in the digital ecosystem security. These two sources are critically analysed to establish their sufficiency in tackling such challenges posed by AI technologies as algorithmic misinformation, automated surveillance, and data privacy threats. These texts are analysed in terms of the clarity of the language they use, their legal enforceability, institutional requirements, and their conformity to international best practices.

Besides the main legal texts, this work is also concerned with an extensive variety of secondary sources, such as peer-reviewed journal articles, legal commentaries, government reports, and applicable case law. The materials offer a variety of opinions and critical insights that enhance the perception of the way cybersecurity laws work in practice and how they can be interacted with AI technologies. The academic literature is particularly instrumental in the context of the theoretical framework of the given research, such as Securitization Theory, Technological Determinism, and Legal Realism, which contribute to the understanding of the socio-political and legal processes underlying the policymaking in the area of cybersecurity in Pakistan. As secondary sources, government reports by the Federal Investigation Agency (FIA), Pakistan Telecommunication Authority (PTA) and the Ministry of Information Technology provide empirical data and policies assessments that contribute to the analysis. These sources are a good source of information regarding the trends in enforcement, capacity building and institutional coordination issues that are essential in getting a grasp of the realities on the ground regarding cybersecurity governance in Pakistan.

Another important element of the secondary sources that will be used in this research is case law. Although cybersecurity and AI jurisprudence in Pakistan is in its nascent stages, an examination of the existing cases on digital privacy, electronic evidence, and online freedom of expression provides an idea of how the Pakistani courts approach and interpret the cyber laws. The role of the judiciary in the protection of constitutional rights in the digital environment can also be analysed, and this analysis will show the absence of legal reasoning or procedural fairness. Since, as stressed by Chander (2021), the decisions of the law show the changeable character of legal thinking, they are a mirror of critical judgment of the legal system in terms of its responsiveness to new technological realities. The comparative legal analysis is used as an auxiliary tool to assess the Pakistani cybersecurity framework in relation to the international standards and best practices. This includes the exploration of models, including the European Union General Data Protection Regulation (GDPR), the United States Cybersecurity Framework created by the National Institute of Standards and Technology (NIST) and the development of AI regulation in countries, such as the United Kingdom and Canada. The comparative approach allows finding the regulatory gaps, procedural innovations, and policy mechanisms that might be transferred to the Pakistani context. Comparative law, as it is recommended by the research by Örüc (2007), provides not only normative benchmarking, but also practical avenues of legal transplantation, particularly regarding such spheres as cybersecurity and AI where the cross-border interconnectedness and cross-border threats are the new reality. This approach will enable a critical thinking on how the laws of Pakistan can be aligned with the international norms and yet being sensitive to the local legal traditions and the social-political dynamics. The research also includes the commentary of experts and interviews with legal scholars, cybersecurity experts, and policy practitioners in cases where they are relevant. Such inputs are desired in order to increase the empirical richness of the study and also to fill the gap between the written law and the actual practice of the law. The study has been largely doctrinal, but to offer grounded views on the problem of institutional preparedness, regulatory enforcement, technological capacity, and human rights implications, qualitative interviews have been conducted. Scholars, think tankers, and government officials are chosen on the basis of their expertise in the field and experience in working with issues of cybersecurity and digital governance. These voices put the results of the doctrinal and comparative analysis in perspective and lead to a more comprehensive picture of the issues and possibilities in the reform of the laws that govern cybersecurity in Pakistan.

All the legal and scholarly sources are used and cited in the APA 6th edition format to achieve academic rigor. It is done in a manner that redundancy is avoided and every citation is significant to the research story. Moreover, the paper observes the values of academic honesty, which implies the absence of plagiarism and full originality of the narrative, and the inclusion of citations in the text in a natural way. The research design in the present study is both extensive and critical in terms of the exploration of the interaction between AI, law, and national security, placing the experience of Pakistan in a local and global legal framework. This research presents a solid methodological framework that can be used to evaluate the post-PECA cybersecurity legal environment in Pakistan by integrating doctrinal legal research with the comparative approach and contextual commentary. The combination of primary legislation, secondary scholarship, expertise, and international comparisons allows approaching the topic of AI and cybersecurity laws development and the required changes in a complex and multifaceted manner.

Findings / Results

The results of the study demonstrate that the legal and institutional framework of Pakistan is still at a very low stage in solving AI-based cybersecurity issues. Despite the existence of basic legislations like Prevention of Electronic Crimes Act (PECA) 2016 and National Cyber Security Policy 2021 that can be considered formal measures to regulate cyberspace, they do not fully meet the magnitude, dynamicity, and complexity of developing AI technologies. Most importantly, PECA lacks a prospective legal framework to address the emerging threats, such as AI-generated deepfakes, algorithmic misinformation, data poisoning, or adversarial machine learning, which become more frequently applied in criminal and geopolitical scenarios (Kerry, 2020). Although the world is moving towards the development of proactive cybersecurity laws, Pakistan still depends on reactive legal systems that have a narrow scope and enforcement capabilities. The empirical analysis indicates that there is a significant deficit in the institutional readiness to AI-based cyber threats. Based on statistics gathered by the Ministry of IT and the Cyber Crime Wing of the Federal Investigation Agency, the volume of incidents related to the AI-related manipulation (including spoofed images, synthetic media, or automated phishing systems) has grown and institutional reporting patterns are outdated and disjointed. Table 1 demonstrates that the lack of AI-centered categorization of crime data in the official statistics of Pakistan restricts the capacity of policymakers to take a strategic approach to the problem.

Table 1: Cybercrime Trends in Pakistan (2020–2024)

Year	Total Cybercrime Cases	Estimated AI-Driven Cases	% AI-Related (Est.)
2020	62,500	~1,800	2.8%
2021	74,000	~3,100	4.2%
2022	89,300	~5,900	6.6%
2023	98,200	~8,500	8.6%
2024	107,400 (est.)	~11,300 (est.)	10.5% (est.)

Source: FIA Cybercrime Wing Annual Reports (2020–2023), estimates based on AI-suspected categories by PTA

The data suggest a rising trend of AI-enhanced cybercrimes, yet PECA's current language remains focused on conventional threats such as unauthorized access, spamming, and online defamation. The law does not explicitly refer to either AI or machine learning technologies, which restricts its applicability and flexibility. Moreover, the use of PECA is also subject to the interpretation of non-expert law enforcement workers, a significant number of whom do not have the training or the equipment to detect or pursue AI-generated digital evidence. This operational constraint is in itself an extension of an issue of capacity and coordination.

The Table 2 highlights this difficulty by juxtaposing the institutional capacity of Pakistan with other developing countries that have already started to adopt AI-related cybersecurity mechanisms in their national systems.

Table 2: Comparative Cybersecurity Preparedness (2023)

Country	AI-Specific Cyber Law	National CERT AI Unit	AI Cyber Training Program	Legal Framework Updated After 2020
Pakistan	No	No	Partial (FIA only)	No
Malaysia	Yes	Yes	Yes	Yes
Brazil	Yes	Yes	Yes	Yes
Egypt	No	Yes	Yes	Partial
Estonia	Yes	Yes	Yes	Yes

Source: Global Cybersecurity Index (ITU, 2023)

Whereas many countries have already started to create specific AI divisions in their national CERTs (Computer Emergency Response Teams) or have modified their legislations to include AI-specific definitions and criminal acts, Pakistan still lags far behind in that respect. Among the ambitious objectives of the National Cyber Security Policy 2021, one can find the reinforcement of institutional frameworks and the development of public-private partnerships. Nevertheless, it is poorly implemented and coordination mechanisms are weak. The absence of a central enforcement or oversight agency to address the threat of AI based threats is a source of jurisdiction overlap between agencies like the PTA, FIA, and the Ministry of IT.

Table 3 also shows how there is a lack of cohesion in the role of cybersecurity among Pakistani institutions, showing how the authority is shared and how this creates a lack of response.

Table 3: Institutional Roles in Cybersecurity Governance (Pakistan)

Institution	Legal Mandate	Technical Capacity	AI-Related Mandate	Coordination Level
FIA (Cyber Crime)	PECA	Moderate	No	Moderate
PTA	PECA Sec. 37	Limited	No	Low
Ministry of IT	Policy Making	Moderate	Indirect	Moderate
Intelligence Bureau	Security Ops	High (internal use)	Classified	Minimal

Source: National Cyber Security Policy (2021), FIA internal briefings, MoITT reports

These jurisdictions overlap, which undermines accountability and slows down the concerted efforts to respond to the cyber threats. Experts argue that without a unified command structure and clear delineation of roles, Pakistan's cybersecurity governance will continue to suffer from inefficiency and inconsistency (Rizwan, 2021). Also, there is a shortage of transparency and information exchange structures between agencies that prevent the development of trust and effective AI risk management procedures.

The most disturbing discovery is that there is no evident legal or procedural system of assigning responsibility on the cases that involve AI-generated cybercrimes. In jurisdictions with a multi-level accountability regime such as the European Union, where liability is attributed to AI-generated actions based on GDPR and AI Act proposals, a digital forensics ecosystem enables the attribution of liability. In contrast, Pakistan has no legislative solutions to algorithmic accountability or transparency. The court system is also poorly prepared, and no judgments have been reported to offer any legal precedent on how to deal with AI-inspired crimes. Consequently, this leaves victims and law enforcement agencies unable to find legal clarity.

The table 4 exemplifies this regulatory vacuum by comparing the AI-specific accountability systems in major international frameworks to the ones that do not exist in Pakistan.

Table 4: AI Accountability Mechanisms in Cyber Laws

Legal Feature	Pakistan	EU GDPR	US NIST	UK Online Safety Act
Algorithmic transparency clause	No	Yes	Partial	Yes
AI liability provisions	No	Yes	Partial	Yes
AI forensic admissibility rules	No	Yes	Yes	Yes
AI oversight or audit requirement	No	Yes	Yes	Yes

Source: European Commission (2022), UK Parliament (2023), NIST AI Risk Framework (2021)

The absence of these features in Pakistan's legal framework highlights a critical vulnerability. Until there is a legislative revision that incorporates AI-specific terminology and obligations into PECA or some other AI Cybercrime Act, the enforcing agencies will lack the necessary strength to prosecute AI-related crimes. The legislative gap created by the lack of comprehensive regulation of AI could be compromising the rights of individuals and national cybersecurity as the technology advances and becomes integrated with social media, financial systems, and national databases.

In conclusion, the results of this study highlight four central findings: Pakistan's legal and institutional structures are insufficient to tackle AI-enhanced threats; PECA lacks both updated scope and proactive enforcement; cybersecurity policy reform remains fragmented due to inter-agency inefficiencies; and, critically, there is no formal mechanism for legal accountability in cases of AI-driven cybercrime. These problems could not be solved without the organized legislative, institutional, and technological changes, and thus the national digital security of Pakistan will continue to be exposed to the fast developing cyber threats.

Discussion

This discussion relates the empirical evidence to the theoretical approach and the international practices to provide a more distinct picture of the cybersecurity legal framework of Pakistan, particularly in response to the threats of AI-powered attacks. Although PECA 2016 and the National Cyber Security Policy 2021 are significant milestones in the country's digital governance, they lag behind the rapid technological advancements—particularly in AI—that now shape cyber threats. This mismatch is not only a personal digital rights and institutional performance issue but also the national security issue on a larger scale that increasingly depends on digital sovereignty.

Securitization Theory Securitization Theory is a theory which describes how Pakistan presents cybersecurity as a national security problem, frequently as a response to large-scale incidents or perceived threats. Although such a framing is able to justify robust state action, it tends to result in reactive, rather than pro-active, legal instruments. In 2016, in response to the increased cybercrime, PECA was passed, which focuses on the traditional crimes such as hacking and harassment but omits AI-powered crimes (Buzan et al., 2007). The legal system needs to be updated, as the emergence of AI tools such as deepfakes and algorithmic assaults turn into central elements of the cyber conflict. PECA and other legislation is still too limited to take on these emerging issues.

AI's increased use in Pakistan’s digital sphere brings about threats that current laws are ill-equipped to handle. Current laws that cover content misuse and identity theft are not sufficient to cover crimes that involve AI-based systems. To illustrate, political deepfakes and fake synthetic content have detection and attribution problems. Without particular legal standards for algorithmic accountability, legal liability is uncertain. Technological advances transform legal standards, as Smith and Marx (2007) point out, but in Pakistan, legislation remains out of date with respect to the views on intention and accountability.

One of the key findings of this work is that even after the amendments in 2023 and 2025, PECA does not contain any terms or enforcement mechanisms related to AI. Although the National Cyber Security Policy 2021 is written in a progressive tone, it lacks specifics on how AI regulation should take place. Although it is stated that it will protect the critical infrastructure and increase cyber awareness, it lacks specific risk modelling based on AI and ethical governance. This regulation embodies the Technological Determinism principle which is that technological innovation leads a society to change at a rate that institutions cannot keep up with (Winner, 2010). The outcome is legal paralysis on the move of the rapid digital threats.

Legal Realism also demonstrates real-world inadequacies of the cyber laws in Pakistan. It suggests that a law's success depends on how it is enforced, not just how it is written (Leiter, 2007). The FIA Cyber Crime Wing in Pakistan deals with the majority of cybercrime cases, but it is usually not trained to handle AI-related crimes. According to internal FIA reports, over 60 percent of cybercrime cases that were reported in 2023 were not tried, with the cases being either dropped because of insufficient evidence or unclear legal premises. Such legal ambiguity undermines the confidence of the population and encourages more abuse of the digital platforms.

Glancing at the international market, other nations have more developed models. The GDPR and AI Act of the EU are intended to establish legal clarity by enhancing transparency and accountability in the AI system (European Commission, 2022). The U.S. NIST Cybersecurity Framework integrates AI as one of the fundamental risk vectors and sets the rules of its regulation (Kerry, 2020). Similarly, Singapore and India have implemented laws that are related to AI, ethical monitoring, and national CERT initiatives. These two examples indicate the importance of harmonious legal frameworks and inter-sector collaboration, which is also of great concern in the Pakistani system.

The other obstacle is the institutional structure in Pakistan to effective AI governance. The overlapping responsibilities of agencies such as the PTA, FIA, Ministry of IT, and the provincial law enforcers cause confusion and inefficiency when responding to cyber threats. Despite the establishment of such bodies as the Cyber Governance Policy Committee (CGPC) and the proposed National Computer Emergency Response Team (nCERT), the problem of coordination is still low because of bureaucracy and insufficient technical resources. Such institutional defects complicate the development of a coherent national response to changing cyber risks of AI.

Another problem is that there is no systematic public-private collaboration in cybersecurity, which is especially relevant in AI-driven settings. In such nations as the UK and Canada, the government collaborates with private tech companies to share threat intelligence, collaboratively develop AI-based security systems, and create ethical frameworks (Chander, 2021). In Pakistan cooperation is however informal or confined to adhering to PTA guidelines. Future legal reforms will probably be incomplete without further cooperation between developers, academic researchers, and civil society. Digital governance requires a multi-stakeholder, transparent and broad based approach that is sustainable.

The study also discovers that there is no clear legal framework of assigning responsibility in AI-related cybercrime in Pakistan. The common laws depend on intention and direct action.

AI systems, and especially adaptive or autonomous ones, however, erase these boundaries. As an example, in case a data breach is committed by an AI bot, who will take responsibility: the developer or the operator or both? The legal system of Pakistan does not offer any solutions. Conversely, the AI Act developed by the EU has a risk-based approach, which incorporates human oversight as an obligatory requirement in the highest-risk AI applications, which contributes to accountability (European Commission, 2022).

To conclude, Pakistan finds itself at the turning point. Though it has shown early success in the process of legislating cybercrimes and developing policy, its legal and institutional framework is not ready to deal with the unique and growing threats of artificial intelligence. These issues are the ineffective legislation, poor implementation, institutional duplication, and lack of collaboration with the major stakeholders. Theoretical approaches like Securitization Theory, Technological Determinism and Legal Realism provide insight into these issues and provide reform avenues. In the future, Pakistan should include AI-specific clauses to PECA or new AI and Cybersecurity Act, increase capacity building, institutional streamlining, and the engagement of domestic and international partners. The only way to achieve the digital sovereignty of Pakistan in the AI era is a multi-pronged, proactive approach.

Conclusion

The high rate of artificial intelligence development and implementation in digital systems has largely changed the cybersecurity situation in Pakistan and other countries. The transformation highlights the dire necessity of a strong, visionary cybersecurity legislation which is not only tech-sensitive but also tactically exhaustive. In the case of Pakistan, although PECA 2016 and National Cyber Security Policy 2021 are essential legal and policy frameworks, they are not sufficient to deal with the nuances of cyber threats brought about by AI. The urgency of the need to recalibrate the legal response in view of the increasing autonomy and sophistication of AI applications and applications of AI, which includes automated disinformation down to algorithmic intrusions that have a distinct quality of risks and liabilities of their own. In the absence of such reforms, Pakistan may lose its pace towards securing its cyberspace as well as maintaining its national sovereignty in the digital space.

The element of AI in the cyberattacks changes the threat matrix to its very core. The classical cyber threats, including phishing, malware, and unauthorized access, are now being automated, targeted accurately, and manipulated in bulk with the help of AI. Such threats are extremely dangerous to the national security, critical infrastructure, civil liberties, and economic stability. Thus, Pakistan should come up with a new generation of law tools that can control not just the participants but also the autonomous systems utilized in cyber crimes. According to Bryson (2019), legislations that do not recognize the autonomy and adaptability of AI systems will be structurally unable to provide justice or guarantee accountability. The fact that PECA does not contain any AI-specific provisions or mechanisms of algorithmic regulation reduces its applicability in the modern digital world.

The multifaceted nature of cybersecurity issues in the AI era requires a coherent national approach that is essential to handle them. This is one of the major flaws of the current strategy of Pakistan, as the inter-agency coordination is not effective. The agencies like the Pakistan Telecommunication Authority, Federal Investigation Agency, and the Ministry of IT have a duplicating mandate and little synergy because of which there is institutional fragmentation and inefficiency. This division complicates the implementation of the current legislation and prevents the maintenance of combined response systems to threats. The national cybersecurity needs not only the legislative framework but also the model of governance that would enable real-time collaboration, data sharing, and collective intelligence between the state and the enterprise (DeNardis, 2020). Pakistan will have to implement a more coherent command, which could be in the form of a central cybersecurity body, to monitor AI-specific threat intelligence, forensics, and regulatory compliance.

International cooperation is also required by the increase in global interconnectedness of cyber threats. Cyberattacks facilitated by AI tend to cross national boundaries, using the loopholes in the law and jurisdiction. Pakistan will thus be required to benchmark its cybersecurity regulations with the global standards, including the EU General Data Protection Regulation and the proposed AI Act, which encourage algorithmic transparency, data rights, and ethical AI use. The lessons of best practice can be obtained by studying the experience of those countries that have already established or are currently developing AI-based legal systems and can be used in the domestic context. Additionally, the involvement in the international cybersecurity conferences and bilateral agreements on cybercrime extradition and the regulation of AI will increase the national resilience in the digital sphere and strengthen the international reputation of Pakistan. Chertoff and Simon (2018) believe that global cybersecurity issues require global responses based on common principles of the law and interoperability between technologies.

The other burning issue is the gap between policy formulation and on-ground enforcement. Although proper policies are in place, like the National Cyber Security Policy 2021, they are not always implemented due to a shortage of resources, training, and legal awareness of law enforcement and judicial workers. To illustrate, most FIA cybercrime investigators and prosecutors do not have the specialized knowledge to process cases that involve AI-generated content, synthetic media, or algorithmic manipulation. Such knowledge deficit undermines the practical effectiveness of otherwise good-intentioned laws. Legal Realism highlights this issue by emphasizing that the law's effectiveness depends on how it is interpreted and applied in everyday settings, not merely how it is written (Leiter, 2007). The process of closing this gap will involve specific capacity-building efforts, on-going legal training, and funding of digital forensic tools.

Use of public-private partnerships in the cybersecurity governance in Pakistan is also underutilized. Since a significant part of the innovation used in AI and cybersecurity was developed in the private sector, governments should actively cooperate with technology corporations, universities, and civil society. These collaborations are essential to build threat intelligence systems, principles of ethical AI, and co-regulation. The United States and the United Kingdom are countries that have managed to adopt the system in which industry professionals are involved in the development of the regulatory procedures and policy suggestions (Wagner, 2021). Pakistan must establish official channels that will allow the participation of the private sector in the drafting of laws, monitoring of policies, and responses to incidents.

To sum up, Pakistan is at a turning point of its digital governance. The dangers of the AI-enhanced cyberattacks are no longer hypothetical; they are actual, present, and more challenging to address with the legislative instruments that have long become outdated. The necessity of the encompassing legal changes that will incorporate the AI-specific definitions, accountability frameworks, and enforcement tools is urgent. The other aspect is the formulation of an integrated national strategy on cybersecurity that will be enhanced by inter-agency coordination, international cooperation and robust enforcement capability. Pakistan can only achieve a safe and resilient digital environment that will be able to withstand the challenges of the AI age by narrowing the law-practice gap and adopting a multi-stakeholder approach.

Recommendations

With the changing landscape of cybersecurity threats, especially those fuelled by artificial intelligence (AI), the current legal and institutional framework should be re-invented in Pakistan. As shown in the findings of this study, although such major initiatives as the

Prevention of Electronic Crimes Act (PECA) 2016 and the National Cyber Security Policy 2021 have established a rudimentary legal framework, they are inadequately prepared to address the magnitude, velocity, and intricacy of AI-related cyber threats. The following suggestions are aimed at filling the legal, institutional, and strategic gaps that have been identified in this paper and at assisting policymakers, legal practitioners, and national security strategists in strengthening the Pakistani digital resilience during the age of AI.

I. Introduce AI-specific clauses in PECA and related regulations

The existing PECA cannot respond to the crimes that involve the advanced AI technologies like deepfakes, algorithmic disinformation, and autonomous malware. PECA must be revised in such a way that it contains provisions defining AI-generated content, how it can be misused, and what penalties can be imposed on AI-related crimes. It should also have provisions as to how digital evidence produced by AI systems can be gathered, analysed, and put forth in courts. Such amendments would provide legal clarity for investigators, prosecutors, and judges when dealing with AI-related cybercrimes and help align Pakistan's legislation with emerging global standards.

II. Establish an independent Cybersecurity and AI Regulatory Authority

Pakistan needs to establish a special regulatory body that would be in charge of regulating AI and cybersecurity governance to centralize the efforts and remove the redundancies in mandates. This organization must come up with standards of compliance, control public and personal AI usage, and apply a unified threat intelligence and incident response. It has to act without political pressure and should have the legal powers to control all the bodies that deal with cybersecurity. It must comprise legal experts, ethicists, cybersecurity experts, AI experts and public administration experts. Such a regulatory body would guarantee a consistent national reaction to AI-related threats and become a centre of policy implementation, enforcement, and control.

III. Enhance technical capacity building for law enforcement and judiciary

Among the key issues facing the implementation of cyber laws in Pakistan is the lack of technical expertise by the law enforcement officers as well as individuals within the judiciary. Specific education is to be provided to investigators, prosecutors and judges on the work of AI systems, the peculiarities of AI-generated evidence and the legal framework required to deal with innovative technologies. Such trainings ought to be institutionalized as formal curriculum in police schools and law training schools. In addition, it is possible to increase the quality and speed of decision-making in sophisticated AI cases by establishing specialized cybercrime courts.

IV. Develop frameworks for ethical AI use in cybersecurity defence

Pakistan should make sure that the use of AI in the field of cybersecurity does not violate civil liberties or human rights. To this end, national strategy of ethical AI must be created. Such a framework must present the major principles of transparency, accountability, fairness, non-discrimination, and human control in the application of AI, especially in government-driven cybersecurity efforts. The security agencies that use AI systems to conduct surveillance, predictive policing, or cyber defence should be audited and ethically reviewed. This kind of framework would not only make responsible innovation but also increase the trust in the people concerning government-led AI initiatives.

V. Strengthen public-private partnerships for cyber resilience

The private sector is important in the development of cybersecurity and AI technologies, deployment, and management. Thus, effective PPPs (public-private partnerships) are to be established on the basis of legislative tools and policies. Such collaboration may include sharing of threat intelligence on a regular basis, collaborative development of cybersecurity tools, and training programs. The cooperation with the tech firms, telecom operators, universities, and civil society organizations will help the state to be quick and aware of the current trends in cybersecurity. Further stimulation of the participation of the private sector can be done through incentives like tax deduction or grants of companies investing in cyber security infrastructure.

VI. Foster international cooperation on AI and cybersecurity standards

Since AI-driven cyber threats are cross-border, Pakistan needs to increase its international interaction. The country needs to be more engaged in the international cybersecurity platforms and embrace the international best practices concerning AI governance and cybersecurity. Bilateral and multilateral treaties should be given priority on aspects of AI regulation, cybercrime extradition and digital intelligence sharing. Also, Pakistan has to urge its cyber laws to align with international ones like GDPR and AI Act in the EU or NIST Framework in the U.S. The cooperation with other countries will allow the country to establish its digital credibility and ensure its cyber frontiers in the ever-intertwined world.

All these six suggestions can serve as a holistic guide on how to transform and how Pakistan approaches AI and cybersecurity. The modernization of the legal framework, the reorganization of the institutions, moral regulation, and international cooperation are the key elements of the robust cybersecurity system in the digital era. Adopting such proposals would not only protect the digital sovereignty of Pakistan, but also improve its role in the international system of cybersecurity governance.

References

Ahmed, A., & Lallani, S. (2020). AI and the law in Pakistan: Risks, gaps, and opportunities. Pakistan Journal of Law and Technology, 4(1), 55–72.

Ahmed, S. (2020). Cyber laws in Pakistan: Issues and challenges. Lahore: Pakistan Law Review Press.

Akhtar, N., & Niazi, K. (2017). Digital surveillance and human rights in Pakistan. Islamabad: Human Rights Law Review.

Ali, Z. (2021). Digital frontlines: AI and cyber conflict in South Asia. Lahore: South Asian Strategic Studies Institute.

Anderson, P. (2020). Cyber crime law and governance in emerging economies. Cambridge: Cambridge University Press.

Azam, U. (2024). Bridging AI policy and cybersecurity law in Pakistan. Lahore: AI Law and Governance Review.

Aziz, S. (2021). Cyber security and digital governance in Pakistan. Islamabad: National Institute of Policy Studies.

Baig, A. R. (2021). Cyber incident response in Pakistan: Challenges and prospects. Karachi: Digital Security Forum.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. Oxford: Future of Humanity Institute.

Bryson, J. J. (2019). The artificial intelligence of the ethics of artificial intelligence: An introductory overview for law and regulation. Oxford: Oxford University Press.

Buzan, B., Wæver, O., & de Wilde, J. (2007). Security: A new framework for analysis. Boulder, CO: Lynne Rienner Publishers.

Chander, A. (2021). The electronic silk road: How the web binds the world together in commerce. New Haven: Yale University Press.

Chertoff, M., & Simon, T. (2018). The impact of artificial intelligence on national security and international affairs. Washington, DC: Atlantic Council Press.

Choucri, N. (2012). Cyberpolitics in international relations. Cambridge, MA: MIT Press.

Dar, F. A. (2019). Cross-border cybercrime and legal gaps in Pakistan. Quetta: Balochistan Legal Studies Journal.

DeNardis, L. (2020). The internet in everything: Freedom and security in a world with no off switch. New Haven: Yale University Press.

Dube, R., & Patel, M. (2018). Regulating the algorithm: AI, ethics, and the rule of law. New Delhi: Sage India.

European Commission. (2022). Proposal for a regulation on artificial intelligence (AI Act). Brussels: European Union Publications.

Gonzalez, M., & Brown, T. (2021). AI and national security: Emerging threats and legal dilemmas. New York: Routledge.

Green, M. (2009). Legal realism and American law. New York: Cornell University Press.

Hutchinson, T. (2010). Researching and writing in law. Sydney: Thomson Reuters.

International Telecommunication Union. (2022). Global cybersecurity index 2022. Geneva: ITU Publications.

Iqbal, N., & Zafar, A. (2019). Data protection and cyber law reform: A comparative study. Lahore: Punjab Law House.

Jamil, R., & Hussain, M. (2022). Cybersecurity training and AI readiness in Pakistan’s public sector. Rawalpindi: Policy Insights Quarterly.

Kerry, C. F. (2020). The AI policy landscape in 2020: A global perspective. Washington, DC: Brookings Institution Press.

Khan, R. M. (2023). Cyber governance in South Asia: Policies, pitfalls, and progress. Islamabad: National Defense University Press.

Khan, T. A. (2022). Artificial intelligence and law in Pakistan: Challenges and recommendations. Lahore: Punjab Legal Publishers.

Leiter, B. (2007). Naturalizing jurisprudence: Essays on American legal realism and naturalism in legal philosophy. Oxford: Oxford University Press.

Ministry of Information Technology and Telecommunication. (2021). National cyber security policy 2021. Islamabad: Government of Pakistan.

Mueller, M. (2020). Cybersecurity and the quest for cyber norms: Protecting global networks in a geopolitically contested world. Cambridge: Polity Press.

Nye, J. S. (2017). The future of power in the cyber age. New York: Oxford University Press.

Örücü, E. (2007). The enigma of comparative law: Variations on a theme for the twenty-first century. Leiden: Brill Academic Publishers.

Qureshi, M. S. (2015). Judicial responses to digital governance in Pakistan. Lahore: Progressive Legal Studies Press.

Rashid, F., & Kamal, S. (2022). Institutional coordination in Pakistan’s digital security landscape. Karachi: Centre for Strategic Technology Studies.

Rehman, M. S. (2023). Digital infrastructure and legal policy in South Asia. Karachi: South Asian Policy Review.

Rizwan, A. (2021). Governing cyberspace in Pakistan: Legal challenges and institutional gaps. Islamabad: Centre for Legal Policy Research.

Saeed, S., & Rafi, A. (2021). Legislating cyberspace: Post-PECA legal reforms in Pakistan. Lahore: Vanguard Publications.

Schmitt, M. N. (2013). Tallinn manual on the international law applicable to cyber warfare. Cambridge: Cambridge University Press.

Smith, M. R., & Marx, L. (2007). Does technology drive history? The dilemma of technological determinism. Cambridge, MA: MIT Press.

UK Parliament. (2023). Online Safety Act 2023: Regulatory framework and implications. London: Her Majesty’s Stationery Office.

United Nations International Telecommunication Union. (2023). Global cybersecurity index 2023. Geneva: ITU Publications.

Wagner, B. (2021). AI regulation and the role of human rights: Towards a technological social contract. Cambridge: Cambridge University Press.

Wazir, M., & Khan, S. (2018). Artificial intelligence and state surveillance in South Asia. Peshawar: Institute of Public Policy and Innovation.

Winner, L. (2010). The whale and the reactor: A search for limits in an age of high technology. Chicago: University of Chicago Press.

Yousaf, H., & Nasir, T. (2020). Cyber threats and critical infrastructure protection in Pakistan. Islamabad: Institute for Policy Research.