ACADEMIA International Journal for Social Sciences
Volume 5, Issue 3(c), 2026 ISSN-L (Online): 3006-6638

Collaborative Professionalism: The Role of Professional Learning Communities in Transforming Teaching Quality

Dr. Abdul Khaliq
abdulkhaliq@cuvas.edu.pk
Assistant Professor, Department of Social and Allied Sciences, Cholistan University of Veterinary and Animal Sciences, Bahawalpur, Pakistan

Umama Shafique
22-cuvas-0121@student.cuvas.edu.pk
BSCS scholar, Department of computer science and information technology, cholistan University of veterinary and animal sciences, Bahawalpur

Maryam Bibi
22-cuvas-0118@student.cuvas.edu.pk
BSCS scholar, Department of computer science and information technology, cholistan University of veterinary and animal sciences, Bahawalpur

Corresponding Author: Dr. Abdul Khaliqabdulkhaliq@cuvas.edu.pk

Received: 15-01-2026 **Revised:** 03-02-2026 **Accepted:** 16-02-2026 **Published:** 13-03-2026

ABSTRACT

The high rate of digitalization of the economy and governance structures in Pakistan has increased vulnerability to cyber threats requiring proper cybersecurity governance to be a national agenda. This paper provides a critical review of Pakistan cybersecurity regulation and governance, by looking at some of the major tools, including the Electronic Transactions Ordinance 2002, the Prevention of Electronic Crimes Act (PECA) 2016, and the National Cyber Security Policy 2021. The research employs a qualitative method of analysis, using secondary data, in the form of policy documents, legal frameworks, and academic literature and employs thematic analysis to pinpoint structural issues and regulatory gaps. The results show that despite the fact that Pakistan has established a multi-layered cybersecurity framework, the effectiveness of the framework is limited by the fragmented governance system, poorly established enforcement procedures, the lack of a set of data protection laws, the rise in cyber threats, and the insufficient institutional capacity. The research also indicates that there is a major disconnect between policy development and reality, which decreases the overall strength of the national cybersecurity ecosystem. Based on the international best practices, the study suggests that centralized governance, enforcement of the law, capacity building and coherence of the policies should be enhanced. It concludes that a comprehensive, unified, and agile solution is needed to create a secure and resilient digital space in Pakistan.

Keywords: *cybersecurity governance, regulatory frameworks, Pakistan, cyber policy, data protection.*

INTRODUCTION

Background of the Study

The increasing rate of digital transformation has completely changed the nature of economic operations, political systems, and social relations throughout the world, thus cybersecurity becomes the core of national security and economic prosperity. Governments and institutions are becoming more dependent on digital infrastructures in terms of financial transactions, delivery of public services and communication systems.

This change can be observed in Pakistan, through the rapid development of digital banking, mobile financial services, e-commerce platforms, and e-governance programs, which have not only made accessibility and efficiency much more effective. Nonetheless, this virtual growth has also made the nation susceptible to a broad range of cyber attacks, such as hacking, identity theft, phishing, financial fraud, ransomware, and cyber terrorism (Ministry of IT & Telecommunication [MoITT], 2021).

Recent developments show that cyber incidents are on the increase with a sharp growth, which is not only a result of the increased digital footprint but also a result of the increased sophistication of cybercriminal networks. Cyberattacks are increasingly organized, technologically sophisticated and financially driven and are a severe threat to both the public and the entities of the private sector. These threats may have disproportionately high impact, such as financial losses, reputational damage, and disruption of vital services, in developing economies such as Pakistan, where cybersecurity awareness and infrastructure are still developing.

To address these new realities, Pakistan has established a sequence of laws and policies to govern the cyberspace and to increase the digital security. The most important legislative tools are the Electronic Transactions Ordinance (ETO) 2002 that legalizes electronic documents and transactions and the Prevention of Electronic Crimes Act (PECA) 2016, which is the main legal means of combating cybercrime. Recently, the National Cyber Security Policy 2021 has given a strategic roadmap on how to protect national digital assets, secure critical information infrastructure, and enhance a robust cybersecurity ecosystem (MoITT, 2021).

The National Cyber Security Policy advocates a whole-of-government strategy, with centralized coordination via institutionalized processes like the Cyber Governance Policy Committee. It also emphasises on capacity building, incident response, risk management and public-private collaboration. In line with these initiatives, the emergence of institutions like the National Cyber Crime Investigation Agency (NCCIA) and the Pakistan Computer Emergency Response Team (PKCERT) indicates a rising interest in improving governance of cybersecurity and the capacity of the country to respond to cybercrimes.

Although these developments have been made, the governance of cybersecurity in Pakistan has been disjointed and dynamic. There are several institutions with overlapping mandates that pose coordination issues and inefficiencies. Moreover, the inadequacy between the development of the policies and their adaptation to the real world remains a limitation that hinders the efficiency of current frameworks. These challenges highlight the importance of a holistic, unified, and dynamic approach to cybersecurity governance that should be in place to respond to the dynamic aspect of cyber threats.

Problem Statement

Despite significant advances in the field of cybersecurity laws and policies, the existing governance structure is marked by institutional fragmentation, a lack of enforcement mechanisms, and poor inter-agency coordination in Pakistan. Although PECA 2016 offers a legal basis to combat cybercrime, it has been largely criticized due to the challenge in implementation, limitation of the procedure, and the lack of deterrence power (MoITT, 2021).

One of the big issues is the lack of an inclusive data protection legislation, which poses considerable regulatory loopholes in the protection of personal and organisational data. When data is a key asset, the absence of effective data protection devices will enhance the susceptibility to cyber exploitation and the mistrust people will have towards digital systems. Moreover, the gradual emergence of centralized

cybersecurity governance frameworks constrain the capacity of the nation to adequately respond to massive and advanced cyber attacks.

The fast-changing environment of cyber risks, which is the result of the new technological trends, including artificial intelligence, cloud computing, and the Internet of Things (IoT), needs to be regulated by adaptive, proactive, and enforceable regulations. Nevertheless, the current policies are frequently not able to follow the current technological progress. This brings a huge disparity between cyber threat dynamics and governance capacity that requires a critical analysis of the cybersecurity ecosystem in Pakistan.

Research Objectives

The study will attempt to accomplish the following objectives:

1. To critically examine the current cybersecurity governance and cybersecurity regulatory frameworks in Pakistan.
2. To spot the main challenges, gaps, and limitations in the cybersecurity policies implementation.
3. To assess the roles, responsibilities, and coordination processes of important institutions engaged in cybersecurity governance.
4. To make extensive policy recommendations on how to enhance cybersecurity governance and regulatory effectiveness.

Research Questions

This research aims to answer the following research questions:

1. What are the key elements of the cybersecurity governance and regulation system in Pakistan?
2. What do the existing policies on cybersecurity and their enforcement seek to address? What are the significant weaknesses and gaps?
3. To what extent are the current institutional set-ups effective in dealing with cyber threats and promoting digital security?
4. What are the policy changes and other strategic actions necessary in improving the governance of cybersecurity in Pakistan?

Study Importance

The paper has important theoretical, practical and policy level implications especially in the developing nations such as Pakistan. Theoretically, it adds to the increasing literature on cybersecurity governance and regulatory frameworks, providing an in-depth analysis of the interaction of the legal, institutional, and policy elements in a national system of cybersecurity. The study places context-specific details on Pakistan, which are usually underrepresented in the research of cybersecurity across the world.

In practical sense, the research provides useful insights to policy makers, legal practitioners, cybersecurity experts and institutional leaders. It points out the acute shortcomings of current frameworks and offers

practical suggestions to improve the coherence of policies, enforcement of regulations, and coordination of institutions. Such understanding can help to create more efficient cybersecurity policies, which can eventually enhance national resilience to cyber threats.

At the policy level, the research is consistent with strategic goals of Pakistan digital transformation programs as it underlines the necessity of integrated governance, strong legal framework, and capacity building. It also helps in the development of evidence-based policy changes, promoting compliance with international standards, including the NIST Cybersecurity Framework and global-best practices. The research aids in developing a safe, reliable, and reliable online space by tackling the structural and operational issues.

Study Limitation

The present study is prone to some limitations that outline its scope and the scope of analysis. It can be restricted to the analysis of the national cybersecurity governing and regulatory framework of Pakistan, including major legislation, policy, and organizational structures. The research lacks a detailed comparative study with other nations, but where appropriate, there are references to international best practices.

Moreover, the study mainly takes the policy and governance approach, which concentrates on the legal framework, the role of institutions, and regulatory mechanisms. It does not go into the technical side of implementation of cybersecurity, including system architecture, encryption technologies or network security protocols.

Although these constraints can limit the scope of the analysis, they allow conducting a narrow and deep discussion of the issues related to governance and policy implications, so that the study would be relevant and applicable to the situation in Pakistan.

LITERATURE REVIEW

The issue of cybersecurity governance has become a key area in the field of public policy and information systems studies, and it refers to the legal, institutional and strategy systems that the organization uses in order to address cyber risks and safeguard digital infrastructures. It goes past just technical protection to encompass regulatory frameworks, organizational coordination, risk management practices, and policy enforcement mechanisms (Klimburg, 2017). The current literature highlights the idea that successful cybersecurity governance must be multi-layered and integrated, consisting of legal tools, institution, and technology to achieve national cyber resilience (Siemens & Baker, 2012; Dunn Cavelty, 2014). The necessity to establish coherent and enforceable cybersecurity governance frameworks has become more urgent in developing countries where digital transformation is occurring at a blistering pace, such as Pakistan.

In theory, the current research is based on a framework that connects the structure of cybersecurity governance, the effectiveness of regulations and the national cyber resilience. In this model, legal and policy tools like PECA 2016 and National Cyber Security Policy 2021 serve as independent variables that influence the outcome of governance, whereas such factors as institutional coordination, enforcement capacity, and regulatory coherence serve as the mediating variables that affect the effectiveness of cybersecurity systems. This final dependent outcome is the degree of cyber resilience and risk mitigation capability in the national digital ecosystem. The conceptualization is that with more robust governance frameworks and integrated institutional mechanisms, better cybersecurity results and less susceptibility to cyber threats can be achieved.

Cybersecurity Governance Theory, Institutional Theory, and Risk Management Theory are sources of the theoretical foundation of this study. The Cybersecurity Governance Theory highlights the importance of policy frameworks and institutional coordination to regulate cyber risks on a national scale (Klimburg, 2017). Institutional Theory emphasizes the role of organizational structures, rules, and norms in defining the governance systems in terms of implementation and effectiveness (Scott, 2014). The Risk Management Theory, especially when embodied in models like the NIST Cybersecurity Framework, places significant emphasis on the need to perform constant risk assessment, monitoring, and adaptive response measures in achieving cybersecurity resilience (NIST, 2018). Combined, these theoretical approaches offer a holistic approach to the examination of the weaknesses and strengths of Pakistan cybersecurity governance framework.

Cybersecurity governance in the Pakistani context has developed in a sequence of legislative and policy efforts, yet the literature in this field is still quite scarce and disjointed. The policy analysis by Rahman and Iqbal (2019) of legislation of cybercrime in Pakistan revealed that PECA 2016 offers a legislative framework but is unclear in terms of enforcement processes and procedural practices. Ahmed et al. (2020) studied institutional responses to cyber threats and found that the coordination of agencies, including FIA, PTA and other regulatory authorities, is poor. Khan and Raza (2021) investigated the issue of digital security in Pakistan and found the absence of technical knowledge and inadequate infrastructure to be some of the impediments to effective governance. Ali and Saeed (2021) examined regulatory frameworks and they reported that the current policies tend to be reactive but not proactive. Hussain et al. (2022) examined the dynamic of cybercrime and discovered that financial fraud and identity theft have risen considerably, which underscores the insufficiency of the existing preventive measures. Tariq and Malik (2022) examined the use of cybersecurity policies and found that the policies are not uniformly enforced at institutions. Shah and Rehman (2023) identified gaps in training and capacity building in their study of the public sector preparedness in cybersecurity. Akhtar et al. (2023) concentrated on digital governance and pointed out the necessity of comprehensive policy frameworks. Siddiqui et al. (2024) examined cybersecurity awareness and discovered low rates of the general population, which also contributes to vulnerability. Lastly, Zafar and Qureshi (2024) have assessed the National Cyber Security Policy 2021 and have found that whereas this policy offers strategic guidance, its action is still restricted because of the systemic fragmentation. Together, these country reports indicate that there are common problems of poor enforcement, poor coordination and absence of comprehensive regulatory mechanisms.

The field of cybersecurity governance has been widely researched internationally which provides useful comparative knowledge. Dunn Cavelty (2014) examined national cybersecurity policies and highlighted the need to incorporate policy, technology, and organization structure. Klimburg (2017) examined the models of cybersecurity governance on a global scale and emphasized the usefulness of centralized coordination mechanisms. The NIST Cybersecurity Framework (2018) offers a popular framework to address cyber threats using capabilities including identification, protection, detection, response, and recovery. Von Solms and Van Niekerk (2013) analyzed the systems governing the issue and came to the conclusion that cybersecurity should be incorporated in the organizational systems of governance. ENISA (2019) researched European policies on cybersecurity and discovered that effective regulatory implementation and intersector cooperation support resilience. Bada et al. (2019) examined the awareness of cybersecurity and highlighted the importance of human factors in the effectiveness of governance. Choucri et al. (2014) also delved into the development of cyber policy and also emphasized the role of adaptive governance in the dynamic cyber threat environments. Shackelford (2016) reviewed the concept of international cyber governance and found that it was necessary to develop harmonized regulatory standards. Carr (2016) explored the subject of cyber security policy, and observed that policy should be constantly developed at the national level to respond to the emerging cyber threat. Lastly, Kshetri (2016) examined the cybersecurity ecosystems in developing countries and discovered that institutional capacity

and governance structures are key determinants of success. These cross-border analyses repeatedly indicate that centralization of governance, effective legal enforcement, and ongoing risk management are the main factors to successful cybersecurity models.

An analysis of both national and international literature indicates that there is a definite mismatch between the capacity to develop policy and to implement it. Although developed nations have developed built-in and adaptive cybersecurity regulatory frameworks, Pakistan is still confronted with issues of fragmentation, enforcement loopholes, and institutional inefficiencies. Furthermore, current studies in Pakistan are more likely to concentrate on the individual parts of cybersecurity, including the legal frameworks or trends in cybercrime, instead of offering a detailed overview of the structure of governance and its efficiency.

Thus, the main gap that the current research fills is the gap in holistic, policy-based understanding of cybersecurity governance and regulatory frameworks in Pakistan, specifically regarding the institutional coordination, enforcement mechanisms, and policy implementation. The paper will focus on filling this void by offering a comprehensive assessment of legal, policy, and institutional aspects and evidence-based suggestions on how to improve cybersecurity governance in Pakistan.

RESEARCH METHODOLOGY

The proposed study will use a qualitative analytical research design to critically analyze governance and regulatory frameworks of cybersecurity in Pakistan. A qualitative approach is deemed the most suitable since the research is aimed at policy evaluation, institutional analysis, and interpretation of legal frameworks, which demand in-depth and context-sensitive analysis instead of numerical measurement (Creswell and Creswell, 2018). It is more of an exploratory and interpretive design, with an aim of comprehending how current laws, policies, and institutions operate together to make up a national cybersecurity ecosystem.

The research is based on secondary data sources, which are gathered systematically and on a broad scope of reliable and authoritative sources. They are governmental publications, official government policy documents, legislative documents, institutional reports, and scholarly academic publications. The main sources include the legal foundations like the Electronic Transactions Ordinance (ETO) 2002 and the Prevention of Electronic Crimes Act (PECA) 2016 and the strategic policy frameworks such as the National Cyber Security Policy 2021 published by the Ministry of Information Technology and Telecommunication (MoITT). Moreover, the structure of operation and response mechanisms were also studied by reviewing institutional reports and publicly available information on organizations like the National Cyber Crime Investigation Agency (NCCIA) and the Pakistan Computer Emergency Response Team (PKCERT). It is possible to have an in-depth and policy-oriented analysis and at the same time have access to official and up-to-date information through the use of secondary data (Bowen, 2009).

Following the conceptual and theoretical backgrounds of the literature review, the study is geared towards the three main dimensions of analysis namely: legal frameworks, policy frameworks and institutional structures. Legal dimension measures the extent of, effectiveness, and enforcement ability of the cyber laws, especially PECA 2016, in dealing with cybercrime and cybersecurity issues. The policy aspect looks at the strategic orientation, implementation mechanisms, and the governance structure of the National Cyber Security Policy 2021. The institutional dimension examines the role, responsibilities and coordination of primary cybersecurity agencies such as NCCIA, PKCERT and other regulatory agencies. The choice of these dimensions is influenced by the developed models of cybersecurity governance, which focuses on coordinating legal, organizational, and strategic aspects (Klimburg, 2017; NIST, 2018).

To analyze the data, the research will utilize a thematic analysis methodology that is common in qualitative research studies to identify, analyze and interpret the trends in a textual data (Braun and Clarke, 2006). It was done in a systematic manner, which included a number of steps. First, key themes concerning cybersecurity governance were identified by carefully reviewing and coding the relevant documents. Second, these codes were clustered into more general groups, including policy fragmentation, enforcement issues, institutional coordination, and regulatory gaps. Third, the themes were decoded within the conceptual framework and theoretical perspectives of the study, which allowed gaining a better insight into the strengths and limitations of the system of cybersecurity governance in Pakistan. This will enable rigorous and flexible analysis that is also contextually relevant.

In order to increase the validity and reliability of the results, the research used data triangulation, which involved comparing data on various sources, such as legal texts, policy documents, and academic research (Yin, 2018). This served to create consistency and minimize the possible interpretation bias. Moreover, the theoretical frameworks such as Cybersecurity Governance Theory and Institutional Theory, were used in the analysis and presented a solid analytical perspective to assess the effectiveness of governance.

There were also ethical considerations that were keenly followed during the research process. Since the research will be founded on publicly accessible secondary sources, challenges of confidentiality and consent of participants are reduced to a minimum. Nevertheless, no sources were referenced and acknowledged improperly and in accordance to the requirements of APA 7th edition, which guaranteed academic integrity and transparency.

On the whole, this methodology is a systematic, theory-based, and comprehensive framework to analyze cybersecurity governance in Pakistan. The combination of policy analysis and thematic interpretation provides a subtle view of the issues of regulation and institutional processes, as well as leads to the development of evidence-based implications to improve policies and governance.

FINDINGS AND ANALYSIS

Thematic analysis of the legal tools, policy frameworks and institutional arrangements suggests that the country has developed a multi-layered cybersecurity governance structure that includes statutory laws (e.g., ETO 2002, PECA 2016), strategic policy (the National Cyber Security Policy 2021) and operational organizations (e.g., NCCIA, PKCERT). Although this architecture offers a baseline set of understanding of cyber risk management, its overall performance is limited by the structural, regulatory, and capacity issues. The results are summarized under five themes that are interconnected and reflect a critical aspect of governance efficiency.

Table 1: Summary of Thematic Findings in Cybersecurity Governance

Theme	Core Issue	Evidence Base	Governance Impact
Fragmented Governance	Overlapping mandates, weak coordination	Multiple agencies with parallel roles	Delayed decision-making, policy incoherence
Weak Enforcement	Limited implementation capacity	Low conviction/operational follow-through under PECA	Reduced deterrence, compliance gaps
Data Protection Gap	Absence of comprehensive law	No fully enacted, unified data protection regime	Privacy risks, regulatory ambiguity

Rising Cyber Threats	Increasing frequency/complexity of attacks	Growth in fraud, phishing, ransomware	Exposure of critical sectors
Institutional Capacity	Skills, resources, infrastructure deficits	Limited CERT reach, training gaps	Slower response, limited resilience

Table 1 integrates the essence of the governance challenges that have been revealed in the study of documents. It shows that even with the existence of legal and policy tools, system-level limitations, especially in the area of coordination, enforcement, and capacity, greatly weaken overall effectiveness.

One of the most predominant results is the disintegration of the governance of cybersecurity, with several organizations, such as the Federal Investigation Agency (FIA/NCCIA), Pakistan Telecommunication Authority (PTA), MoITT, and PKCERT, having overlapping mandates. This is due to the lack of a clearly empowered central coordinating body leading to duplication of policies, inconsistent implementation of policies and slow response to incidents.

Table 2: Institutional Roles and Coordination Gaps

Institution	Mandate	Overlap Area	Observed Gap
NCCIA (FIA)	Cybercrime investigation	Incident response, forensics	Limited coordination with CERTs
PTA	Telecom regulation	Platform control, compliance	Regulatory–operational disconnect
MoITT	Policy formulation	Strategy & governance	Weak enforcement linkage
PKCERT	Incident response	Threat intelligence	Limited national coverage

Table 2 shows that institutional requirements are present, but the overlapping of the functions and poor inter-agency guidelines form a bottleneck in coordination. This division compromises the whole-of-government approach as envisaged in the National Cyber Security Policy.

Despite the fact that PECA 2016 offers a legal framework of the control of cybercrime, the analysis shows that the control is rather weak in the context of procedural limitations, gaps in investigation capabilities, and delays in the judicial process. This diminishes the value of the law in deterring and dilutes the compliance within sectors.

Table 3: Assessment of Legal Framework Effectiveness

Legal Instrument	Strength	Limitation	Overall Effectiveness
ETO 2002	Legal recognition of e-transactions	Outdated for modern threats	Moderate
PECA 2016	Comprehensive cybercrime coverage	Enforcement and procedural gaps	Moderate–Low
Cyber Policy 2021	Strategic direction	Weak implementation mechanisms	Moderate

Table 3 shows that Pakistan has a moderately to low operational effectiveness of its legal architecture, despite the apparent formal sufficiency of the legal architecture, which can be explained by lack of enforcement, and changing threat environment.

The absence of a fully implemented, comprehensive regime of data protection is a critical governance gap. In the framework of growing levels of digitization, lack of clear guidelines on data collection, processing, storage, and cross-border transfer introduces legal uncertainties, and heightens privacy risks.

Table 4: Data Protection and Privacy Landscape

Dimension	Current Status	Implication
Personal Data Protection	Draft/partial frameworks	Regulatory uncertainty
Institutional Compliance	Inconsistent	Weak accountability
User Rights Protection	Limited codification	Privacy vulnerabilities
Cross-Border Data Rules	Underdeveloped	Trade and compliance risks

As shown in Table 4, any data protection gaps undermine trust in digital systems and make it difficult to meet international standards, impacting citizen protection and digital economy development.

The assessment establishes an increase in cyber attacks, such as phishing, online financial fraud, identity theft, and ransomware. The fast pace of digital services adoption, and in many cases faster than security investments, has increased the attack surface of banking, telecom, and public services.

Table 5: Major Cyber Threat Trends in Pakistan

Threat Type	Growth Trend	Target Sector	Risk Level
Phishing & Social Engineering	High	Individuals, banking	High
Financial Fraud	Increasing	FinTech, e-commerce	High
Identity Theft	Moderate–High	Public services	Medium–High
Ransomware/Malware	Emerging	SMEs, institutions	Medium

As Table 5 points out, the attack threat is dominated by behavioral and financially motivated attacks, which reveals vulnerabilities in the user awareness, authentication controls, and monitoring systems.

Lastly, the research reveals the capacity constraints in the form of skilled labor force, technical infrastructure, and readiness to respond to incidents. Whereas organizations such as PKCERT are a step in the right direction, coverage, tooling, and integration are lacking on a national level.

Table 6: Institutional Capacity Assessment

Capacity Dimension	Current Status	Impact on Governance
Technical Expertise	Limited specialist pool	Slower detection & response
Infrastructure	Developing, uneven	Incomplete coverage
Training & Awareness	Sporadic initiatives	Human-factor vulnerabilities
Incident Response	Partially operational	Delayed mitigation

Table 6 shows that operational effectiveness is limited by capacity gaps, especially in real-time threat detection and coordinated response which are critical to contemporary cybersecurity governance.

Themes In general, the results suggest that the governance of cybersecurity in Pakistan is institutionally sound yet limited in its activities. Legal and policy tools offer a requisite base, but fragmented governance, lax enforcement, lack of comprehensive data protection, growing threats, and capacity shortages restrain their effectiveness. The evidence indicates that to achieve better results, there is a need to change the approach to centralized coordination, enforceable regulation, the development of capabilities, and consistent risk management, which are in line with the best practices on the international level, including the NIST framework.

The ecosystem of cybersecurity in Pakistan is undergoing a transition stage, i.e. the stage of policy establishment into a more challenging stage of coordinated, enforceable and capacity-supported governance. This transition should be enhanced to enhance sustainable cyber resilience in a more digital economy.

DISCUSSION

The current paper aimed at assessing the efficacy of cybersecurity governance and regulation systems in Pakistan through analyzing legal tools, policy guidelines, and institutional designs. The results show that Pakistan has achieved significant gains in the development of a multi-layered cybersecurity architecture, but the effectiveness of the architecture is limited by its systemic vulnerabilities, the most notable of which are disjointed governance, ineffective enforcement, regulatory gaps, the increasing complexity of threats, and limited institutional capacity. The results can be interpreted better when they are placed in the context of established theoretical perspectives and international best practices.

One of the key conclusions of the research is that cybersecurity governance is in fragments, as evidenced by duplication of mandates and poor coordination between agencies like NCCIA, PTA, MoITT, and PKCERT. This is consistent with the principal assumption of Cybersecurity Governance Theory that the effective management of cyber risk should be centralized and have clear institutional roles and functions (Klimburg, 2017). Lack of central authority or coordinated model of governance in Pakistan creates discrepancies in the policies, repetition of actions, and slow reaction to cyber attacks. The same can be said about international research, in which fragmented governance frameworks are linked to reduced cyber resilience (Shackelford, 2016). Conversely, those nations that embrace centralized or well coordinated governance systems are likely to exhibit better incident management and implementation of policies.

Poor application of law frameworks, especially PECA 2016 which, despite having extensive coverage of cyber offenses, has implementation issues, is also mentioned in the study. This observation is consistent with the Institutional Theory, which assumes that the efficiency of formal rules is not only based on their design but also on the ability of institutions to implement them (Scott, 2014). In Pakistan, the deterrence effect of cyber laws is minimized due to restrictions in investigative capacity, procedural inefficiencies, and judicial delays. In line with the same, earlier research also points out that legal frameworks that lack effective enforcement systems do not bring about the desired regulatory effects (Kshetri, 2016). This implies that enhancing enforcement capacity is as important as formulating the legal provisions.

The other notable challenge is the lack of a universal data protection law that poses a big regulatory loophole in the cybersecurity landscape in Pakistan. The personal and organizational data have become important assets in the age of data-driven economies that must be effectively secured. Absence of a single law model that regulates data privacy is a weakness that erodes the trust of users and exposes them to cyber exploitation. This observation is aligned with the global literature, which highlights that data protection is one of the foundations of cybersecurity governance and the precondition of digital trust and economic development (ENISA, 2019). The higher the data protection regime of the country (the country in

accordance with GDPR standards), the more mature the state of cybersecurity and the confidence of the users.

The research also indicates that cyber threats such as phishing, financial frauds, identity theft, and ransomware attacks have greatly risen. The trend is indicative of the growing online presence of the Pakistani economy and the increasing complexity of cybercrimes. Theoretically, this concurs with Risk Management Theory, which emphasizes the necessity of active monitoring, dynamic responses, and prevention of risk in the dynamic threat environment (NIST, 2018). The results indicate that the existing governance model in Pakistan is more of a reactive model that deals with responding to incidents and not with the risk management. This is unlike the international best practices, which have cybersecurity frameworks that focus on anticipation, prevention and resilience-building.

Another critical challenge that has been noted in the study is the institutional capacity constraints. Lack of technical skills, poor infrastructure and lack of training initiatives are factors that do not help institutions to be able to adequately respond to cyber threat. This is in line with previous studies that show that effective cybersecurity governance relies on human capital and technical capacity, especially in developing economies (Kshetri, 2016). Even the policies that are well-designed cannot be effective without a skilled personnel and sophisticated technological equipment. The paper also emphasizes that it is necessary to engage in continuous capacity building and invest in cybersecurity infrastructure, which will be needed to improve national resilience.

Notably, the results indicate a bigger problem: the mismatch between the development of policy and its practical application. Although Pakistan has come up with various policies and strategies, their implementation is hampered by poor coordination, enforcement, and capacity. Such a gap aligns with what Dunn Cavelty (2014) refers to as the implementations deficit in the field of cybersecurity governance wherein policies are theoretically established but not practically implemented. The gap between the two has to be filled by both institutional reforms as well as a change in the direction towards integrated forms of governance that balances legal, technical, and organizational aspects.

Compared to global standards like the NIST Cybersecurity Framework, the approach of Pakistan does not have a full-fledged system of constant risk assessment, monitoring, and feedback mechanisms (NIST, 2018). The NIST model focuses on five primary functions, including identify, protect, detect, respond, and recover, that can help develop a comprehensive and adaptive approach to cybersecurity. The lack of such systematic and cyclical process in Pakistan restricts its ability to react to new threats in an effective way.

On balance, the discussion demonstrates that the cybersecurity governance in Pakistan is in its transitional phase, with a solid base of policy formulation, but limited operational maturity. Although the creation of legal frameworks and institutions is a good move, the effectiveness of such moves hinges on how the coordination is strengthened, improved enforcement, how regulatory loopholes are eliminated, and the institutional capacity is developed. The results support the idea of a comprehensive and coordinated approach to cybersecurity governance that responds to national policies and adheres to international standards but also considers context-dependent issues.

CONCLUSION

This paper offers a thorough overview of cybersecurity governance and regulatory frameworks in Pakistan, including legal tools as well as policy frameworks and institutional organization. The results indicate that Pakistan has laid the groundwork of a cybersecurity architecture by using such tools as the Electronic Transactions Ordinance 2002, Prevention of Electronic Crimes Act (PECA) 2016, and the National Cyber

Security Policy 2021, as well as developing functional agencies, including NCCIA and PKCERT. These changes are indicative of an increasing awareness of cybersecurity as a national priority in an increasingly digital world.

Nevertheless, the paper finds that, regardless of this development, the overall effectiveness of cybersecurity governance in Pakistan is weak and unequal. Institutional fragmentation, poor enforcement mechanisms, lack of encompassing data protection laws, rising cyber threats, and lack of technical and organizational capacity are all limitations of the governance framework. All these issues result in a disconnect between policymaking and concrete action-taking, making the state less effective in its response to changing cyber threats.

The research also concludes that the state of cybersecurity governance in Pakistan is in a transitional state, in which the policies are already implemented, but they are relatively immature and need operational maturity to be put into practice. The lack of a coordinated and integrated system of governance is a major constraint to coordination and accountability in institutions. Moreover, the absence of active risk management and systematic monitoring systems makes the country limited in its capacity to establish long-term cyber resilience.

Essentially, although Pakistan has made significant strides toward developing a cybersecurity framework, structural changes, institutional coordination, and alignment to international standards would put in place a secure, resilient, and trustworthy digital ecosystem. The future success of cybersecurity governance will be determined by how the country will shift towards policy-based approach to a fully operationalized, enforcement-based system of governance.

RECOMMENDATIONS

Considering the findings and conclusions of this paper, the following policy-relevant recommendations are made, to enhance the cybersecurity governance in Pakistan:

The most important one is the creation of a centralized national cybersecurity body with specific powers and duties. This kind of authority would be used as the main coordinating force, which guarantees the coordination of policy, inter-agency efforts, and response mechanisms. The centralized form of governance has been found to be very effective in supporting cybersecurity efforts through lessening institutional fragmentation and enhancing accountability.

It is critical to reinforce the mechanisms of enforcement of the current legal frameworks, especially PECA 2016. This involves increasing the capacity of the law enforcement agencies, improving the investigative processes and providing the timely judicial proceedings. Legal frameworks cannot be used as effective preventive measures to curb cybercrime without effective enforcement.

A policy that focuses on passing a comprehensive data protection law that articulates data privacy, data security, and cross-border data flows standards should be a priority of the government. This type of legislation is necessary to safeguard the rights of citizens, and to gain confidence in the digital systems as well as to match Pakistan to the international standards of regulations.

It is also critical that institutional capacity building and technical infrastructure be invested in. These involve creating a highly proficient cybersecurity workforce, setting up sophisticated threat detectors, and enhancing incident response capabilities. The existing skills gap can be addressed through continuous training programs and collaboration with academic institutions and the private sector.

Also, it is necessary to implement a risk-based and proactive approach to cybersecurity, and it is consistent with the international frameworks, including the NIST Cybersecurity Framework. This would entail the continuous risk assessment, real-time monitoring, and adaptive response strategies in order to respond effectively to the emerging cyber threats.

Another recommendation is the increase in the cooperation between the government and the business community. Since much of the critical infrastructure is handled by the private sector, robust collaborations among government agencies, industry players, and technology vendors are essential to proper cybersecurity governance. The national resilience can be enhanced by information sharing and mechanisms of joint response.

Besides this, the government must establish national cybersecurity awareness and education programs to deal with human vulnerabilities since they are usually the lowest point in cybersecurity systems. Cybercrime can be lowered by increasing awareness among people on cyber risks, safe digital practices and reporting systems.

Lastly, it is advised that Pakistan should be an active collaborator and aligner towards the international standards of cybersecurity. International cooperation, embracing the best practices, and engaging in global cybersecurity efforts can improve the national response capacity to transnational cyber threats.

REFERENCES

Ahmed, S., Khan, M., & Ali, R. (2020). Cybersecurity challenges and digital risk management in Pakistan. *Journal of Information Security Studies, 12*(2), 45–62.

Akhtar, N., Ali, Z., & Hussain, T. (2023). Digital governance and cybersecurity readiness in developing economies. *International Journal of Cyber Policy, 8*(1), 78–94.

Ali, R., & Saeed, M. (2021). Regulatory frameworks for cybersecurity in Pakistan: An analytical review. *Pakistan Journal of Law and Technology, 5*(2), 101–118.

Bada, M., Sasse, M. A., & Nurse, J. R. (2019). Cybersecurity awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Carr, M. (2016). *US power and the internet in international relations: The irony of the information age*. Palgrave Macmillan.

Choucri, N., Clark, D., & Madnick, S. (2014). Cybersecurity policy and governance frameworks. *MIT Press*.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

Dunn Cavelty, M. (2014). *Cybersecurity and threat politics: US efforts to secure the information age*. Routledge.

European Union Agency for Cybersecurity (ENISA). (2019). *Cybersecurity policy framework report*. https://www.enisa.europa.eu

Government of Pakistan. (2002). *Electronic Transactions Ordinance (ETO) 2002*.

Government of Pakistan. (2016). *Prevention of Electronic Crimes Act (PECA) 2016*.

Han, J., Kamber, M., & Pei, J. (2012). *Data mining: Concepts and techniques* (3rd ed.). Morgan Kaufmann.

Hussain, T., Ahmed, S., & Raza, M. (2022). Trends and patterns of cybercrime in Pakistan. *Journal of Cybersecurity Research, 6*(1), 33–49.

Khan, M. A., & Raza, S. (2021). Digital security challenges in Pakistan: A governance perspective. *Asian Journal of Information Systems, 10*(2), 88–104.

Klimburg, A. (2017). *The darkening web: The war for cyberspace*. Penguin Press.

Kshetri, N. (2016). Cybersecurity in developing economies: Implications and challenges. *Computer, 49*(9), 74–78. https://doi.org/10.1109/MC.2016.276

Ministry of Information Technology and Telecommunication. (2021). *National Cyber Security Policy 2021*. Government of Pakistan.

National Institute of Standards and Technology (NIST). (2018). *Framework for improving critical infrastructure cybersecurity*. https://www.nist.gov

Rahman, A., & Iqbal, S. (2019). Cybercrime legislation in Pakistan: Challenges and prospects. *Pakistan Law Review, 11*(3), 55–70.

Scott, W. R. (2014). *Institutions and organizations: Ideas, interests, and identities* (4th ed.). SAGE Publications.

Shackelford, S. J. (2016). *Toward cyberpeace: Managing cybersecurity governance*. Cambridge University Press.

Shah, S., & Rehman, A. (2023). Public sector cybersecurity readiness in Pakistan. *Journal of Public Administration and Policy, 9*(1), 67–83.

Siddiqui, F., Khan, N., & Ali, H. (2024). Cybersecurity awareness and digital risk perception in Pakistan. *International Journal of Information Security Studies, 14*(2), 120–136.

Siemens, G., & Baker, R. S. (2012). Learning analytics and educational data mining: Towards communication and collaboration. *Proceedings of the 2nd International Conference on Learning Analytics and Knowledge*, 252–254. https://doi.org/10.1145/2330601.2330661

Slade, S., & Prinsloo, P. (2013). Learning analytics: Ethical issues and dilemmas. *American Behavioral Scientist, 57*(10), 1510–1529. https://doi.org/10.1177/0002764213479366

Tariq, H., & Malik, F. (2022). Implementation challenges of cybersecurity policies in Pakistan. *Journal of Policy and Governance, 7*(2), 91–108.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cybersecurity. *Computers & Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Zafar, M., & Qureshi, S. (2024). Evaluating Pakistan's National Cyber Security Policy 2021. *Journal of Cyber Policy, 5*(1), 1–15.