Journal of Public Policy Practitioners (JPPP)
Volume 5 Issue 1, Spring 2026
ISSN$_{(P)}$: 2959-2194, ISSN$_{(E)}$: 2959-2208
Homepage: https://journals.umt.edu.pk/index.php/jppp

Title:	**Cybersecurity Governance in Pakistan: Evaluating Public Sector Preparedness through International Telecommunication Union Global Cybersecurity Index**
Author (s):	Talat Ahmad Bhutta and Athar Rashid
Affiliation(s):	National University of Modern Languages, Islamabad, Pakistan
DOI:	https://doi.org/10.32350/jppp.51.03
History:	Received: March 18, 2026, Revised: April 23, 2026, Accepted: May 30, 2026, Published: June 25, 2026
Citation:	Bhutta, T. A., & Rashid, A. (2026). Cybersecurity governance in Pakistan: Evaluating public sector preparedness through international telecommunication union global cybersecurity index. *Journal of Public Policy Practitioners*, *5*(1), 54–87. https://doi.org/10.32350/jppp.51.03
Copyright:	© The Authors
Licensing:	This article is open access and is distributed under the terms of Creative Commons Attribution 4.0 International License
Conflict of Interest:	Author(s) declared no conflict of interest

A publication of
School of Governance and Society
University of Management and Technology, Lahore, Pakistan

Cybersecurity Governance in Pakistan: Evaluating Public Sector Preparedness through International Telecommunication Union Global Cybersecurity Index

Talat Ahmad Bhutta* and Athar Rashid

National University of Modern Languages, Islamabad, Pakistan

Abstract

Cybersecurity has emerged as a serious dimension of public sector governance in the digital age. The increased reliance on digital technologies for public service delivery has significantly expanded its exposure to cybersecurity risks. In Pakistan, rapid digital transformation has identified the need of robust and coherent cybersecurity framework to secure the cyberspace. In recent years, a series of legal, policy, and institutional reforms and initiatives have been introduced by the government to secure cyberspace. Despite these initiatives, the effectiveness and alignment of Pakistan's cybersecurity preparedness with globally-recognized benchmarks remain insufficient. Using the qualitative research methodology through analysis of academic literature, national, and international reports, the current study evaluated the cybersecurity preparedness for public sector organizations. The study addressed the research question, to what level Pakistan's cybersecurity preparedness is aligned with the five pillars, that is, legal, technical, organizational, capacity development, and international cooperation of Global Cybersecurity Index (GCI) of International Telecommunication Union (ITU). The findings identified that Pakistan has made progress in legal and organizational domains. However, key challenges and gaps remain in enforcement, technical workforce, and linkages with international organizations. The study concluded by proposing to align cybersecurity governance of public sector organizations with global best practices. It contributed to existing body of knowledge by mapping GCI with Pakistan's cybersecurity framework and provided policy recommendations for public sector organizations.

Keywords: cybersecurity, cybersecurity governance, cyber legislation, global cybersecurity index, public sector

*Corresponding Author: talat_ah@hotmail.com

Introduction

The growing reliance of public sector departments and organizations on digital services and technologies has inevitably increased the cybersecurity risks, particularly in least developed and developing countries (Shad, 2019). E-Governance platforms and interorganizational connectivity for communication, transparency, service delivery, and efficiency have increased dependency of public institutions on cyberspace. For public service delivery and government functions, proliferation of digital platforms has increased the cyber attach surface for those nations facing limited technical and institutional capabilities (Dutton et al., 2019). Public sector entities manage public personal data and critical infrastructure, have essential service obligations, and face unique cybersecurity vulnerabilities that can lead to data theft and unauthorized access. Digital transformation for public governance has increased tasks for government to manage information, deliver services, and to increase public trust in the system.

Sophisticated cyberattacks and emerging technologies have increased vulnerabilities for public sector organizations of Pakistan with limited resources and technical manpower. Cyber threats ranging from data breaches to ransomware attacks and disruption of critical infrastructures have increased globally. Developing countries, where legal frameworks, technical capabilities, and institutional capacity are still evolving, have faced more serious cyberthreats (Haque et al., 2023).

The Government of Pakistan (GOP) has aggressively embarked on digital transformation and internet penetration over the past decade (Sadat et al., 2025). The key objectives of Digital Pakistan Policy are to build holistic digital ecosystem with focus on innovation, increase IT exports, infrastructure development, increase investment in digital skills, and high-speed connectivity (Ministry of Information Technology and Telecommunication., 2018). The digital agenda of government include e-government services, online public services, digital taxation system, digital identity, and citizen portal (News Desk, 2020). This shift in service delivery has increased dependency on information and communication technology of different sectors including financial sector, telecom sector, transport sector, health sector, and public administration. However, this digital transformation has widened the cyber risks across autonomous bodies, departments, regulatory authorities, and ministries / divisions. Public sector initiatives have created new vulnerabilities and cyberattack opportunities

pertaining to critical infrastructure and government network system. New vulnerabilities include cybercrimes, disruption of services, state level aggression, and public trust in digital system (Dhirani, 2024).

Cybersecurity has been recognized as a national security issue in security policy of GOP. For the first time, the cyber domain has been included as one of the five threat domains which has given importance to cybersecurity (Ministry of Information Technology and Telecommunication, 2022; Virk, 2022). Pakistan has experienced threat spectrum including website defacement, financial frauds, information intrusions, and state-sponsored attacks in last few years (Qasim et al., 2025). To address technical and governance challenges of cybersecurity, the GOP has recognized the strategic importance of cyber legislations. Furthermore, it has enacted a series of cyber-related reforms which include substantive legislations, institutional creations, and strategic cyber policies. However, comprehensive cybersecurity preparedness to fulfil national needs of public sector institutions and global indices remains a priority. Cyber, legal, and institutional initiatives taken by government to secure the cyberspace, critical infrastructure, and public sector organizations, highlight the growing importance and acknowledgement of cybersecurity preparedness as a national security and governance issue (Ashraf et al., 2023).

Despite cybersecurity-related legal structures introduced by government, academic literature and existing scholarship in the domain of cybersecurity suggest that effectiveness and robustness of cybersecurity preparedness depend not on presence of laws, policies, and institutions but their practical implementations in letter and spirit and alignment with international best practices is required (Usmani, 2023). Literature has highlighted key themes including weak legal framework, shortage of skilled workforce, absence of centralized organization authority, and limited cooperation at national and international level. Global Cybersecurity Index (GCI) of International Telecommunication Union (ITU) provides a comprehensive analytical foundation to evaluate national cybersecurity maturity. GCI measures cybersecurity commitment of country across five interconnected pillars which include legal, technical, organizational, capacity development, and international cooperation (Rafiq, 2019).

Several studies have highlighted deficiencies, such as absence of specialized institutions, cybersecurity preparedness, and technical measures by applying GCI's five pillar model to Pakistan (Saleem et al., 2025).

Pakistan's overall score (96.69/100) in 5th edition of GCI 2024 has increased as compared to 4th edition of GCI 2021 (64.88/100). Moreover, the country has been listed in tier-1 role modelling nation having score between 95-100. Areas of relatively stronger achievements include legal, organizational, and capacity development measures where potential growth is required for technical and cooperation measure at different levels (International Telecommunication Union, 2020, 2024). Public sector organizations including regulatory bodies, ministries, service delivery institutions, and departments need to implement existing policies and laws to fill the gap of technical measures. Core challenges are fragmented, and overlapping mandates of institutions have limited technical manpower and capabilities. Slow implementation of policy directions and measures is another key challenge of public sector organizations (Bokhari, 2023). The current study focused to translate the GCI country level lens into public sector organization preparedness to provide operational cybersecurity model for agencies, ministries, departments, and autonomous bodies in order to assess risks and enhance preparedness. The study addressed the gap by analysing recent institutional evolution, cyber legislations, threat landscape, and implementation barriers and challenges.

Research Question

The current study aimed to answer the following question: At what level Pakistan's cybersecurity preparedness based on legal and institutional structure is aligned with five pillars legal, technical, organizational, capacity building, and international cooperation measures of GCI? (Ahmad, 2022; Bokhari, 2023; Dhirani, 2024; Khan, 2015; Saleem et al., 2025).

This study systematically explored the cybersecurity governance in Pakistan with a specific focus on preparedness of public sector organizations by adopting five pillars of GCI as analytical model. The introduction is followed by relevant literature review, which examined global, regional, and indigenous cybersecurity governance indices and approaches. Literature review discussed the GCI five pillar model by comparing its strengths and weaknesses with other models. The methodology outlines the data sources, research design, and approach used to evaluate the cybersecurity governance in Pakistan. Cybersecurity preparedness mechanism of public sector organizations is mapped on five pillars by emphasizing the recent initiatives in the domain of cybersecurity. The result section presents the findings where Pakistan stands across the

core pillars of GCI. Conclusion section concludes with policy recommendations to enhance cybersecurity governance at national level. Finally, the discussion section interprets the findings, identifies strengths, and areas to improve.

Literature Review

Cyber Threat Landscape in Pakistan

Cyber threat landscape being faced by Pakistan is multidimensional and transnational in nature which includes organized cybercrimes, cyberwarfare, financial frauds, information, and data stealing (Rehman & Ahmad, 2025). State institutions and public sector organizations have faced severe cyber-attacks, leading to disruptions of public service delivery. Financial and information losses from critical public infrastructure have challenged the public trust in digital transformation (Bhutta & Rashid, 2026). Different studies have documented that outdated systems, pirated software, lack of digital literacy, absence of incident response mechanism, interorganizational coordination, and limited cyber forensic facilities are key vulnerabilities and challenges to protect the cyberspace (Baig, 2023; Kausar, 2026; Nadeem et al., 2023). At public level, lack of cybersecurity awareness and training along with risky behaviours expand the cyber-attack surface. A recent study has explored that university students who excessively use digital devices and infrastructure often ignore security practices for personal digital devices and social media accounts (Khan et al., 2022). Weak socio-technical behaviours, awareness, and institutional gaps provide an environment of cyberattack (Saleem et al., 2025). Different studies have identified weaknesses in cybersecurity governance for public sector organizations and recommended to improve the cybersecurity profiles to counter the risks (Fatima, 2022). Recently, online payments and billing systems of Capital Development Authority (CDA) were hacked and disrupted the digital network. Hackers threatened to upload the citizen data on dark web (Abbasi, 2026). Such incidents highlight the importance of cybersecurity for public sector organizations to provide digital services.

Cybersecurity Policy and Institutional Response

In last few years, Pakistan has taken vital steps to build national cybersecurity mechanism in order to protect cyberspace. PECA 2016 is a basic cyber legislation which provides the foundation to address cybercrimes (Mirza & Akram, 2022). National Cybersecurity Policy 2021

defines the strategic objectives to secure cyberspace through organized and coordinated approaches (Kashan et al., 2023). Policy analysts, however, highlight that these policy instruments remained generic, fragmented, and insufficient due to weak implementation and execution mechanism. NCSP is very comprehensive and looks perfect in documents and discussion but it is necessary to implement it effectively in order to achieve the objectives (Masudi & Mustafa, 2023). The challenges to Pakistan's cyberspace include absence of data governance regulations, lack of indigenous information technology industry, insufficient resources, technical manpower, and dependency on foreign resources (Ahmad & Baig, 2024).

The prime objectives to be achieved through National Cybersecurity Policy include, cybersecurity preparedness for online privacy, security of critical information infrastructure, cyber threats information sharing, cybersecurity awareness, security operation centre, public private partnership, national and international cooperation, and collaboration in the domain of cybersecurity. These objectives are mandatory to produce skilled cybersecurity professionals as well as for the establishment of research and development activities in order to fulfil national requirements (Ali, 2022).

Five Pillar Model of International Telecommunication Union (ITU)

GCI of ITU is a benchmark to measure cybersecurity commitments of nations across five pillars. The index is used for self-assessments of countries in the domain of global coordination and good practices of other countries, to enhance cybersecurity measures at national level. Different studies have applied the GCI outlook to analyse and evaluate the cybersecurity preparedness profile. Furthermore, these studies have also suggested to align cybersecurity policy, institutional structure, and technical infrastructure in order to develop holistic cybersecurity ecosystem for public sector organizations (Pytlak & Siebens, 2024). The scope of GCI is primarily national, to rank the cybersecurity preparedness of a country. However, five pillars are implementable at public sector organizations and institutions to compare and analyse the sectoral and organizational cybersecurity preparedness (Haque et al., 2023). United Nations E-Government Development Index (EGDI) similarly measures the member states' progress to use information and communication technology on three pillars. These include online service delivery, telecom infrastructure, and development of human capital (United Nations, 2024). UN E-Government index shows the country readiness relative to one another. To address

cybersecurity issues and risk management in an organization, PRISM framework (Prioritize, Resource, Implement, Standardize, Monitor) is being used. This framework is used to achieve required objectives in order to assist top management. However, PRISM framework focuses to identify and provide tailored approach in order to mitigate risks through investment in organization. PRISM is criticized due to its inward and subjective approach while ignoring multi stakeholder, cooperation, and technical pillars as defined in GCI (Goel et al., 2020). AVARCIBER framework is another approach to identify and assess cyber risks based on relationships among five elements, such as assets, vulnerabilities, risks, threats, and countermeasures for public sector organizations. The framework is based on ISO 27005 and does not provide legal and cooperation controls as provided by GCI. Moreover, its focus is on internal models and processes. This is why, it is viewed as an operational risk framework (Rea-Guaman et al., 2020).

ITU cybersecurity model is multi-dimensional which is explicitly based on law, institutions, technical skills, and international engagement. ITU five pillars model recognizes that cybersecurity is not only the technical failure of organizations but a governance failure to protect infrastructure. United Nations EGDI, as compared to ITU index, is development centric, not security centric. Moreover, EGDI treats digital governance, whereas ITU treats risk governance. EGDI encourages digitization and benchmarking without security measures, which is a weakness as compared to ITU model. PRISM is based on multi-layered governance architecture, whereas ITU is based on institutional governance of law, policy, and cooperation. PRISM lacks policy and legal structure which are core in ITU model. Scope of AVARCIBER framework is limited to a region, whereas ITU is universal for each country. AVARCIBER framework focuses on regional policy, whereas ITU focuses on broad policy issue. ITU, EGDI, PRISM, and AVARCIBER frameworks are competing paradigms and not easily reconcilable. For instance, EGDI racking of a country may be higher due to increased digital exposure, however, lower in ITU ranking due to weak cybersecurity preparedness. ITU model operationalizes the cybersecurity governance through explicit integrations of law, institutions, cooperation, and skills. Countries can achieve development in five pillars of ITU simultaneously under state centric governance approach for international compliance.

Recent GCI 2024 of ITU has indicated that Pakistan's cyber readiness assessments have improved. However, establishment of technical bodies, organizational setups of cybersecurity, institutional technical capacity, and cooperation at both national and international level are weak areas which need further improvement (International Telecommunication Union, 2024). The major barriers to enforce cybersecurity laws and regulations include slow judicial process, sector specific cyber regulations, legal ambiguities, discriminations, and operational institutions (Bokhari, 2023).

Global cybersecurity outlook reports of World Economic Forum (WEF) have provided a detailed understanding of cyber risks landscape for organizations, particularly cyber capacity and technical resources disparities which are closely aligned with GCI of ITU. A detailed review of WEF reports has revealed the gaps in cybersecurity preparedness, especially with reference to public sector organizations, which is a central pillar and concern of GCI model. The 2022 report has mentioned the increase in cyberattacks across critical infrastructure of different organizations following rapid digital transformation observed due to COVID-19 pandemic. The key challenge identified in report included, cybersecurity capacity gaps between developed and developing economies, which reflects the technical and organizational measures of GCI (World Economic Forum, 2022). In 2023 report, disruption of global supply chain was identified as a major vulnerability due to state-sponsored attacks on organizations. This highlighted the importance of international cooperation and cyber response mechanism to achieve cybersecurity maturity (World Economic Forum, 2023). The concept of cyber inequity was introduced in 2024 report where large organizations enhanced the cyber capacity, while small organizations lagged behind. The report highlighted the importance of skilled workforce, policy implementation, and technical infrastructure for public institutions to achieve cybersecurity maturity (World Economic Forum, 2024). The 2025 report highlighted the cybersecurity weaknesses in public sector organizations, where 38% had insufficient cyber resilience and 49% lacked cybersecurity technical human resources (World Economic Forum, 2025). The 2026 report highlighted the impact of Artificial Intelligence (AI) on cybersecurity, where 23% public sector organizations had insufficient cyber resilience. Report stressed to enhance collaboration to counter cyber risks, which is an essential pillar of GCI (World Economic Forum, 2026). All five reports (2022-2026) have repeatedly identified the cybersecurity preparedness gaps in public and private sector organizations. These include

technical skills, financial resources, and investment in manpower. This aligns the WEF findings with ITU GCI assessments.

Existing literature discusses several issues related to cybercrime, cyber threat landscape, legal and policy implementations, and challenges. Moreover, literature has also discussed the GCI five pillars' high-level lens with reference to Pakistan. However, it has not been specified that how public sector organizations should implement the five pillars approach to prepare themselves against cyber risks. Different barriers, such as cybersecurity literacy, lack of technical expertise, institutional capacities, and coordination have been identified. However, limited public sector guidelines and preparedness have been discussed for security of infrastructure (Shahrose et al., 2024). This study articulated the cybersecurity preparedness for public sector organizations of Pakistan by mapping current legal and institutional structure with GCI five pillar model.

Methods

The current study was based on qualitative research methodology by the analysis of relevant literature in the domain of cybersecurity focused on legal, technical, organizational, capacity building, and international cooperation. Primary data sources were used to review literature including national cyber legislations, official documents published by Ministry of Information Technology and Telecommunication (MoITT), Pakistan Computer Emergency Response Team (PKCERT), Global Cybersecurity Index reports of ITU, and reports published by different national and international institutes and research centres in the domain of cybersecurity preparedness. Furthermore, other sources consulted for this study included peer reviewed national and international journals' articles. The cybersecurity preparedness for public sector organizations of Pakistan was evaluated through the synthesis of literature and mapping on ITU GCI. The study was limited to secondary data sources rather than empirical data, such as interviews or surveys from organizations. Moreover, cybersecurity preparedness of public sector organizations of Pakistan was analysed through GCI of ITU as primary assessment framework. The scope of study excluded private sector organizations, comparative analysis of different countries, technical assessment, and specific institutional implementation challenges.

Cybersecurity Preparedness for Public Sector Organizations

GCI-based metrics are being incorporated by member states into national cybersecurity activities and plans, which shows its applicability, acceptance, and quality. GCI results of every new edition highlight significant improvements achieved by countries in the domain of legislation, cyber incident response mechanism, development in national cyber plan, awareness and training for public at large, as well as engagement to work together at national and international level in order to counter cyber threats. The ITU GCI emphasizes that effectiveness of cybersecurity initiatives undertaken by member states targeting public sector institutions and organizations should be supported by a mechanism to measure the quality, impact and effectiveness. Such mechanisms facilitate countries to identify gaps, measure progress and to improve the overall cybersecurity posture.(International Telecommunication Union, *2024*). For public sector organizations, GCI five pillar model having clear objectives and components, has been mapped on the basis of themes identified through literature to enhance cybersecurity governance.

Pillar 1: Legal and Regulatory Measures

For legal and regulatory compliance, public sector organizations should operate within the boundary of National Cybersecurity Policy and laws. Obligations of cyber legislations for operationalization of everyday functions are compulsory for organizations and institutions.

Prevention of Electronic Crimes Act 2016 and Amendment 2025

PECA 2016 is a primary cybercrime legislation to combat cybercrimes, such as data breaches, identity theft, unauthorized access to electronic devices, and data (Prevention of Electronic Crimes Act, 2016). It criminalized the electronic fraud, cyber terrorism, and social media crimes by granting investigative power to law enforcement bodies (Abbas et al., 2021). Academic analyses label the PECA as reactive and an enforcement centric approach to achieve specific objectives of political elite (Mirza & Akram, 2022; Shah, 2024). To address evolving cyber threats and modern cybercrime challenges, necessary amendments have been introduced in 2025 (Prevention of Electronic Crimes Act, 2025). PECA amendments have expanded enforcement powers and modernized the different definitions as required to fill the legal gaps. Recent amendments have stirred a debate about digital rights and freedom of expression as guaranteed in constitution

of 1973. There is a need to balance civil liberties and security requirements in order to implement cyberlaws. Legal scholarships accept the amendments as a need towards cybersecurity legislation. However, there are concerns to safeguard fundamental rights and capacity of enforcement agencies (Zafar & Ali, 2025).

National Cyber Security Policy 2021

First National Cybersecurity Policy approved by Federal Cabinet provides policy guidelines of cybersecurity for incidence response mechanism, critical infrastructure protection, cyber governance guidelines, and cooperation at national and international level (Ministry of Information Technology and Telecommunication, 2021). Cybersecurity Policy outlines the data privacy, public awareness, and institutional mechanisms to secure the cyberspace of nation. Studies suggest that policy objectives and implementations have not been achieved and translated into reliable organizational practices across departments and ministries (Iqbal & Shan, 2024).

Computer Emergency Response Team Rules 2023 and Standards

To institutionalize the cyber incidents response, government has approved the CERT Rules 2023 under PECA 2016 and Cybersecurity Policy 2021. Under CERT Rules, hierarchy of PKCERT, Sectoral CERTs, Organizational CERTs, Government CERTs, and Provincial CERTs has been introduced to counter cyber incidents and manage their domain.

Despite these initiatives, academic literature has highlighted the absence of technical capacity and manpower to achieve the objectives. Peer reviewed studies on Cybersecurity Policy and legislation argue that these legal measures provide baseline. However, they are not sufficient to address emerging threats of AI and quantum computer attacks (Hussain & Bhatti, 2026). Cloud security and advance persistent vulnerabilities are other challenges which need to be addressed through laws (Bokhari, 2023).

Cybersecurity Act

To strengthen national cybersecurity posture and to protect critical infrastructure, government has decided to establish National Cybersecurity Authority (NCA) under Cybersecurity Act. The prime role of Cybersecurity Authority is to implement cybersecurity initiatives taken by Federal Government to secure the cyberspace (Ali, 2025). New authority would

increase compliance challenges for public sector organizations and departments to become more accountable to different law enforcement agencies (Desk, 2025). Critics argue that in the presence of PKCERT, CERT Council, and PTA, there is no need to establish another authority to shrink the digital spaces. New authority would overlap the operational functions which are already being performed by PKCERT (Mahmood, 2025).

Pillar 2: Technical Capabilities Measures

Technical capability and preparedness are central pillars of cybersecurity framework. To achieve national resilience, technical measures establish the backbone structure of national cybersecurity framework. Literature reveals that national technical capabilities in Pakistan are yet evolving due to uneven landscape.

Pakistan Computer Emergency Response Team and Incident Response Infrastructure

The establishment of PKCERT is a central shift to achieve technical capabilities measures. PKCERT plays a vital role in technical cybersecurity infrastructure because it is significant to enhance incident response capabilities. The mandate of PKCERT is to coordinate cyber incident, generate response, proactive threat detection, digital forensic, intelligence sharing, and capacity building across public and private sectors (Pirinen et al., 2026). Academic assessments highlight that formalization and operationalization of PKCERT represent a significant improvement aligned with technical pillars defined by ITU in the GCI (International Telecommunication Union, 2024). Structured mechanism of PKCERT to monitor incidents aligned with global best practices is a major achievement to address the noted gaps where Pakistan lacked behind previously.

Literature has identified call for further investments to establish Security Operation Centres (SOC) for the enhancement of security operations capabilities at different public sector organizations (Figueroa et al., 2025). Other challenges include lack of technical capacity for threat hunting, incident handling, harmonization of security controls and implementation of technical standards in government ministries, as well as departments and public sector organizations (Majeed et al., 2026).

Pakistan Security Standards (PSS) 2023

To protect information technology systems and for threat response, a strong technical standard framework at national level is required. The GOP has introduced cybersecurity standard with the name Pakistan Security Standards (PSS) for public and private sectors as a mandatory requirement. PSS framework is aligned with globally recognized benchmarks. Minimum security control, such as secure development, cryptography, hardware, and software compliance are foundational technical measures to be implemented by organizations. This gives national intent to regulate national technical measures and practices to align with international best practices. Studies have highlighted that actual compliance, implementation, and adoption are key challenges in public sector organizations, ministries, divisions, and regulatory bodies to achieve the real objective. Other difficulties include training gaps, lack of technical manpower, vendor readiness, and certifications (Ali, 2026).

Pakistan Information Security Framework (PISF) 2025

National CERT of Pakistan has released the Pakistan Information Security Framework (PISF) in 2025. This would provide the information security controls for all federal and provincial autonomous bodies, ministries, divisions, corporations, departments, and designated CERTs throughout the Pakistan. PISF provides a comprehensive list of controls for asset and risk management, communication protection, data protection, privacy, incident response, supply chain management, critical infrastructure, data centre, and web hosting for all organizations and departments. This framework is aligned with global best practices with an emphasis on risk-based governance framework having compliance-based approach to secure the cyberspace (National Cyber Emergency Response Team, 2025).

Critics argue that PISF would increase state control over cyber and digital space which, in turn, would lead towards censorship by restricting freedom of speech and expression. Moreover, mandatory controls would place financial and managerial burden on federal and provincial public organizations. Compliance deadline of June 2028 has further increased difficulties to hire technical experts, manage logistics, and to provide resources for implementation (Zayn, 2026).

Pillar 3: Organizational Strategy Measures

Organizational measures require coordination mechanisms of public sector organizations, departments, and institutes with a focus on clear mandate, structure, and authority. This measure demands to focus on cybersecurity governance structure in public and private sectors. Cybersecurity literature acknowledges the important evolution and development achieved by Pakistan for cybersecurity governance, although gaps still exist.

Institutional Architecture of Cybersecurity in Pakistan

Cybersecurity ecosystem of Pakistan includes multiple actors, such as Ministry of Information Technology and Telecommunication (MoITT), Pakistan Telecommunication Authority (PTA), National Telecommunication and Information Technology Security Board (NTISB), Pakistan Computer Emergency Response Team (PKCERT), and National Cyber Crime Investigation Agency (NCCIA). These actors have specific functions in Pakistan's cybersecurity ecosystem.

These government agencies collectively frame the organizational and institutional framework to implement the cybersecurity policy. This multi-institutional architecture reflects the complexity in cybersecurity governance. This is because challenges remain in clear mandate, resource allocation, coordination, and responsibility. Literature argues that unclear demarcation of authority of institutions and inadequate resources make it difficult to achieve effective cybersecurity governance in country (Shabbir & Adnan, 2025).

Table 1

Institutional Architecture of Cybersecurity in Pakistan and its Key Functions

S#	Name of Institution	Function of Institution
1	Ministry of Information Technology and Telecommunication (MoITT)	Primary function of MOITT is to derive the policy under the direction of Government
2	Pakistan Telecommunication Authority (PTA)	PTA is the regulator of telecommunication sector with prime responsibility to oversight the security of sector

S#	Name of Institution	Function of Institution
3	National Telecommunication and Information Technology Security Board (NTISB)	NTISB's mandate is to share cybersecurity advisory to government organizations
4	Pakistan Computer Emergency Response Team (PKCERT)	PKCERT is incident response body with a focus to share incidents with sectoral and organizational CERTs
5	National Cyber Crime Investigation Agency (NCCIA)	NCCIA is an investigation agency to investigate cybercrimes in country
6	National Centre for Cybersecurity (NCCS)	Function of NCCS is to secure cyberspace of Pakistan through training, education, research, and development
7	Pakistan Digital Authority (PDA)	Aims to transform Pakistan into digital society, economy, and governance

Strategic Leadership and Governance

Organizational measure highlights the importance of interagency harmonization and departmental cybersecurity committees for consistent command and control structure. Cohesive command and control frameworks are fundamental measures to achieve strong cybersecurity in public sector. National cybersecurity policy highlights the importance to bring public, private, and academic sectors on same page in order to achieve the policy objectives (Ministry of Information Technology and Telecommunication, 2021). Authors argue that mechanism to bring all stakeholders on board to operationalize the policy is yet not activated. Without interagency working groups, regular meetings, clear mandate, risk prioritization, and future paths, infrastructure protection would not be achieved (Azhar et al., 2025).

Organizational Challenges

Policy coherence and organizational internal culture play an important role to achieve effective cybersecurity governance (Willie, 2023). Many organizations have not established the dedicated cybersecurity wings to address the cyber risks. Cybersecurity is being treated as an information

technology problem in public sector institutions and departments. That is why, strategic importance of cybersecurity has not been accepted (Khan, 2025). Studies reveal that lack of technical manpower, cyber risk officers, inadequate budget allocation, effective communication, cybersecurity leadership role, and departmental cybersecurity policy are key challenges to achieve the cybersecurity governance (Gilbert & Gilbert, 2024).

Pillar 4: Capacity Development Measures

Capacity development measure is one of the most important pillars of GCI. To achieve resilient cybersecurity ecosystem awareness, skilled workforce and research networks are crucial requirements.

Human Resource Development and Capacity-building

Capacity-building and skilled human resources are most significant challenges in Pakistan to build reliable cybersecurity ecosystem. Studies have constantly highlighted the limited training opportunities, integration of cybersecurity education in civil service programs, shortage of cybersecurity professional in public sector organization, and public awareness program to counter cyberattacks (Irfan & Saeed, 2025; Triplett, 2022). Critical gaps in capacity development include:

- Insufficient collaboration for cybersecurity training to fill the gaps and needs of public sector organizations
- Limited cybersecurity curricula for schools and colleges
- Inadequate public awareness drives and campaigns for every segment of society
- Cybersecurity standardization challenges to be implemented across government departments and organizations

In 2018, the GOP established National Centre for Cybersecurity (NCCS) with a prime objective to develop research and development activities in universities to fulfil the cybersecurity requirements of public sector organizations. Other tasks assigned to NCCS include cybersecurity education program, literacy and technical manpower development through workshops, as well as trainings and seminars at different levels. NCCS played very important role to enhance cyber literacy, however, only one initiative was not enough to meet the demand. Demand and supply gap still exist in both public and private sector organizations and departments.

Research and Development

Cybersecurity research contributes to identify the challenges and difficulties in different sectors as well as key developments and opportunities to enhance cybersecurity ecosystem. For sustainable cybersecurity growth, researchers and academicians play an important role in policy-making and governance, which is missing in Pakistan as highlighted by different studies (Ahmad & Akhter, 2026; Gilbert & Gilbert, 2024; Javed, 2022). Analytical insights contributed by researchers through literature are disconnected in policy implementation phase (Kashan et al., 2023).

Public Awareness and Cultural Change

Academic literature and national cybersecurity policy have emphasized the need of regular cybersecurity drills and public awareness programs to enhance capacity of public sector institutions and departments. However, empirical research has highlighted this gap (Anwar & Yamin, 2021; Ministry of Information Technology and Telecommunication, 2021; World Economic Forum, 2025). From senior management to clerical staff, training and awareness plan of cybersecurity often lack as mentioned in official documents (Iftikhar et al., 2025). Cybersecurity awareness among decision-makers and public servants is a critical gap (Masudi & Mustafa, 2023). There is a need to change the inner culture of public sector organizations and institutions to achieve cybersecurity ecosystem (Osburn, 2025). Pakistan Information Security Association (PISA), a not-for-profit organization, has played a very important role to create cybersecurity awareness through workshops, seminars, conferences, and engagement with parliamentarians (Malik, 2018; Tufail, 2018; Tahir et al., 2019; Ahmad & Khan, 2022).

Academic and Industry Collaboration

Universities are offering different cybersecurity programs at bachelors and masters level, however, they are not aligning with practical needs of industry and organization due to lack of collaboration (Sendjaja et al., 2024). Requisite skillsets required for government departments and institutions include penetration testing, secure system design, incident response skills, security operation centre operations management, and coordination among sectors, which are largely not being taught at university level (Ball et al., 2025; Jumaan et al., 2025).

PKCERT has taken an initiative with Cyber Innovation Ecosystem (CIE) to connect academia, research institutes, private and public sector organizations, technology innovators, and government bodies to develop technical workforce, share threat intelligence, enhance cybersecurity solution, and drive innovation through partnership and collaboration (National Computer Emergency Response Team, n.d.). Academic collaboration plays an important role to strengthen cybersecurity for public sector organizations. Recently, University of Management and Technology (UMT), a private sector university has signed Memorandum of Understanding (MOU) with NCCIA for joint research project and development in the field of cybersecurity. Such collaboration plays an important role to expand training to fulfil future requirements (Staff Reporter, 2026).

Pillar 5: National and International Cooperation Measures

To enhance national cybersecurity resilience, international cooperation plays a vital role. International cooperation facilitates in information sharing, joint response mechanism, capacity development, and standardized practices to response transnational threats.

Global Cybersecurity Index (GCI) and Pakistan's Engagement

Pakistan has engaged with ITU and has improved ranking in Tier-1 category as a role model nation. Improvement in cybersecurity ranking reflects the global recognition of Pakistan's cybersecurity efforts aligned with global best practices (Associated Press of Pakistan, 2024). This improvement is across five pillars of GCI, particularly introduction of cybersecurity policy, establishment of national CERT, and legal framework.

Academic literature argues that GCI may be used as a diagnostic tool, however, this ranking does not reflect the operational effectiveness. Studies indicate that Pakistan's formal bilateral cybersecurity agreements and participation in international cybersecurity networks are limited. There is a need of deeper engagement at international level to enhance cybersecurity cooperation (Ahmad, 2022; Nadeem et al., 2023).

Bilateral and Multilateral Cyber Engagement

Bilateral and multilateral cooperation and treaties on cybercrime investigations are part of efforts to harmonize the cybersecurity norms at

global level. Pakistan supports the global framework against the cybercrime at UN level and is also engaged by affirming the applicability of International Humanitarian Law and UN Charter to cyberspace (Iqbal, 2025). Academic literature has highlighted that Pakistan has limited international cyber cooperation and engagement. However, government announcements and recent developments on diplomatic fronts have mentioned that engagements through treaties with international networks and forums are an ongoing process (Ali et al., 2022; Awais, 2025).

To enhance international cooperation, address criminal matters, and to combat cross border crimes, GOP has introduced Mutual Legal Assistance (MLA) Act 2020. MLA Act provides framework to prosecute and investigate transnational crimes through international cooperation.

Cross Border and Global Incident Response

To enhance international cooperation, it is essential to join international and regional cybersecurity information sharing, threat analysis, and cyber intelligence centres and forums. Pakistan being a founding member of "Organization of Islamic Cooperation - Computer Emergency Response Team" played an important role to establish links among Islamic countries in the domain of cybersecurity, which are needed to be enhanced further. Recently, PKCERT joined Asia Pacific - Computer Emergency Response Team and Forums of Incident Response of Security Teams, which is a major achievement to strengthen the cooperation at international level. Full membership of elite international network is a significant success to enhance national cyber resilience through globally-trusted partnership. Experts argue that Pakistan should engage with different international CERTs networks and other regional countries' CERTs to combat cyber-crimes and to share threat intelligence (Tufail, 2018). Such engagement would provide real-time awareness of threats, to take proactive defence measures for public sector organizations (Ali, 2022; Majeed et al., 2026).

Table 2

Mapping of GCI Pillars on Pakistan's Cybersecurity Framework

S#	ITU GCI Pillar Name	Analytical Focus	Key Gaps Identified	Pakistani Instruments
1	Legal Measures	Cyber Laws, Regulations	Generic Cyber Rules. Enforcement	Prevention of Electronic Crimes Act 2016.

S#	ITU GCI Pillar Name	Analytical Focus	Key Gaps Identified	Pakistani Instruments
			Constraints. Legal Ambiguity. Weak enforcement of cyber laws	Prevention of Electronic Crimes (Amendment) Act 2025. National Cyber Security Policy 2021. Computer Emergency Response Team Rules 2023.
2	Technical Measures	Computer Emergency Response Team, Framework, Standards	Weak technical standards and controls. Low cyber forensics readiness	Pakistan Computer Emergency Response Team and Incident Response Infrastructure. Pakistan Security Standard 2023. Pakistan Information Security Framework 2025.
3	Organizational Measures	Agencies, Institutions	Absence of centralized cyber agency. Fragmented mandates of different departments	Ministry of Information Technology and Telecommunication. Pakistan Telecommunication Authority. National Telecommunication and Information Technology Security Board. National Cyber Crime Investigation Agency. Pakistan Digital Authority.
4	Capacity Building	Awareness, Training, Education, Capacity Development	Low cyber literacy. A Shortage of technical experts. Weak	National Centre for Cyber Security. Pakistan Information Security Association. Cyber Innovation Ecosystem.

S#	ITU GCI Pillar Name	Analytical Focus	Key Gaps Identified	Pakistani Instruments
			cybersecurity training programs.	
5	International Cooperation	National and Global Engagement	Limited international cooperation. Lack of regional cybersecurity engagement.	International Telecommunication Union. Organization of Islamic Country-CERT. Mutual Legal Assistance Act. Asia Pacific - Computer Emergency Response Team. Forums of Incident Response of Security Teams

Results

Legal Alignment

Pakistan's legal framework is strongly aligned legal pillars of GCI through cybercrime legislations and amendments. Recent regulations have further strengthened the legal pillars, however, despite comprehensive legislation and policies, challenges persist on enforcement of law and availability of resources. Lack of technical capabilities and expertise in judicial institutions and investigation processes needs to be addressed through trainings, workshops, and awareness sessions.

Technical Preparedness

Establishment of PKCERT, mandatory security standards, and frameworks is a positive development to achieve technical measures for cybersecurity preparedness. However, training of manpower and financial resources are key challenges to achieve this objective. It has been identified that inconsistent framing of cybersecurity standards and frameworks in public sector organizations has undermined the operational and implementation effectiveness. Technical preparedness is partially aligned with the GCI's technical measures. National CERT has been established. However, operationalization of sectoral, organizational, and regulatory

CERTs is a key challenge.

Organizational Governance

For effective cybersecurity governance across government agencies, central and coordinated authority is required to achieve the objective of GCI's organizational pillars. Fragmented institutional structure, unclear responsibility matrix, and weak coordination mechanism need to be addressed to enhance organizational governance. Pakistan faces multiple challenges to achieve and align with GCI's organizational pillars due to fragmented and overlapping institutional mandates.

Capacity Constraints

Shortage of technical human capital is the most critical weakness of public sector organizations. To operationalize the technical and organizational measures of GCI pillars, cybersecurity education for different levels of public sector organizations is essential. Availability of skilled cybersecurity manpower in government institutions and departments is recommended across the board. Beyond skilled cybersecurity manpower, structured cybersecurity training programs, massive cybersecurity awareness drives, and industry-academia collaborations for trustworthy cybersecurity ecosystem are required.

Cooperation Expansion

It has been identified that regional and international cooperation is very important for effective national cybersecurity preparedness. In recent years, Pakistan has enhanced its engagement with different international cybersecurity forums, networks, and CERTs. This demonstrates partial alignment with GCI's cooperation pillar. Pakistan has limited cross border collaboration through cybersecurity treaties and agreements, which requires to be strengthened for national cybersecurity preparedness. Additional challenges include cooperation with foreign CERTs, participation in international cyber drills, as well as engagement with cyber threats intelligence and analysis centres to improve incident response mechanism and information exchange.

Discussion

Public sector organizations and agencies of Pakistan stand at the front line of cyber risk. The use of ITU GCI five pillars approach as a foundation, a tailor-made framework based on legal, technical, organizational, capacity-

building, and cooperative measures, has provided a mechanism for ministries, divisions, and departments to address cyberthreats. A measurable progress has been achieved by GOP by aligning its public sector cybersecurity preparedness with GCI. Furthermore, significant advancement has been achieved through the establishment of national cyber emergency response team, cyber legal reforms, cybersecurity awareness efforts, and alignment with global benchmarks. Research has consistently highlighted that merely cybersecurity laws, policies, and regulations are not enough. To secure the cyberspace, however, consistent implementation capacity, development of technical workforce, interorganizational engagement, public private partnerships, and deep international cooperation are equally important. To achieve resilient public sector cybersecurity preparedness in Pakistan, a tactical multi-stakeholder approach aligned with global best practices and frameworks is essential for cybersecurity governance. It is recommended to align the cybersecurity standards with critical infrastructure before implementing to avoid any difficulties. Moreover, each organ of state dealing with cybersecurity governance should have clear mandate to strengthen the cybersecurity for public sector organizations. It is need of time to restructure the government departments and Ministry of Information Technology and Telecommunication to align with global best practices. For future research, quantitative approach may be applied to validate the qualitative findings and to measure the cybersecurity governance of public sector organizations of Pakistan. Comparative studies of different organizations and with other countries using GCI can provide more valuable insights. Researchers may explore further by examining the impact of policies on private sector organizations and provincial level cybersecurity preparedness by using the ITU index.

Conclusion

In 21st century, cybersecurity governance has been recognized as a fundamental component of digital transformation and national security. The need of robust cybersecurity governance framework for public service delivery and protection of critical infrastructure has grown significantly for governments. The current study aimed to evaluate the Pakistan's cybersecurity preparedness aligned with GCI of ITU based on five pillars, that is, legal, technical, organizational, capacity development, and international cooperation. The use of internationally-recognized GCI as a comprehensive framework enabled an organised evaluation of

cybersecurity readiness of public sector organizations of Pakistan by exploring existing gaps, strengths, and weak areas requiring improvement. Significant challenges remain in coordination among government organizations, shortage of cybersecurity professionals, and limited technical resources. The findings identified that Pakistan has achieved progress in legal and organizational pillars. However, development of technical workforce, capacity-building, enforcement mechanism, and organizational hierarchy remain the key challenges to align the cybersecurity preparedness of public sector organizations with GCI. Findings indicated that notable progress has been achieved in developing and establishing cybersecurity ecosystem in recent years. This demonstrates the commitments of government to achieve the objectives. The evaluation suggested the effective implementation of national cybersecurity policy throughout the public sector organizations to secure the cyberspace. By aligning domestic cybersecurity governance practices with international best practices, Pakistan can build its own resilience cybersecurity ecosystem to enhance public confidence in digital governance. Findings may contribute to the knowledge of cybersecurity and provide significant insights for researchers, policy practitioners, and opinion makers to contribute further for effective cybersecurity governance system for public sector organizations of Pakistan.

Author Contribution

Talat Ahmad Bhutta: conceptualization, resource, investigation, methodology, writing – original draft. **Athar Rashid:** Supervision, writing-review & editing.

Conflict of Interest

The authors of the manuscript have no financial or non-financial conflict of interest in the subject matter or materials discussed in this manuscript.

Data Availability Statement

Data availability is not applicable as no new data was created.

Funding Details

No funding has been received for this research.

Generative AI Disclosure Statement

The authors did not use any type of generative artificial intelligence software for this research.

References

Abbas, M. U. R., Aamir, R., & Mahmood, N. (2021). Contemporary challenges of digital world and cybercrime and management solutions

in the light of Cyber Crime Bill 2016 of Pakistan and Islamic management perspective. *Indian Journal of Economics and Business*, *20(3)*, 1577–1594.

Abbasi, K. (2026, June 19). Hackers target Capital Development Authority's billing system, demand ransom in Bitcoin. *Dawn*. https://www.dawn.com/news/2008949

Ahmad, M. I., & Akhter, D. R. (2026). Aligning domestic cybersecurity laws with international best practices: Comparative lessons. *Pakistan Journal of Law, Analysis and Wisdom, 5(1)*, 125–140.

Ahmad, R. Z. ud din, & Baig, M. S. R. (2024). A controversial hypercritical examination of cybersecurity policies in Pakistan that cannot be ignored. *Global Strategic & Securities Studies Review*, *9(2)*, 43–54. https://doi.org/10.31703/gsssr.2024(IX-II).04

Ahmad, S. (2022). Cyber security threat and Pakistan's preparedness: An analysis of National Cyber Security Policy 2021. *Pakistan Journal of Humanities and Social Sciences Research, 5(1)*, 25–40. https://doi.org/10.37605/pjhssr.v5i1.381

Ahmad, S. B., & Khan, D. M. S. (2022). Cyber threat to Pakistan national security: National security and threat perception. *Pakistan Review of Social Sciences, 3(1)*, 1–12.

Ali, A. (2022). Cyber security policing: Analysing national cyber security policies of India and Pakistan. *Spotlight on Regional Affairs, 40(8)*, 1–4.

Ali, A., Khan, I., & Bashir, S. (2022). Need of international legislation regarding cybercrimes: Pakistan perspective. *Pakistan Journal of Social Research*, *4(2)*, 1136–1144. https://doi.org/10.52567/pjsr.v4i2.608

Ali, K. (2025, November 29). Cybersecurity Act essential to national security, says IT minister. *Dawn*. https://www.dawn.com/news/1958092

Ali, K. (2026, January 7). Experts identify gaps in national cyber security efforts. *Dawn*. https://www.dawn.com/news/1965503

Anwar, S. S., & Yamin, T. (2021). Civil military cooperation (CIMIC) in cyber security domain: Analyzing Pakistan's prospects. *Global Strategic & Securities Studies Review*, *6(1)*, 68–81.

https://doi.org/10.31703/gsssr.2021(VI-I).08

Ashraf, S., Mustafa, G., & Ali, G. (2023). Pakistan's National Security Policy: An analysis. *Annals of Human and Social Sciences, 4(3)*, 167–176. https://doi.org/10.35484/ahss.2023(4-III)16

Associated Press of Pakistan. (2024, September 13). Pakistan ranks among 46 top-tier countries in ITU Global Cybersecurity Index 2024. *The Express Tribune*. https://tribune.com.pk/story/2495974/pakistan-ranks-46-among-top-tier-countries-in-itu-global-cybersecurity-index-2024

Awais, F. (2025). Enhancing legal frameworks to address cybercrime in the digital age: A critical perspective. *UCP Journal of Law & Legal Education, 3(2)*, 56–82. https://doi.org/10.24312/ucp-jlle.03.02.533

Azhar, S., Ahmad, W., & Tahir, M. (2025). An exploratory analysis of the nexus between cybercrime and national security in Pakistan: Evaluating the existing legal framework, investigative challenges, and proposing a comprehensive strategy for effective cybercrime prevention and prosecution. *Journal for Current Sign, 3(2)*, 615–632.

Baig, Y. J. (2023). Implementation of cyber security in corporate sector of Pakistan. *International Journal of Advanced Engineering, Management and Science, 9(10)*, 27–33. https://doi.org/10.22161/ijaems.910.3

Ball, J., Lyons, M., & Evans, K. (2025). Bridging the cybersecurity skills gap: Aligning educational programs with industry needs. *Journal of the Colloquium for Information Systems Security Education, 12(1)*, 9–9. https://doi.org/10.53735/cisse.v12i1.196

Bhutta, T. A., & Rashid, A. (2026). Evaluating the cybersecurity framework of Pakistan: Challenges, gaps, and policy reforms. *University of Wah Journal of Social Sciences, 9(1)*, 1–25. https://doi.org/10.56220/uwjss.v9i1.315

Bokhari, S. A. A. (2023). A quantitative study on the factors influencing implementation of cybersecurity laws and regulations in Pakistan. *Social Sciences, 12*(11), Article e629. https://doi.org/10.3390/socsci12110629

Catalyic Security. (2025, November 7). *Pakistan's new cybersecurity mandate: Why the PSS framework matters now*. https://catalyicsecurity.com/pakistan-new-cybersecurity-mandate/

Desk, M. (2025, November 24). Govt moves to set up federal cybersecurity authority. *Profit by Pakistan Today*. https://profit.pakistantoday.com.pk/2025/11/24/govt-moves-to-set-up-federal-cybersecurity-authority/

Dhirani, L. L. (2024, January 8). *Data security, privacy and cyber policy of Pakistan: A closer look* [Paper presentation]. Proceedings of IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC), Tandojam, Pakistan. https://doi.org/10.1109/KHI-HTC60760.2024.10482125

Dutton, W. H., Creese, S., Shillair, R., & Bada, M. (2019). *Cybersecurity capacity: Does it matter? Journal of Information Policy, 9, 280–306*. https://doi.org/10.5325/jinfopoli.9.2019.0280

Fatima, I. (2022). A comparative analysis of the 2020 Global Cybersecurity Index scores of India and Pakistan. *Regional Studies*, *40(1)*, 39–60.

Figueroa, V., Sánchez Crespo, L. E., Santos-Olmo, A., Rosado, D. G., & Fernández-Medina, E. (2025). Building a holistic cybersecurity framework for e-government based on a systematic analysis of proposals. *International Journal of Information Security*, *24(3)*, 1–91. https://doi.org/10.1007/s10207-025-01024-0

Gilbert, C., & Gilbert, M. A. (2024). Organizational and leadership aspects of cybersecurity governance. *International Journal of Research Publication and Reviews*, *5(12)*, 1174–1191. https://doi.org/10.55248/gengpi.5.1224.3429

Goel, R., Kumar, A., & Haddow, J. (2020). PRISM: A strategic decision framework for cybersecurity risk assessment. *Information and Computer Security*, *28(4)*, 591–625. https://doi.org/10.1108/ICS-11-2018-0131

Government of Pakistan. (2022). *National Security Policy of Pakistan 2022–2026*. https://nsd.gov.pk/SiteImage/Downloads/NSP%20Policy%20(1).pdf

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

Hussain, T., & Bhatti, S. H. (2026). National security imperatives versus

data protection standards: A comparative evaluation of Pakistan and the European Union. *Pakistan Journal of Law, Analysis and Wisdom*, *5(2)*, 30–44.

Iftikhar, Dr. M., Batool, Dr. H., Asghar, Z., & Shabahat, S. (2025). Digital transformation in Pakistan: Cyber-security laws, digital media, and youth gig workers-assessing awareness, vulnerabilities, and economic impact (2024–2025). *Policy Research Journal, 3(10)*, 135–147. https://doi.org/10.5281/zenodo.17265151

International Telecommunication Union. (2020). *Global cybersecurity index 2020* (4th ed.). https://www.itu.int/epublications/publication/global-cybersecurity-index-2020

International Telecommunication Union. (2024). *Global cybersecurity index 2024* (5th ed.). International Telecommunication Union. https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

Iqbal, G. (2025, June 24). *How does international law byte into Pakistan's cyber governance?* Stimson Commentary. https://www.stimson.org/2025/how-does-international-law-byte-into-pakistans-cyber-governance/

Iqbal, Z., & Shan, R. us. (2024). Pakistan's cybersecurity landscape: Information and communications technology readiness, challenges and opportunities. *Journal of Strategic Studies*, *12(2)*, 105–131.

Irfan, S. M., & Saeed, D. N. (2025). A study of cybersecurity frameworks in organizations of Pakistan. *ACADEMIA International Journal for Social Sciences*, *4(4)*, 1803–1824. https://doi.org/10.63056/ACAD.004.04.1031

Javed, Z. (2022). The role of artificial intelligence in the enhancement of cyber security of Pakistan. *Journal of Contemporary Studies*, *10(2)*, 1–14. https://doi.org/10.54690/jcs.v10i2.188

Jumaan, S., Kuzminykh, I., Xiao, H., & Ghita, B. (2026). Understanding the skills gap between higher education and industry in cybersecurity. In P. Legg et al. (Eds.), *Advances in teaching and learning for cyber security education* (Lecture Notes in Networks and Systems, Vol. 1791). Springer.

Kashan, A. H., Mehmood, A., Khan, S. U. R., Aziz, T., & Orakzai, J. K. (2023). Implementation strategies of cybersecurity in Pakistan. *Khyber Journal of Public Policy*, *2(4)*, 183–217.

Kausar, S. (2026). The role of cyber policing in controlling dark web crimes in Pakistan. *Journal of Political Stability Archive*, *4(1)*, 120–137. https://doi.org/10.63468/jpsa.4.1.07

Khan, A. U. A. (2025). Cyber crime in Pakistan: Trends, challenges, and legal responses. *Advance Social Science Archive Journal*, *4(1)*, 1358–1366. https://doi.org/10.55966/assaj.2025.4.1.080

Khan, N. F., Ikram, N., Saleem, S., & Zafar, S. (2022). Cyber-security and risky behaviors in a developing country context: A Pakistani perspective. *Security Journal*, *36(2)*, 373–405. https://doi.org/10.1057/s41284-022-00343-4

Khan, Z. (2015). Strategizing cyber revolution within the domain of security studies. *Islamabad Policy Research Institute*, *15(2)*, 95–112. https://ipripak.org/wp-content/uploads/2015/10/5-art-s-15.pdf

Mahmood, F. (2025, December 8). *Will the new cybersecurity act strengthen defences, or create bureaucratic conflict? The Express Tribune*. https://tribune.com.pk/story/2581090/can-new-authority-resolve-cybersecurity-paradox

Majeed, Y., Majeed, A., & Minhas, M. T. (2026). Cybersecurity governance in the digital era and IT: Integrating regulatory oversight, risk management, and organisational resilience in Pakistan. *Social Science Review Archives*, *4(1)*, 1806–1829. https://doi.org/10.70670/sra.v4i1.1711

Malik, M. B. (2018). Architecture of cyberspace as an evolving security paradigm in South Asia: Pakistan-India cyber security strategy. *Regional Studies, 36(2)*, 3–35.

Masudi, J. A., & Mustafa, N. (2023). Cyber security and data privacy law in Pakistan: Protecting information and privacy in the digital age. *Pakistan Journal of International Affairs*, *6(3)*, 356–366. https://doi.org/10.52337/pjia.v6i3.906

Ministry of Information Technology and Telecommunication. (2018, February 7). *Digital Pakistan Policy*. Government of Pakistan. https://moitt.gov.pk/SiteImage/Misc/files/DIGITAL%20PAKISTAN%

20POLICY.pdf

Ministry of Information Technology and Telecommunication. (2021, July 27). *National Cyber Security Policy 2021*. Government of Pakistan. https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf

Mirza, M. N., & Akram, M. S. (2022). 3-Cs of cyberspace and Pakistan: Cybercrime, cyber-terrorism, and cyber warfare. *Strategic Studies, 42(1)*, 62–80. https://doi.org/10.53532/ss.042.01.00134

Mutual Legal Assistance (Criminal Matters) (Amendment) Act, Act No. XI of 2021 (2021). https://na.gov.pk/uploads/documents/1628576689_548.pdf

Mutual Legal Assistance (Criminal Matters) Act, Act No. XXII of 2020 (2020). https://na.gov.pk/uploads/documents/1597653825_608.pdf

Nadeem, M. A., Hashmi, S., & Khan, M. A. (2023). Exploring the interplay of cybersecurity and cybercrime in Pakistan's digital landscape. *Contemporary Issues in Social Sciences and Management Practices, 4(4)*, 207–222. https://doi.org/10.61503/cissmp.v2i4.94

National Computer Emergency Response Team. (n.d.). *Cyber innovation ecosystem (CIE).* Government of Pakistan. Retrieved July 29, 2026,https://pkcert.gov.pk/cie.asp

National Cyber Emergency Response Team. (2025). *Pakistan Information Security Framework 2025*. Government of Pakistan. https://pkcert.gov.pk/uploads/2025/11/PISF-Introduction.pdf

News Desk. (2020, April 23). *Digital Pakistan. The Digital Pakistan Policy: Vision and Execution*. Digital Pakistan. https://digitalpakistan.pk/the-digital-pakistan-policy-vision-and-execution/

Osburn, L. D. (2025). Telling stories about vendors: Narrative practices to negotiate risk and establish an organizational cybersecurity culture. *Journal of Cybersecurity*, *11*(1), Article etyae030. https://doi.org/10.1093/cybsec/tyae030

Pirinen, P., Perälä, P., & Lehto, M. (2026). Analysis of cybersecurity strategies across continents. *International Conference on Cyber Warfare and Security*, *21*(1), 668–675.

https://doi.org/10.34190/iccws.21.1.4418

Prevention of Electronic Crimes Act. (2016). *Act No. XL of 2016*. https://www.na.gov.pk/uploads/documents/1472635250_246.pdf

Prevention of Electronic Crimes Act. (2025). *Act No. II of 2025.* https://na.gov.pk/uploads/documents/679b243193585_457.pdf

Pytlak, A., & Siebens, J. (2024, January 8). *Advancing accountability in cyberspace: Models, mechanisms, and multistakeholder approaches (p*. 142). The Stimson Center. https://www.stimson.org/2024/advancing-accountability-in-cyberspace/

Qasim, M. S., Ahmad, Z., Maqsood, S., Zafar, S., & Azam, M. (2025). Assessing cybersecurity challenges and response readiness in Pakistan: A comprehensive analysis. *Kashf Journal of Multidisciplinary Research*, *2(1)*, 115–125. https://doi.org/10.71146/kjmr215

Rafiq, A. (2019). Challenges of securitising cyberspace in Pakistan. *Strategic Studies*, *39(1)*, 90–101. https://doi.org/10.53532/ss.039.01.00126

Rea-Guaman, A. M., Mejía, J., San Feliu, T., & Calvo-Manzano, J. A. (2020). AVARCIBER: A framework for assessing cybersecurity risks. *Cluster Computing*, *23(3)*, 1827–1843. https://doi.org/10.1007/s10586-019-03034-9

Rehman, H. M. J. U., & Ahmad, M. (2025). Responsibilities of concerned institutions to overcome cybercrime. *Advance Social Science Archive Journal*, *4(02)*, 2736–2747.

Sadat, A., Lawelai, H., Younus, M., & Nurmandi, A. (2025). Comparative analysis of National Cyber Security Index: A case study of Pakistan and Indonesia. *Kasetsart Journal of Social Sciences, 46*(1), Article e12. https://doi.org/10.34044/j.kjss.2025.46.1.01

Saleem, H. A. R., Bukhtiar, A., Zaheer, B., & Farooq, M. A. U. (2025). Challenges faced by the judiciary in implementing cybersecurity laws in Pakistan. *The Critical Review of Social Sciences Studies*, *3(1)*, 1052–1066. https://doi.org/10.59075/1wyx0v30

Sendjaja, T., Irwandi, Prastiawan, E., Suryani, Y., & Fatmawati, E. (2024). Cybersecurity in the digital age: Developing robust strategies to protect against evolving global digital threats and cyber-attacks. *International*

Journal of Science and Society, *6(1)*, 1008–1019. https://doi.org/10.54783/ijsoc.v6i1.1098

Shabbir, N., & Adnan, M. (2025). Cyber security: A growing challenge to Pakistan. *Annals of Human and Social Sciences*, *6(1)*, 372–384. https://doi.org/10.35484/ahss.2025(6-I)32

Shad, M. R. (2019). Cyber threat landscape and readiness challenge of Pakistan. *Strategic Studies, 39(1)*, 1–19. https://doi.org/10.53532/ss.039.01.00115

Shah, S. K. A. (2024). A critical analysis of efficacy of the Prevention of Electronic Crimes Act, 2016: Irritants and remedies. *Journal of Pakistan Administration*, *45(2)*, 66–91.

Shahrose, A., Zafar, Y., Khalid, H., & Khan, A. M. Y. (2024). A comprehensive analysis of Pakistan's cybersecurity landscape and its solutions. *Al-Qirtas*, *3(3)*, 73–80.

Staff Reporter. (2026, June 21). NCCIA signs MoU on cybersecurity. *Dawn*. https://www.dawn.com/news/2009554

Tahir, M., Farrukh, T., & Shahid, M. (2019). Cyber laws and cyber security in Pakistan: Myths and realities. *Global Social Sciences Review*, *4(1)*, 485–493. https://doi.org/10.31703/gssr.2019(IV-I).62

Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy*, *2(3)*, 573–586. https://doi.org/10.3390/jcp2030029

Tufail, T. (2018). *Comparing the national cyber security framework of Pakistan with India and United Kingdom* [Master thesis]. Tallinn University of Technology. https://digikogu.taltech.ee/en/Download/56aa279d-3c19-4610-b25d-a33defc6d149

United Nations. (2024). UN E-Government Survey 2024: Accelerating digital transformation for sustainable development (United Nations E-Government Surveys, p. 206). https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024

Usmani, M. A. (2023). Analyzing the key responsible factors: Cyber security in Pakistan. *Journal of Pakistan Administration, 44(2)*, 111–

122.

Virk, S. K. (2022). National internal security policy: An assessment. *Journal of Public Policy Practitioners*, *1(2)*, 49–78. https://doi.org/10.32350/jppp.12.03

Willie, M. M. (2023). The role of organizational culture in cybersecurity: Building a security-first culture. *Journal of Research, Innovation and Technologies*, *2*(4), 179–198. https://doi.org/10.57017/jorit.v2.2(4).05

World Economic Forum. (2022). *Global cybersecurity outlook 2022: Insight report*. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

World Economic Forum. (2023). *Global cybersecurity outlook 2023: Insight report*. https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

World Economic Forum. (2024). *Global cybersecurity outlook 2024: Insight report*. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

World Economic Forum. (2025). *Global cybersecurity outlook 2025: Insight report*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

World Economic Forum. (2026). *Global cybersecurity outlook 2026: Insight report*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

Zafar, P., & Ali, S. (2025). The PECA Amendment 2025: A critical analysis. Shaikh Ahmad Hassan School of Law. https://sahsol.lums.edu.pk/sites/default/files/2025-11/The%20PECA%20Amendment%202025%20A%20Critical%20Analysis.pdf

Zayn. (2026, January 24). *Govt seeks final feedback on Pakistan's new cybersecurity framework PISF 2025*. https://www.icci.pk/govt-seeks-final-feedback-on-pakistans-new-cybersecurity-framework-pisf-2025/