Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 4 No. 5 (May) (2026)

Pakistan's National Cyber Security Strategy: A Critical Analysis, Gap Assessment, and Recommendations for Strengthening Cyber Resilience

Arsalan Rajper
Department of Information Technology, Shaheed Benazir Bhutto University, Shaheed Benazirabad, Sindh, Pakistan. arslanrajper47@gmail.com

Mairaj Nabi
Department of Information Technology, Shaheed Benazir Bhutto University, Shaheed Benazirabad, Sindh, Pakistan. mairajbhatti@sbbusba.edu.pk

Baby Marina
Department of Information Technology, Shaheed Benazir Bhutto University, Shaheed Benazirabad, Sindh, Pakistan. marina@sbbusba.edu.pk

Rahila Parveen
Department of Law, Shaheed Zulfiqar Ali Bhutto University of Law, Karachi, Sindh, Pakistan. rahila.tallal@gmail.com

Maqsood Ahmed Dero
Department of Information Technology, Shaheed Benazir Bhutto University, Shaheed Benazirabad, Sindh, Pakistan. Maqsood.ahmed0717@gmail.com

Muhammad Asif Ali
Department of Information Technology, Shaheed Benazir Bhutto University, Shaheed Benazirabad, Sindh, Pakistan. asifjalbani458@gmail.com

Mah Saba Maheen
Department of Information Technology, Shaheed Benazir Bhutto University, Shaheed Benazirabad, Sindh, Pakistan. sabamaheen@sbbusba.edu.pk

ABSTRACT
From 2022 to 2025, there has been exponential growth in the rate of digital transformation in Pakistan. The increase in the rate of cyber threats experienced by critical national infrastructure, the financial sector, government portals and the civilian user base have grown at the same speed as the growth rate of digital transformation in Pakistan. The implementation of the National Cyber Security Policy (NCSP) in 2021 has not resolved the major structural, legislative and operational deficiencies Pakistan has in regards to its cyber defense posture. This research paper provides a comprehensive analysis of the cyber security strategy environment in Pakistan benchmarked against international best practices utilizing a comparative research design involving leading countries such as USA, UK, Germany, India, Malaysia, Turkey and Australia. The study adopts a mixed-method approach that includes systematic document analysis, gap assessment, and expert-informed evaluation to identify parameters and some critical deficiencies across ten key dimensions: legal foundations, governance structure, protection of critical infrastructure, incident response capabilities, public-private partnerships, cyber awareness, research and development, international cooperation, offensive cyber doctrine, and mechanisms for strategy reviews. The study indicated that although the NCSP 2021 has structural

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 4 No. 5 (May) (2026)

soundness with respect to intent, it is critically weak with regards to operationalization, funding, and legislative backing. This paper provides an actionable road map to policymakers, security practitioners, and legislators to increase significantly Pakistan's cyber resilience against modern threats and recommends a fully articulated list of prioritised recommendations across short, medium, and long timelines.

Keywords: National Cyber Security Strategy; Pakistan; Cyber Resilience; PECA 2016; Critical Infrastructure Protection; PKCERT; Cyber Policy; Gap Analysis

1. Introduction

The global landscape for cyber threats has changed dramatically over the last ten years. Various types of actors are increasingly capable of committing economic, political, and physical harm via the Internet. The militarization of cyberspace is a defining characteristic for modern conflicts and rivalries in the 21st Century, such as the SolarWinds supply chain compromise (2020), the Colonial Pipeline Ransomware Attack (2021), and repeated distributed denial-of-service (DDoS) attacks against Ukrainian critical infrastructure in 2022 (Smeets, 2022).

The Nation's citizenry are well aware of the rapid process of modernization. With a current population of over 230 million people, Pakistan is experiencing an increasing vulnerability due to changing conditions in the cyber threat landscape. Over the past few years, cyber events have noticeably risen within the country, including the 2023 breach of data at FBR (Federal Bureau of Revenue [FBR], 2024) as well as numerous breaches at various peripheral systems of NADRA (National Database and Registration Authority [NADRA]), ransomware attacks on hospitals and a national-scale financial crime via mobile banking systems (Pakistan Telecommunication Authority [PTA], 2023). From 2022 until 2024, over 100,000 cybercrime complaints were filed with the Federal Investigation Agency (FIA) through Complaints Against Cyber Crime Unit (CACC) (FIA, 2024). Compared to the prior two years there is an increase of approximately 47% over the previous two year period.

Pakistan introduced its first-ever complete National Cyber Security Policy (NCSP) in 2021 as a means to tackle these issues. This policy marks an important step forward for cyber governance in the country; nevertheless, the lack of implementation details, budget models, and failure to respond to emerging threats (such as those posed by artificial intelligence (AI), cloud services, and the Internet of Things (IoT) devices) has raised many concerns from experts and academics (Yousaf et al., 2023).

This research responds to these issues via a complete comparative and evaluative analysis. Through a detailed analysis of the Cyber Security Strategy of Pakistan 2021 (NCSP 2021), the author provides a systematic evaluation of the national Cyber Security Strategies (NCSSs) of seven countries, selected based on geographic diversity, progress level, and cyber maturity. In evaluating NCSP 2021 against the NCSSs of these seven countries, there are significant deficiencies in NCSP 2021 as identified by 10 criteria. Based on the deficiencies identified in NCSP 2021, the author provides tailored recommendations for Pakistan's socio-political, economic and technical contexts.

1.1 Research Objectives

The primary objectives of this research are:

- To evaluate Pakistan’s NCSP 2021’s content and structure against a set of evaluation metrics.
- Benchmark Pakistan’s cyber security posture against seven comparator nations.

ISSN Online: 3007-3154
ISSN Print: 3007-3146

- To find out and quantify the gaps in Pakistan's cyber security strategy on ten major dimensions.
- To provide a prioritized and actionable set of recommendations to strengthen the national cyber resilience of Pakistan.

1.2 Novelty of the Research

No previously published systematic multi-dimensional gap analysis that employs an established evaluation framework exists, which compares the NCSP 2021, to any comparable set of international strategies by the authors' knowledge, therefore, the authors are conducting what can be considered a completely original piece of research in this area. The novelty of this research lies in: (a) The use of a new and expanded ten-parameter evaluation framework based on the NCSS evaluation methodology developed by ENISA; (b) The inclusion of up to date (i.e. 2022-2025) threat intelligence data relevant to Pakistan; and, (c) The development of institutionally contextually relevant, and time-sensitive recommendations based upon Pakistan's limited institutional capacity.

2. Problem Statement

Pakistan is increasingly reliant on digital technologies for governance, economy, health services and national security; however its cybersecurity governance system is falling well short of the rapidly growing threat landscape. The NCSP of 2021 is a positive initial strategic document, but it has several significant weaknesses. There is no legally binding enforcement mechanism, essential infrastructure is not categorized with statutory protection and an offensive cyber philosophy is not articulated. Additionally, there is no periodic review process. These weaknesses create significant vulnerability in Pakistan's cyberspace, and hence its national security and economic stability.

Moreover, Pakistan is among the few key regional states which have not ratified the Budapest Convention on Cybercrime; thus hampering its ability to institutionalize international cooperation in law enforcement. The main legislative framework that governs cyber activity in Pakistan is the Prevention of Electronic Crimes Act (PECA) of 2016. There have been no substantial amendments to PECA regarding issues of cloud computing, AI-derived threats, deepfake technology, or the protection of critical infrastructure. Due to the lack of a formal public-private partnership (PPP) framework, the private sector, which is responsible for a large percentage of all digital infrastructure in Pakistan, has been excluded from the overall national cyber defence structure.

This article seeks to provide answers to the central question of this research: What are the critical weaknesses found within the Pakistani national cyber security policy, and what evidence-based measures should be taken to solve these weaknesses?

3. Literature Review

Over the last 10 years, there has been an increase in the number of academic articles concerning the national cyber security policies of different nations. Analyses done to compare national cyber security frameworks across countries include preliminary assessments of their individual national cyber security measures to determine each country's cyber security framework in terms of their legal standing, technological capabilities, and organizational structures (Dunn Cavelty, 2014; Klimburg, 2012). The latest research has shown that developing countries do not have the same level of capacity as industrialized countries and this difference has been taken into consideration when evaluating the effectiveness of NCSS (Tschider, 2023).

3.1 Global NCSS Comparative Research

Shafqat and Masood (2016) executed a substantial comparative analysis which consisted of twenty nation wide cyber security schemes within the first twenty-four hours of the commencement of their research and defined a standard for future research. They assessed

ISSN Online: 3007-3154
ISSN Print: 3007-3146

these strategies on a basis of their timeframes; aims; definitions of crucial terminology; threat classification; organisational structure; key infrastructure; incident response; legislative actions; building capabilities; and collaboration. Their approach is the methodological base that will be used by this study. The authors found that although the overall objective of each strategy was the same there are considerable differences regarding the implementation of these strategies, the level of legislative support afforded by law enforcement agencies, and the stance toward the use of offensive measures. According to Bada et al. (2019), studying twelve different national cybersecurity awareness programs worldwide, they found that educational programs integrated into formal sponsored classroom settings were more successful in creating long-lasting change (raising awareness) compared to those that operated independently of established programs. This is very important in relation to Pakistan, whose digital literacy poses a considerable threat to its citizens.

Smeets (2022) looked at how countries have developed their offensive cyber warfare capabilities over time and how each of these countries (i.e., The United States, United Kingdom, Netherlands, and Australia) have increasingly acknowledged and accepted the use of offensive cyber warfare as part of their overall national strategy on cyber deterrence. The results of this analysis also provide insight into Pakistan's strategic uncertainty relating to offensive cyber warfare and potentially undermining its own cyber deterrent capability.

3.2 Pakistan-Specific Cyber Security Research

The literature on Pakistan’s cyber-securities is sparse and insufficient. For example; Yousaf, Khan, and Rehman (2023) assess the PECA 2016 legislation in relation to modern-day cybercrime; they determine that its jurisdictional rules, evidence requirements, and definitions of crime do not provide sufficient support to charge persons with complex cyber-offences. They propose an independent Cyber-Security Act based on the United Kingdom’s Network and Information Systems (NIS) Regulations.

Ahmad and Qayyum (2024) investigate the operational effectiveness (effectiveness of operations) of Pakistan’s national Computer Emergency Response Team (PKCERT) and identify (identify) severe operational deficiencies in regard to personnel, technological resources, and collaboration between agencies. They reveal that there is no official mandate for PKCERT to cooperate with provincial law enforcement or commercial sector CERTs; lack of this mandate diminishes the capability of PKCERT to respond effectively to cyber-incident(s).

A 47% increase in online cybercrime was reported by the PTA for 2024 in its Annual Report on Cyber Crime and Internet Security. The criminal activity was mainly phishing, account compromise, and internet financial theft. The report identified new and growing threats, such as AI-assisted social engineering and deepfake-based fraud, which have not yet led to any clear legislative or technical countermeasures in Pakistan.

3.3 Regional Comparisons

The most relevant benchmark for Pakistan's direction is the National Cyber Security Strategy (NCSS) of India. The Indian National Cyber Security Policy introduced in 2013 has put into place a multi-tier cyber governance structure that includes CERT-In, the National Critical Information Infrastructure Protection Centre (NCIIPC) and the Cyber Swachhta Kendra (botnet cleaning centre). According to Sharma and Gupta (2023), India has improved its ranking on the ITU Global Cybersecurity Index through the sector-specific character of the CERT organisations and mandatory incident reporting mechanisms. An important example for the legislative reform plan of Pakistan is the Cyber Security Act in Malaysia, which was enacted in 2024 and requires cybersecurity for the national critical information infrastructure (MCMC, 2024).

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 4 No. 5 (May) (2026)

4. Methodology

The current study employs a mixed methods research design that combines qualitative document analysis with a structured quantitative gap-scoring framework.

4.1 Document Analysis

The major sources used for this analysis were NCSP (2021) document from Pakistan; PECA (2016) document; PTA annual report (2022, 2023, 2024); and FIA cybercrime statistics. The Government of Pakistan requested access to the comparatives of other countries' cyber security documents including the USA (2023); United Kingdom (UK) (2022) Germany (2021); India (2013/updated 2020); Malaysia (2020); Turkey (2016-2019); and Australia (2023-2030).

4.2 Evaluation Framework

We designed a new method for analyzing cyber security based on ENISA's evaluation of national strategies for creating a secure cyber environment, known as the ENISA National Cyber Security Strategies Evaluation Methodology, developed by Liveri & Sarri (2014). We've now revised this methodology to incorporate contemporary threats and governance standards. This new methodology contains ten main elements: (1) legal/legislative framework; (2) organizational structure and lead authority; (3) critical infrastructure protection; (4) incident response capability (CERT/CSIRT); (5) threat characterization and intelligence; (6) public-private partnership; (7) cyber awareness and capacity building; (8) research and development; (9) international cooperation; (10) mechanism for strategy review and updating.

4.3 Gap Scoring

Ten different factors were used to evaluate the country plans, with each of these factors being evaluated on a three-point scale: 2 = completely addressed, 1 = partially addressed, and 0 = Not addressed at all. The ratings of Pakistan for each of the ten characteristics were paired to the average ratings of the seven comparison countries to get a Gap Index for each characteristic. After determining the Gap with Comparison Countries, the proposals for improvement were prioritized based on the numerical difference in the Gap between Pakistan and the comparison countries.

4.4 Threat Landscape Analysis

The cyber threat landscape of Pakistan is defined by using information from the Pakistan Telecommunication Authority (PTA) (2024), the Federal Investigation Agency (FIA) (2024), and threat intelligence reports produced by Kaspersky Lab (2023) and Check Point Research (2024) related to Pakistan and South Asia. This contextualization ensures that the gap analysis and recommendations are based on Pakistan's specific threat landscape rather than on general global trends.

5. Analysis and Results

5.1 Pakistan's Cyber Threat Landscape (2022–2025)

According to government records and threat assessments from around the world, table one identifies the main types of cyber risks that threaten Pakistan. The highest volume of reported cases are:- financial fraud, and phishing scams. The most serious risk with the potential for national impact, is state-sponsored attacks on critical infrastructure.

Table 1: Pakistan Cyber Threat Landscape (2022–2025)

Threat Category	Description	Severity / Prevalence in Pakistan
Cyber Crimes	Financial fraud, phishing, identity theft, online harassment	High - FIA reported 100,000+ complaints (2022–2024)

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 4 No. 5 (May) (2026)

Threat Category	Description	Severity / Prevalence in Pakistan
State-Sponsored Attacks	APT groups targeting government, military & critical infrastructure	Very High - multiple incidents on OGDCL, NADRA portals
Ransomware	Encryption of critical data demanding ransom	Rising - healthcare & banking sectors most affected
Disinformation / FIMI	Foreign information manipulation & interference via social media	High - election-related campaigns 2023–2024
Insider Threats	Unauthorized data access by internal actors	Moderate - documented in banking sector
IoT / SCADA Attacks	Attacks on industrial control systems & smart devices	Emerging - energy sector at risk
Data Breaches	Theft of PII from government & private databases	High - FBR & BISP data leaks reported (2023)

Note. Data compiled from PTA (2024), FIA (2024), Kaspersky Lab (2023), and Check Point Research (2024).

5.2 Comparative Analysis: Pakistan vs. Peer Nations

Table 2 Comparison of Pakistan's Cyber Security Strategy with Six Comparator Nations Across Six Key Dimensions. Pakistan has established a CERT and a foundational legislative framework; however, it lags behind other countries in developing formal public/private partnerships, creating a defined offensive cyber capability, and developing a formalized review process for its cyber security strategies.

Table 2: Comparison of Pakistan's Cyber Security Strategy vs. Regional and Global Peers

Country	NCSS Published	Dedicated CERT	Legal Framework	PPP Framework	Offensive Capacity	Review Mechanism
Pakistan	2021	Yes (PKCERT)	PECA 2016	Partial	Not Disclosed	Ad hoc
India	2013	Yes (CERT-In)	IT Act 2000	Yes	Yes (NCIIPC)	Annual
Malaysia	2020	Yes (MyCERT)	Cyber Security Act 2024	Yes	Yes	Biannual
Turkey	2016	Yes	Law No.	Yes	Yes	Annual

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 4 No. 5 (May) (2026)

Country	NCSS Published	Dedicated CERT	Legal Framework	PPP Framework	Offensive Capacity	Review Mechanism
		(USOM)	5651			
USA	2023	Yes (CISA)	CFAA + NIS	Yes	Yes	Frequent
UK	2022	Yes (NCSC)	Computer Misuse Act	Yes	Yes	Annual

Note. Sources: Official NCSS documents for each country; ITU Global Cybersecurity Index 2024.

5.3 Critical Sectors and Infrastructure Vulnerabilities

In Pakistan, without any formal legislation addressing the identification of critical infrastructure (CII), the protection of key industries relies on either informal ministerial guidance or each organisation's established process. Table 3 outlines the critical infrastructure sectors in Pakistan and their respective digital assets, as well as potential cyber threats to these sectors. Of all critical industries in Pakistan, the energy sector (particularly the OGDCL operational technology networks and the WAPDA SCADA systems) poses the greatest level of threat of a cyber-physical attack resulting in real-world consequences.

Table 3: Pakistan's Critical Sectors and Associated Cyber Vulnerabilities

Critical Sector	Key Assets	Primary Cyber Risks
Banking & Finance	SBP-regulated institutions, fintech platforms	Account takeovers, ransomware, insider fraud
Telecommunications	PTCL, Jazz, Telenor, Zong infrastructure	Interception, SS7 attacks, DNS hijacking
Energy & Utilities	WAPDA, OGDCL, gas pipeline SCADA systems	ICS/SCADA attacks, ransomware on OT networks
Government E-Services	NADRA, FBR, SECP digital portals	Data breaches, DDoS, credential stuffing
Healthcare	Hospital management systems, NHIS data	Ransomware, patient data theft
Transportation & Logistics	Air traffic, PRAL customs, port systems	System disruption, cargo fraud
Education	HEC portal, university systems	Data theft, ransomware on academic records
Water & Agriculture	Irrigation SCADA, food supply chains	Emerging IoT threats

Note. Vulnerability assessments informed by PTA (2024), PKCERT advisories (2023-

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 4 No. 5 (May) (2026)

2024), and sector-specific risk literature.

5.4 Gap Analysis: Pakistan's NCSP 2021 vs. International Best Practices

In Table 4, a ten-parameter gap analysis assesses Pakistan's existing condition as compared with global best practices. Eight of the ten parameters are rated as having a high gap indicating that there is limited or no movement towards implementing them. Only two of the ten parameters are rated as having a moderate gap which means that they have been established but are still very basic to Pakistan's level of progress.

Table 4: Gap Analysis - Pakistan's NCSP 2021 vs. International Best Practices

Parameter	Pakistan Status	Best Practice	Gap Level
Clear Key-Term Definitions	Partially defined	Fully defined (ISO/ITU aligned)	Moderate - lacking cyberspace definition
Offensive Cyber Capability	Not explicitly stated	Explicitly declared (UK, USA, Germany)	High - ambiguity in cyber posture
Critical Infrastructure List	General mention	Sector-specific with legal protection	High - no legal CI designation
CERT Mandate & Funding	PKCERT exists but underfunded	Fully mandated with dedicated budget	High - operational gaps
Review & Update Cycle	No fixed cycle	Annual or biannual (Netherlands, Austria)	High - strategy already outdated
Public-Private Partnership	Mentioned conceptually	Formalized with MOUs & frameworks	Moderate - framework lacking
Cyber Awareness Programs	Limited outreach	National campaigns (UK's Cyber Aware)	High - low digital literacy
R&D Investment	Minimal allocation	Dedicated R&D bodies & funding	High - no indigenous capability
International Cooperation	Bilateral MoUs only	Multilateral frameworks (Budapest Conv.)	High - not party to Budapest Convention
Legislative Framework	PECA 2016 (outdated)	Regularly updated cyber law	High - cloud, AI, IoT not addressed

Note. Gap levels: High = critical structural absence requiring immediate attention; Moderate = partial implementation requiring strengthening.

6. Discussion

This research project presents an extensive evaluation of the cybersecurity situation in Pakistan. There is an actual political commitment and level of institutional development; however, there are shortcomings at the legislative level, financial constraints, and challenges regarding interoperability associated with NCSP 2021 performance.

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 4 No. 5 (May) (2026)

6.1 Legislative Deficit

The most significant structural issue discovered is the lack of a full and independent Cyber Security Act. However, while PECA 2016 was revolutionary legislation upon its original enactment, it was largely developed to handle individual instances of cybercrime and to deal with crimes related to the expression of ideas through digital media. PECA 2016 does not provide any framework for critical infrastructure protection, no mandatory breach reporting, and no basic security requirements for key service providers. By contrast, Malaysia's Cyber Security Act 2024 mandates that all operators of Critical Information Infrastructure provide security that can be enforced, and that they notify the national Computer Emergency Response Team of any incidents within an agreed-to time period (MCMC, 2024). Thus far, no legal framework has been in place that would support the enforcement of advanced cyber defense measures against businesses in Pakistan, which means that businesses in Pakistan have no obligation to abide by the standards for security as provided by the government, and thus could not have implemented any of those advanced cyber defense measures even if they had wanted to.

6.2 Institutional Fragmentation

Pakistan's cyber security governance structure is fragmented at the institutional level. Authority for cyber security in Pakistan is split between the MoITT, PTA, FIA's Cyber Crime Wing, PKCERT and military cyber commands assigned to defence operations. The absence of a single cross-Government entity with the authority to manage national cyber security stands in stark contrast to Estonia's centralized information systems authority (RIA) or France's ANSSI. This fragmentation will continue to hinder effective coordination, result in duplicated efforts and facilitate inter-agency information-sharing fallibilities that can be exploited by hostile actors (Ahmad and Qayyum; 2024).

6.3 The Public-Private Partnership Imperative

In Pakistan, most of the nation's digital infrastructure including telephone systems, banking operations, using the internet (cloud), and internet marketplaces (e-commerce) are owned and operated by private companies. As such, effective national cyber security depends on substantial cooperation with the business sector; however, the NCSP 2021 does not contain an operational structure or process for sharing information or any legal framework for cooperation between government and the private sector in relation to hacking incidents. This stands in stark contrast with how things are done in the UK; there, businesses use the UK Cyber Information Sharing Partnership (CiSP), which is a real time, dependable way for the government and the private sector to share intelligence on threats.

6.4 The Awareness and Capacity Crisis

There are two primary issues facing Pakistan: first 130 million people expected to be internet users by 2025; also very low levels of digital literacy and awareness of basic measures for ensuring safe online usage of technology. The NTISB and PKCERT provide regular advisories; however, there is no coordinated national cyber awareness program providing continuous education. As discussed by Bada et al (2019), episodic intervention-type awareness programs result in little long term behaviour modification vs long term campaigns delivered as part of formal education which have much more impact. Because cyber security has not yet been made a requirement by HEC in all undergraduate courses, this increases the skills shortage of both PKCERT and the national SOC.

7. Recommendations

Nine priority recommendations are listed in Table 5 and were developed using gap analysis and comparison. Each recommendation corresponds to the time allocated for implementing the recommendation. The recommendation is designed to help each other; short-term legislative changes create an environment for medium-term institutional and

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 4 No. 5 (May) (2026)

PPP initiatives to develop capabilities, which allows for long-term development of capabilities and integration into the global market.

Table 5: Prioritized Recommendations for Strengthening Pakistan's Cyber Security Strategy

Recommendation	Description	Timeline
Comprehensive Legal Reform	Enact a dedicated Cyber Security Act; update PECA 2016 to address AI, cloud, IoT and data privacy	Short-term (1-2 years)
Formalize Critical Infrastructure Protection	Legally designate and protect CI sectors; mandate security baselines and audits	Short-term (1-2 years)
Strengthen PKCERT	Increase budget, mandate, and sectoral CERTs; establish 24/7 SOC capability	Short-term (1-2 years)
Establish Offensive Cyber Doctrine	Define Pakistan's cyber posture — deterrence, rules of engagement, and escalation thresholds	Medium-term (2-4 years)
Formalize PPP Framework	Institutionalize government-industry collaboration through legally binding framework with shared threat intel	Medium-term (2-4 years)
National Cyber Awareness Campaign	Launch a sustained national campaign modeled on UK's Cyber Aware; integrate into HEC curricula	Medium-term (2-4 years)
Invest in Indigenous R&D	Establish a National Cyber Security R&D Fund; incentivize domestic security product development	Long-term (4-6 years)
Multilateral Engagement	Accede to the Budapest Convention; join ITU GCA programs; enhance SAARC cyber cooperation	Long-term (4-6 years)
Biannual NCSS Review Cycle	Institutionalize a review and update mechanism with multi-stakeholder input every two years	Ongoing

Note. Timelines are indicative and subject to political will, resource availability, and institutional capacity.

8. Conclusion

An in-depth evaluation comparing Pakistan's NCSP 2021 with NCSPs of seven similarly situated countries across ten relevant dimensions is presented in this report. The assessment findings indicate an important foundation created by the NCSP 2021 through establishing PKCERT. However, a vast and meaningful split exists between the original intentions of the NCSP 2021 and the actual operations of cybersecurity execution for Pakistan.

Eight priority deficiencies in the areas of legislative reform, protection of critical infrastructure, offensive cyberspace doctrinal development, capacity of the Computer

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 4 No. 5 (May) (2026)

Security Incident Response Teams (CSIRTs), public-private partnerships, cybersecurity awareness, research and development investment, and international cooperation create a collective and significant strategic vulnerability that adversaries can readily exploit. Additionally, the reluctance of Pakistan to join the Budapest Convention, the absence of a formal designation procedure for Critical Information Infrastructure (CII), and the shortfall of funding of PKCERT are non-oversight deficiencies in the organizational administration of Pakistan's cybersecurity capacity and represent systemic flaws in protecting Pakistan's national interests in the cyberspace environment. These recommendations are based on comparative data and take into account institutional and resource constraints in Pakistan. They do not assume that the country will adopt developed countries' cyber security frameworks right away, but rather propose a practical, gradual strategy for building a much-improved national cyber posture. The need for this goal is imperative because as Pakistan's digital economy grows and its critical infrastructure becomes increasingly dependent on cyberspace, the price of strategic inaction will continue to rise.

9. Future Work

The strategic and policy-related aspects of Pakistan's Cyber-safety Framework are investigated in this paper. Future research will look at additional aspects of this analysis. An empirical quantitative analysis of actual cyber events using classified government data (which is not available to academic researchers), could provide a more accurate assessment of the strategic inadequacies identified in this paper. The experiences of PKCERT practitioners, Chief Information Security Officers in banks, and government IT officials would provide some practical insights into implementation barriers that are not discussed in policy documents. A focused exploration of the potential impacts of future technologies such as Artificial Intelligence (AI), 5th Generation (5G) technology, the use of "cloud-first" systems by the government, and Financial Technology (Fintech) on cybersecurity would be timely and relevant to the implementation of Pakistan's Digital Economy, which is linked to its Digital Pakistan Policy. A longitudinal study tracking the development of Pakistan's National Cybersecurity Strategy (NCSS) over the next 10 years could yield valuable information on how emerging countries develop and sustain national cyber resilience.

REFERENCES

Ahmad, S., & Qayyum, A. (2024). Operational effectiveness of PKCERT: A critical assessment of Pakistan's national cyber incident response capability. Journal of Cybersecurity and Privacy, 4(1), 45–62. https://doi.org/10.3390/jcp4010004

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? International Conference on Cyber Security for Sustainable Society, 6(2), 118–131. https://doi.org/10.1145/3360446

Check Point Research. (2024). Cyber attack trends: 2024 mid-year report — South Asia focus. Check Point Software Technologies. https://research.checkpoint.com/2024/mid-year-report/

Federal Investigation Agency. (2024). Annual cybercrime report 2023–2024. Government of Pakistan. https://www.fia.gov.pk/en/cybercrime-reports

Government of Pakistan. (2016). Prevention of Electronic Crimes Act (PECA 2016). National Assembly of Pakistan. https://moib.gov.pk/Documents/PECA_2016.pdf

Government of Pakistan, Ministry of Information Technology and Telecommunication. (2021). National Cyber Security Policy 2021. MoITT. https://moitt.gov.pk/ncsp2021

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 4 No. 5 (May) (2026)

Kaspersky Lab. (2023). IT threat evolution in South Asia Q3 2023. Kaspersky Security Bulletin. https://securelist.com/it-threat-evolution-q3-2023/111160/

Liveri, D., & Sarri, A. (2014). An evaluation framework for national cyber security strategies. European Union Agency for Network and Information Security (ENISA). https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies

Malaysian Communications and Multimedia Commission [MCMC]. (2024). Cyber Security Act 2024: Overview and implementation guidelines. MCMC. https://www.mcmc.gov.my/en/legislation/acts/cyber-security-act-2024

Pakistan Telecommunication Authority. (2024). Annual cybercrime and internet security report 2024. PTA. https://www.pta.gov.pk/en/media-center/reports

Sharma, R., & Gupta, P. (2023). India's cyber security governance evolution: From CERT-In to NCIIPC. International Journal of Cyber Policy, 3(2), 87–105. https://doi.org/10.1093/ijcp/ijad012

Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cyber security strategies. International Journal of Computer Science and Information Security, 14(1), 129–136.

Smeets, M. (2022). No shortcuts: Why states struggle to develop a military cyber force. Hurst Publishers. https://doi.org/10.1093/oso/9780197638248.001.0001

Tschider, C. (2023). Cybersecurity law and policy in the developing world: Governance capacity, regulatory frameworks, and the global south. Journal of Cyber Policy, 8(1), 12–34. https://doi.org/10.1080/23738871.2023.2187644

Yousaf, M., Khan, A., & Rehman, F. (2023). Adequacy of PECA 2016 in addressing contemporary cybercrime in Pakistan: A legal and technical analysis. Pakistani Journal of Criminology, 15(3), 221–245. https://doi.org/10.31521/pjc.2023.1503.14