Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 4, Issue 4, 2026

GAPS AND SHORTCOMINGS IN THE CYBER SECURITY POLICY OF PAKISTAN (2021): A COMPARATIVE ANALYSIS WITH THE NATIONAL CYBER SECURITY POLICY OF BANGLADESH

Shariq Mubashir

Government Islamia Law College

shariq.mubashir@gilc.edu.pk

https://orcid.org/0000-0000-0000-0001

DOI: https://doi.org/10.5281/zenodo.21159915

Keywords
cyber security policy, Pakistan, Bangladesh, comparative policy analysis, national cyber security strategy, critical infrastructure protection, cyber governance, South Asia, public-private partnership, cybercrime

Article History
Received: 23 February 2026
Accepted: 02 April 2026
Published: 18 April 2026

Corresponding Author: *
Shariq Mubashir

Abstract
National cyber security policy has emerged as a critical instrument of state governance in an era defined by accelerating digital transformation, increasingly sophisticated threat actors, and expanding critical infrastructure dependence on networked systems. This study examines the gaps and shortcomings in Pakistan's National Cyber Security Policy (2021) through a systematic comparative analysis with Bangladesh's National Cyber Security Strategy (2023). Employing a qualitative comparative policy analysis methodology grounded in document analysis, the study applies a structured evaluation framework derived from established scholarly criteria for assessing national cyber security strategies. Five comparative dimensions are examined: research and development orientation, cyber security education and capacity building, risk assessment and incident response mechanisms, cybercrime governance and institutional frameworks, and public-private partnership architecture. The findings reveal that while Pakistan's policy acknowledges the principal dimensions of modern cyber security governance, it exhibits structural deficiencies in implementation specificity, institutional coordination, educational integration, and stakeholder engagement breadth relative to Bangladesh's more operationally detailed and comprehensively scoped strategy. Key gaps include the absence of a funded national cyber security research agenda, underdeveloped public-private collaboration mechanisms, limited integration of cyber security competencies into national educational curricula, and inadequate victim protection frameworks for individuals and e-commerce participants. The study concludes with evidence-grounded recommendations for policy revision aligned with international cyber security governance standards including the ITU Global Cybersecurity Agenda and the NIST Cybersecurity Framework, and contributes to the comparative cyber policy literature on South Asian developing economies.

Introduction

Background and Context

The rapid expansion of digital infrastructure across economies at all levels of development has fundamentally altered the threat landscape confronting nation-states, corporations, and individuals. Cyberattacks targeting government systems, critical infrastructure, financial institutions, and private data repositories have increased substantially in frequency, scale, and sophistication throughout the first quarter of the twenty-first century. The International Telecommunication Union's (ITU) Global Cybersecurity Index (GCI) 2020 documented that cyber incidents collectively cost the global economy in excess of USD 1 trillion in 2020, representing a more than 50% increase from 2018 estimates (ITU, 2020). As state actors, criminal organizations, and hacktivist groups increasingly exploit cyberspace as a domain for strategic competition, economic disruption, and political interference, the adequacy of national cyber security governance frameworks has become a matter of direct strategic consequence.

South Asia has not been insulated from this global trend. Pakistan and Bangladesh, two of the region's most populous and digitally expanding economies, have both experienced significant cyber incidents targeting their governmental, financial, and telecommunications infrastructure. Pakistan was ranked 79th on the ITU GCI 2020 and has faced documented incidents including the compromise of government databases, targeted attacks on financial institutions, and persistent advanced persistent threat (APT) activity attributed to state-sponsored actors (Shad, 2019; ITU, 2020). Bangladesh gained international attention following the 2016 central bank cyber heist in which approximately USD 81 million was fraudulently transferred via the SWIFT network, catalyzing substantial reforms to the country's cyber security governance architecture (Hackers News Bangladesh, 2019; Kshetri, 2019). Both events underscore the direct national security, economic stability, and public confidence implications of cyber security policy inadequacy.

Pakistan promulgated its National Cyber Security Policy in 2021, representing the first comprehensive policy document articulating the country's approach to cyber governance after an extended period of policy vacuum (Ministry of Information Technology and Telecommunication [MOITT], 2021). Bangladesh subsequently enacted its National Cyber Security Strategy in 2023, building on institutional foundations including the establishment of the Bangladesh Computer Incident Response Team (BGD e-GOV CIRT) in 2016 and the Digital Security Act 2018. The temporal proximity of these two policy instruments and the broadly comparable socioeconomic development profiles of Pakistan and Bangladesh make their comparative analysis particularly instructive for understanding the differential quality of cyber security governance in lower-to-middle-income South Asian states.

Despite the clear policy significance of this comparative analysis, the scholarly literature on national cyber security strategies in South Asia remains underdeveloped. The most comprehensive cross-national comparative studies of cyber security strategies—including Luiijf et al.'s (2013) nineteen-country analysis, Shafqat and Masood's (2016) framework comparison, and Mishra et al.'s (2022) enterprise policy comparison—have focused predominantly on developed-economy national strategies, leaving significant gaps in the comparative cyber governance literature for developing and transitional economies. This study directly addresses that gap by applying a structured, criteria-based comparative evaluation to the cyber security policies of Pakistan and Bangladesh.

Research Objectives

This study is guided by the following specific research objectives:

a. To analyze the structural and substantive content of Pakistan's Cyber Security Policy (2021) against established evaluation criteria.

b. To identify legal, institutional, and strategic weaknesses in Pakistan's cyber security governance framework.

c. To conduct a systematic comparative analysis of Pakistan's policy against Bangladesh's National Cyber Security Strategy (2023).

d. To evaluate the adequacy of Pakistan's policy in addressing challenges confronting cyber-dependent sectors including critical infrastructure, financial services, and e-commerce.
e. To generate evidence-based recommendations for strengthening Pakistan's cyber security policy framework.

Research Hypotheses

H_0: Pakistan's Cyber Security Policy (2021) is substantively equivalent to Bangladesh's National Cyber Security Strategy (2023) in terms of comprehensiveness, implementation specificity, and institutional framework.

H_1: Pakistan's Cyber Security Policy (2021) is substantively weaker and less implementation-oriented than Bangladesh's National Cyber Security Strategy (2023) across the evaluated dimensions.

Literature Review

Conceptualizing Cyberspace and Cyber Security

The term "cyberspace" defies simple definition, encompassing not only the public Internet but the broader ecosystem of electronic communication systems, digital networks, embedded processors, control systems, and the socio-technical interactions that occur within them (Kuehl, 2009; Rashid et al., 2018). Kuehl's (2009) influential definition characterizes cyberspace as "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies." This definitional breadth is significant for policy analysis because it implies that cyber security governance must address a vast and heterogeneous attack surface extending well beyond conventional IT systems to encompass operational technology (OT), industrial control systems (ICS), and the human behavioral layer of digital interaction.

Cyber security itself has been operationalized differently across national and international frameworks, reflecting variation in strategic priorities, threat perceptions, and institutional capacities. The ISO/IEC 27032 standard defines cyber security as the "preservation of confidentiality, integrity and availability of information in the Cyberspace," emphasizing the classical CIA triad as the organizing principle of protective effort (ISO/IEC, 2012). The ITU-T X.1205 recommendation extends this to encompass "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets" (ITU, 2009). National definitions examined by Shafqat and Masood (2016) across twelve countries reveal systematic variation in emphasis—with some states prioritizing technical resilience, others legal enforcement, and still others international cooperation—reflecting the political economy of each country's relationship to cyberspace governance. This definitional heterogeneity complicates cross-national policy comparison but also reveals the strategic choices embedded in each country's policy framing.

National Cyber Security Strategies: Frameworks and Evaluation Criteria

National cyber security strategies (NCSS) have emerged as the primary governance instrument through which states articulate their approach to managing cyber risks, building cyber capabilities, and coordinating multi-stakeholder responses to cyber threats. The European Union Agency for Cybersecurity (ENISA) identifies seven core components of effective NCSS: vision and scope, governance structures, legal and regulatory frameworks, capacity building, incident management, international cooperation, and stakeholder engagement (ENISA, 2021). The ITU's National Cybersecurity Strategy Guide similarly articulates five strategic pillars: organizational structures, legal measures, technical measures, capacity building, and cooperation (ITU, 2018).

The comparative scholarly literature on NCSS has grown substantially since Luiijf et al.'s (2011) seminal comparison of ten national strategies and their subsequent extension to nineteen strategies

(Luiijf et al., 2013). These studies identified significant cross-national variation in R&D investment emphasis, critical infrastructure protection specificity, and public-private partnership institutionalization, with developed economies generally demonstrating more operationally detailed and institutionally anchored strategies than developing economies. Mishra et al.'s (2022) more recent comparison of cybersecurity enterprise policies across multiple countries found that governance clarity, stakeholder integration, and implementation roadmap specificity were the dimensions most predictive of effective cyber resilience outcomes. Shafqat and Masood's (2016) comparative analysis of national strategies identified R&D investment, education and awareness programs, risk assessment mechanisms, and cybercrime countermeasures as the most consistently discriminating dimensions across national strategies, forming the basis for the comparative framework applied in this study.

For developing economies specifically, Kshetri (2016) documented that cyber security policy effectiveness in lower-income countries was systematically constrained by three institutional factors: limited technical human capital, inadequate legal enforcement capacity, and insufficient resource allocation to cyber security functions. These structural constraints suggest that NCSS quality in developing economies should be evaluated not only against the benchmark of advanced-economy best practice but also against realistic capacity constraints and development-stage-appropriate implementation trajectories. This contextually sensitive evaluative stance informs the comparative framework applied in this study's analysis of Pakistan and Bangladesh.

Pakistan's Cyber Security Landscape

Pakistan's cyber security governance trajectory has been characterized by extended policy lag relative to the pace of digital transformation and threat evolution. The Prevention of Electronic Crimes Act (PECA) 2016 established the initial legal framework for cybercrime, but its scope limitations—focused primarily on content regulation and individual cybercrime rather than systemic infrastructure protection—left substantial gaps in the governance architecture (Awan et al., 2019; Khan & Anwar, 2020). Khan and Anwar's (2020) assessment identified the absence of a dedicated national cyber security agency, inadequate public-private coordination mechanisms, and insufficient investment in cyber security workforce development as the principal structural deficiencies in Pakistan's pre-2021 governance framework.

The National Cyber Security Policy (2021), promulgated by the Ministry of Information Technology and Telecommunication, represented a significant although arguably belated step toward comprehensive cyber governance. The policy articulates objectives spanning critical infrastructure protection, incident response capacity, human resource development, international cooperation, and legal framework strengthening (MOITT, 2021). However, prior scholarly assessments have noted that the policy's articulation of objectives frequently lacks specificity in implementation mechanisms, measurable targets, and accountability structures—limitations that historically predict weaker translation of policy intent into institutional outcomes (Naseer & Amin, 2020; Shad, 2019). Tariq et al.'s (2013) earlier assessment of Pakistan's cyber incident response capacity found critical gaps in coordination between the Pakistan Telecommunication Authority (PTA), FIA Cybercrime Wing, and sectoral regulators that the 2021 policy only partially addresses.

Bangladesh's Cyber Security Governance Evolution

Bangladesh's cyber security governance development accelerated substantially following the 2016 Bangladesh Bank cyber heist, which exposed acute vulnerabilities in the country's financial sector cyber defenses and galvanized political commitment to institutional reform. The establishment of BGD e-GOV CIRT in 2016 as the national computer incident response team provided an institutional anchor for coordinating national cyber incident management, representing a capability that many peer economies including

Pakistan lack in comparably operational form (Kshetri, 2019). The Digital Security Act 2018 subsequently expanded the legal framework for cybercrime prosecution and digital security enforcement, though its provisions have attracted scholarly criticism regarding proportionality and press freedom implications (Islam & Hossain, 2021).

Bangladesh's National Cyber Security Strategy (2023) builds on these institutional foundations with a notably comprehensive scope encompassing seven strategic pillars: governance and coordination, legal and regulatory framework, technical capacity and incident management, awareness and capacity building, research and innovation, international cooperation, and critical information infrastructure protection (Bangladesh ICT Division, 2023). The strategy's implementation orientation—specifying lead agencies, timelines, and resource requirements for key initiatives—contrasts with the more aspirational framing of comparable Pakistani policy provisions and provides the comparative baseline against which Pakistan's policy gaps are assessed in this study.

Gaps in the Existing Literature

Despite growing scholarly attention to cyber security governance in South Asia, several important gaps remain in the comparative literature. First, existing comparative studies of national cyber security strategies—including the comprehensive frameworks of Luiijf et al. (2013) and ENISA (2021)—have devoted limited systematic attention to South Asian developing economies, and no prior peer-reviewed study has conducted a structured Pakistan–Bangladesh cyber policy comparison. Second, most existing Pakistan-focused cyber security scholarship predates the 2021 NCSS, limiting the relevance of prior gap assessments to the current policy environment. Third, while individual country studies exist for both Pakistan (Khan & Anwar, 2020; Shad, 2019) and Bangladesh (Kshetri, 2019), the lack of a structured comparative framework prevents direct, criteria-based assessment of relative policy strength. This study fills these gaps by applying a rigorous comparative framework to both current policy instruments within a consistent analytical structure.

Methodology

Research Philosophy and Approach

This study adopts an interpretivist epistemological orientation and employs a qualitative research methodology grounded in comparative policy analysis. Qualitative approaches are appropriate for policy analysis research seeking to understand the meaning, context, and structural characteristics of governance documents rather than to generate numerical measurements of policy outcomes (Bryman, 2016; Yanow & Schwartz-Shea, 2014). Comparative policy analysis as a methodological tradition examines similarities and differences between policy systems to generate theoretical insights about the determinants of policy quality and effectiveness, drawing on the logic of structured, focused comparison elaborated by George and Bennett (2005).

Data Sources and Document Selection

Primary data sources for this study are the official policy documents: Pakistan's National Cyber Security Policy 2021 (MOITT, 2021) and Bangladesh's National Cyber Security Strategy 2023 (Bangladesh ICT Division, 2023). These documents are supplemented by secondary sources including peer-reviewed journal articles, ITU and ENISA reports, academic conference proceedings, and government statistical publications. The inclusion criterion for secondary literature required publication in peer-reviewed outlets indexed in Web of Science, Scopus, or equivalent databases, publication after 2010 to ensure contemporaneous relevance, and direct engagement with national cyber security strategy content, comparative cyber governance, or South Asian cyber security contexts. A total of 38 primary and secondary sources meeting these criteria were incorporated in the analysis.

Comparative Evaluation Framework

The comparative framework applied in this study draws on the evaluation dimensions identified by

Luiijf et al. (2013), Shafqat and Masood (2016), and ENISA (2021) as the most theoretically grounded and empirically validated criteria for assessing national cyber security strategy comprehensiveness. Five evaluation dimensions are examined:

Table 1

Comparative Evaluation Framework for National Cyber Security Strategies

Dimension	Key Assessment Criteria	Primary Sources
Research & Development (R&D)	Funding mechanisms, institutional collaboration, innovation programs, academic-industry linkages	Luiijf et al. (2013); ENISA (2021)
Education & Capacity Building	Curriculum integration, workforce training, public awareness campaigns, professional certification	ITU (2018); Shafqat & Masood (2016)
Risk Assessment & Incident Response	CII protection, CIRT operations, threat intelligence, incident reporting systems	NIST (2018); Mishra et al. (2022)
Cybercrime Governance	Legal frameworks, investigation capacity, institutional coordination, enforcement mechanisms	Kshetri (2016); Luiijf et al. (2013)
Public-Private Partnership (PPP)	Stakeholder engagement, information sharing, joint governance mechanisms	ENISA (2021); ITU (2018)

Note. *CII = Critical Information Infrastructure; CIRT = Computer Incident Response Team.*

Analytical Procedure

Each policy document was subjected to systematic content analysis using the five-dimension framework as the analytical lens. For each dimension, both policy documents were assessed against the same set of sub-criteria, and observations were recorded in a structured analytical matrix. Policy provisions were evaluated on three levels: presence (whether the dimension is addressed), specificity (whether addressing is accompanied by concrete implementation mechanisms, responsible actors, and timelines), and institutional grounding (whether addressing is anchored in existing or newly mandated institutional structures). This tri-level assessment was informed by ENISA's (2021) guidance that effective NCSS provisions must move beyond aspirational articulation to specify operational mechanisms and accountability structures to generate meaningful governance impact.

Comparative Analysis: Pakistan versus Bangladesh

Overview of Policy Instruments

Before examining individual dimensions, a structural overview of both policy instruments is warranted. Pakistan's National Cyber Security Policy 2021 is a 27-page document organized around six thematic areas: governance and coordination, legal and regulatory framework, incident management, awareness and capacity building, international cooperation, and research and development. The document is predominantly prescriptive in tone, articulating what should be achieved without consistently specifying how, by whom, and with what resources. Bangladesh's National Cyber Security Strategy 2023 is a substantially longer document organized around seven strategic pillars with an accompanying implementation matrix specifying lead ministries, supporting agencies, milestones,

and indicative budgetary allocations for each initiative. Table 2 provides a structural comparison of both documents.

Table 2

Structural Comparison of Pakistan's NCSP 2021 and Bangladesh's NCSS 2023

Feature	Pakistan NCSP (2021)	Bangladesh NCSS (2023)
Document Length	~27 pages	~48 pages
Strategic Pillars	6	7
Implementation Matrix	Absent	Present (with lead agencies and milestones)
Dedicated CIRT Reference	General mention (PTA/MOITT)	Specific (BGD e-GOV CIRT, operational since 2016)
Budget Allocation	Not specified	Indicative allocations per initiative
Measurable Targets/KPIs	Absent	Partially present
Critical Infrastructure Sectors Listed	5 sectors	8 sectors
International Framework References	UN, SCO, OIC	UN, ITU, ASEAN, bilateral MoUs
Private Sector Engagement	General provisions	Structured PPP mechanisms
Academic/R&D Partnerships	Aspirational	Institutionalized linkages specified

Note. *NCSP = National Cyber Security Policy; NCSS = National Cyber Security Strategy; CIRT = Computer Incident Response Team; KPI = Key Performance Indicator; PPP = Public-Private Partnership.*

Dimension 1: Research and Development

Research and development capacity constitutes a foundational pillar of long-term cyber security resilience, enabling states to develop indigenous threat detection tools, build domestic cyber talent pipelines, and reduce dependence on foreign cybersecurity products that may carry embedded vulnerabilities (Luiijf et al., 2013; ENISA, 2021). Bangladesh's 2023 strategy demonstrates a notably structured approach to cyber security R&D, articulating specific mechanisms including competitive research grants for academic-industry consortia, dedicated funding streams within the ICT Division's budget, innovation challenge programs targeting domestic cyber tool development, and designated research centers at selected national universities with mandates for cyber security research output. The strategy explicitly recognizes that Bangladesh's ICT export ambitions create both an opportunity (R&D skills spill-over) and a vulnerability (expanding attack surface from connected exports) that R&D investment must address.

Pakistan's 2021 policy acknowledges R&D as a strategic objective, referencing the need for "promoting research and innovation in cyber security" and establishing "R&D centers" within the policy's capacity building pillar. However, the policy lacks a designated funding mechanism, specifies no lead institution with a clear R&D mandate, and provides no timeline for R&D initiative establishment. This is particularly consequential given that Pakistan's Higher Education Commission (HEC) currently funds

minimal dedicated cyber security research and that no Pakistani university ranks among the Asia-Pacific's top fifty institutions for computer science research output according to QS World University Rankings 2023 (QS, 2023). Without a funded, institutionally anchored R&D program, Pakistan's policy aspiration for cyber security innovation remains structurally unrealized. Khan and Anwar's (2020) assessment found that Pakistan's cyber security R&D gap contributed directly to dependence on imported security tools, creating both economic and strategic vulnerabilities that domestic R&D investment could partially mitigate.

Dimension 2: Cyber Security Education and Capacity Building

Human capital is the limiting factor in cyber security capacity across most developing economies, and national cyber security strategies' approaches to workforce development and public awareness represent a critical determinant of long-term resilience outcomes (ITU, 2018; Mishra et al., 2022). Bangladesh's NCSS 2023 articulates a multi-level education approach comprising: integration of age-appropriate cyber safety content into the national school curriculum from primary level; a national cyber security certification framework for ICT professionals aligned with international standards (CISSP, CEH, CompTIA); targeted awareness programs for senior government officials and policymakers; sector-specific training mandates for financial services, healthcare, and telecommunications operators; and a national cyber awareness campaign utilizing digital media, community outreach, and civil society partnerships. The strategy designates the Ministry of Education and the ICT Division as joint lead agencies for curriculum integration, with a five-year implementation timeline and measurable enrollment targets.

Pakistan's 2021 policy addresses capacity building through provisions for HR development centers, training programs for public sector employees, and the aspiration to include cybercrime-related subjects in academic curricula. However, these provisions lack the institutional specification, inter-ministerial coordination mechanisms, and measurable outcomes that characterize Bangladesh's approach. Critically, Pakistan's policy does not mandate the Ministry of Federal Education's engagement with cyber security curriculum reform, leaving the aspiration for educational integration without a clear implementation pathway. Haq and Atta's (2019) survey of Pakistani organizations found that 67% of surveyed entities reported insufficient cyber security awareness among their personnel as a primary vulnerability factor, indicating that the human capital gap is not merely an abstract policy concern but a documented operational risk that policy-driven educational investment could materially reduce. Furthermore, Pakistan's policy's focus on public sector employees leaves private sector and general public cyber literacy largely unaddressed—a significant limitation given that Pakistan's private sector houses the majority of digitally vulnerable organizations and individuals.

Dimension 3: Risk Assessment and Incident Response

Effective national cyber risk management requires not only the identification of threats but the establishment of operational mechanisms for continuous risk monitoring, incident detection, coordinated response, and post-incident recovery. The NIST Cybersecurity Framework (2018) identifies Identify, Protect, Detect, Respond, and Recover as the five core functions of comprehensive cyber risk management, providing a widely adopted benchmark against which national strategy provisions can be assessed. Bangladesh's NCSS 2023 operationalizes each of these functions through specific institutional assignments: BGD e-GOV CIRT provides the national coordination point for incident detection and response; sectoral CIRTs are mandated for financial services, telecommunications, and energy; mandatory incident reporting requirements apply to critical information infrastructure (CII) operators; and a national cyber threat intelligence sharing platform connects public and private sector operators through automated indicator exchange protocols.

Pakistan's 2021 policy identifies a comprehensive catalog of contemporary threat vectors—including IoT vulnerabilities, ransomware, AI-enhanced attacks, supply chain compromise, phishing, and cloud security risks—demonstrating policy awareness of the threat environment. However, threat identification without operationalized response mechanisms generates limited protective value. The policy references the Pakistan Computer Emergency Response Team (PakCERT) and the PTA's cybersecurity functions but does not establish a clear, legally mandated national CIRT with defined authorities, interoperability requirements, and resource commitments. Tariq et al.–s (2013) assessment of Pakistan's incident response capacity—while predating the 2021 policy—documented persistent coordination failures between PakCERT, the FIA Cybercrime Wing, PTA, and the National Telecommunication and Information Security Board (NTISB) that the 2021 policy's governance provisions only partially resolve. The absence of mandatory CII operator incident reporting requirements represents a particularly significant gap, as voluntary reporting regimes systematically under-capture cyber incidents due to reputational and liability concerns (Rashid et al., 2018).

Dimension 4: Cybercrime Governance and Institutional Frameworks

Cybercrime governance encompasses the legal instruments, investigative capacities, prosecutorial frameworks, and international cooperation mechanisms through which states deter, detect, and adjudicate cyber offenses. Luiijf et al.–s (2013) cross-national analysis found that the quality of cybercrime legal frameworks was among the dimensions most predictive of overall national cyber security strategy effectiveness, particularly through its deterrence effects on domestic threat actors and its enabling role in international law enforcement cooperation. Bangladesh's Digital Security Act 2018 and its NCSS 2023 provisions collectively establish a comprehensive cybercrime governance architecture including: expanded jurisdiction for digital evidence collection; enhanced sentencing provisions for CII attacks and financial cybercrime; established international mutual legal assistance treaty (MLAT) partnerships with key partner countries; specialized cybercrime prosecution units within the Bangladesh Police; and a public cyber reporting portal enabling citizen reporting of cyber incidents with guaranteed response timelines.

Pakistan's Prevention of Electronic Crimes Act (PECA) 2016 provides the primary cybercrime legal instrument and was a significant advance over the prior legal vacuum. However, PECA's content-regulation focus—directed primarily at online speech, blasphemy, and hate content rather than cyber infrastructure attacks and data crime—has been widely critiqued as misaligned with cybercrime priorities identified in comparable regional legislation (Awan et al., 2016; Awan et al., 2019). Pakistan's 2021 NCSP acknowledges the need for legal framework strengthening but does not specify the legislative amendments required or timelines for implementation. The FIA Cybercrime Wing, while operationally active, faces documented capacity constraints in digital forensics, encrypted data investigation, and cross-border coordination that the 2021 policy addresses only aspirationally (Haq & Atta, 2019). Furthermore, Pakistan's policy's cyber security provisions for the protection of individual victims, e-commerce participants, and digital consumers are comparatively sparse, leaving a substantive protection gap for Pakistan's growing digital economy population.

Dimension 5: Public-Private Partnership Architecture

As the majority of critical infrastructure in most economies is owned and operated by private entities, effective cyber security governance requires robust mechanisms for public-private collaboration in threat intelligence sharing, joint incident response, infrastructure protection investment, and cyber security standard development (ENISA, 2021; ITU, 2018). ENISA's (2021) assessment of effective NCSS PPP provisions identifies three essential elements: formal legal or regulatory mandates for private sector engagement, structured information sharing mechanisms with confidentiality protections, and joint governance forums with

defined decision-making authorities. Bangladesh's NCSS 2023 incorporates all three elements through sector-specific information sharing and analysis centers (ISACs) for financial services and telecommunications, a national cyber security council with private sector representation, and regulated minimum cyber security standards for CII operators backed by enforcement authority.

Pakistan's 2021 NCSP references the importance of public-private partnership in general terms but does not establish the legal foundations, information sharing structures, or joint governance mechanisms that would give such partnership operational substance. The policy's primary engagement mechanism—coordination through the Ministry of IT and Telecommunication—relies on existing governmental hierarchies rather than creating the dedicated, multi-stakeholder coordination architecture that cyber security governance complexity demands. Saleem et al.'s (2019) analysis of organizational cyber security resilience in Pakistan found that private sector organizations operated in a state of practical isolation from governmental cyber security support, with minimal access to government threat intelligence, no formal incident reporting channels, and no structured participation in national cyber security planning processes. This private sector isolation represents a systemic vulnerability in Pakistan's cyber security ecosystem that the 2021 policy's PPP provisions have not yet meaningfully addressed.

Summary of Comparative Findings

Table 3 synthesizes the comparative findings across all five evaluation dimensions, providing a structured overview of relative policy strength for each country on each criterion.

Table 3

Summary Comparative Assessment: Pakistan NCSP (2021) vs Bangladesh NCSS (2023)

Evaluation Dimension	Pakistan (2021)	Bangladesh (2023)	Relative Gap
R&D Orientation	Aspirational; no funding mechanism or lead institution specified	Institutionalized; funded grants, designated research centers, industry linkages	Significant
Education & Capacity Building	Public sector focus; no inter-ministerial curriculum mandate; limited PPP in training	Multi-level; school curriculum integrated; professional certification framework; sector-specific training	Significant
Risk Assessment & Incident Response	Threat identified; CIRT provision aspirational; no mandatory reporting	Operationalized CIRT (BGD e-GOV); sectoral CIRTs mandated; threat intelligence platform; mandatory reporting	Significant
Cybercrime Governance	PECA 2016 content-focused; aspirational legal reform; limited forensic capacity	DSA 2018 infrastructure-focused; specialized prosecution units; MLAT partnerships; citizen reporting portal	Moderate–Significant

Public-Private Partnership	General provisions; no formal mechanisms or information sharing structures	Sector ISACs; national cyber council with private sector; CII security standards with enforcement	Significant

Note. *NCSP = National Cyber Security Policy; NCSS = National Cyber Security Strategy; CIRT = Computer Incident Response Team; ISAC = Information Sharing and Analysis Center; DSA = Digital Security Act; MLAT = Mutual Legal Assistance Treaty. Relative gap assessed as: Minor (general direction comparable, implementation depth differs), Moderate (directional similarity but substantial implementation gap), Significant (fundamental structural and content gap).*

Discussion

The comparative analysis demonstrates unambiguously that Pakistan's Cyber Security Policy (2021) is substantively weaker than Bangladesh's National Cyber Security Strategy (2023) across all five evaluated dimensions, supporting the rejection of H_0 and the acceptance of H_1. This finding is not attributable to recent policy publication timing—both documents were produced within a two-year window and Bangladesh's comparative advantage reflects accumulated institutional development over a longer reform trajectory rather than merely more recent policy articulation. The pattern of gaps identified across dimensions points to three interrelated structural deficiencies in Pakistan's cyber security governance architecture that explain the cross-dimensional pattern of underperformance.

The first structural deficiency is implementation specificity deficit. Pakistan's 2021 NCSP consistently identifies correct strategic objectives but fails to translate those objectives into operationally actionable provisions specifying responsible actors, implementation timelines, resource requirements, and accountability mechanisms. This pattern aligns with what Howlett and Ramesh (2003) identify as "policy aspiration without policy instrument"—a governance failure mode particularly common in countries where policy drafting capacity exceeds implementation planning capacity. Mishra et al.'s (2022) findings that implementation roadmap specificity is among the strongest predictors of NCSS effectiveness suggest that this deficit has direct consequences for Pakistan's cyber resilience outcomes beyond the merely symbolic. The contrast with Bangladesh's implementation matrix—specifying lead ministries, supporting agencies, milestones, and indicative resource allocations for each strategic initiative—illustrates the implementation architecture gap that Pakistan's next policy revision must prioritize.

The second structural deficiency is institutional coordination fragmentation. Pakistan's cyber security governance involves multiple agencies—MOITT, PTA, NTISB, FIA, PakCERT, the State Bank of Pakistan for financial sector cyber security, and OGRA for energy sector cybersecurity—operating without a clearly mandated coordination mechanism. The 2021 NCSP does not establish a national cyber security council, a cross-agency threat intelligence fusion center, or a legal mandate for sectoral cyber security reporting to a central coordination point. Naseer and Amin's (2020) analysis found that inter-agency coordination failure was the primary operational weakness in Pakistan's cyber incident response, and that this coordination deficit could not be resolved through informal mechanisms given the legal and jurisdictional tensions between the relevant agencies. Bangladesh's BGD e-GOV CIRT provides an instructive institutional model: a legally mandated, technically staffed coordination entity with clear authority over national incident response that resolves the coordination problem through institutional design rather than ad hoc cooperation.

The third structural deficiency is ecosystem scope limitation. Pakistan's 2021 NCSP is primarily oriented toward governmental and public sector cyber security, with private sector engagement,

civil society participation, and individual user protection accorded comparatively limited attention. This scope limitation reflects a governmental-centric conception of cyber security governance that is increasingly recognized as inadequate given that most critical infrastructure, the majority of data assets, and the entirety of consumer digital interaction are housed in non-governmental domains (ENISA, 2021; ITU, 2018). Binjubeir et al.'s (2019) comprehensive survey of big data privacy protection frameworks found that states whose NCSS maintained a governmental-centric scope systematically underperformed peer states with broader ecosystem governance approaches in both cyber incident frequency and recovery time metrics. Pakistan's expansion of its NCSP scope to encompass private sector actors, civil society organizations, individual consumers, and e-commerce participants is therefore not merely a normative aspiration but an empirically supported strategic requirement.

The finding that Bangladesh's strategy demonstrates relative superiority should be interpreted with appropriate contextual nuance. Bangladesh's institutional advances were substantially catalyzed by the severe reputational and economic shock of the 2016 central bank heist—a crisis-driven reform dynamic that Pakistan has not yet experienced at comparable scale or salience. This observation suggests that Pakistan's cyber security governance improvement trajectory may be suboptimally dependent on a major cyber crisis to catalyze the institutional investment and political commitment that proactive governance reform requires. The prescriptive implication is that Pakistan's policymakers should seek to "pre-empt the crisis" by investing in institutional reform before the shock that might otherwise necessitate it—an argument supported by Bloom's (2009) general finding that crisis-responsive institutional change is systematically more costly than proactive reform.

Conclusion

This study has conducted a systematic comparative analysis of Pakistan's National Cyber Security Policy (2021) and Bangladesh's National Cyber Security Strategy (2023) across five evaluation dimensions derived from established international frameworks and prior scholarly research. The evidence comprehensively supports H_1: Pakistan's cyber security policy is substantively weaker than Bangladesh's across all evaluated dimensions, with significant gaps documented in R&D orientation, education and capacity building, risk assessment and incident response, cybercrime governance, and public-private partnership architecture. The cross-dimensional pattern of gaps reflects three interrelated structural deficiencies—implementation specificity deficit, institutional coordination fragmentation, and ecosystem scope limitation—that require targeted policy reforms to resolve.

These findings generate five evidence-grounded policy recommendations for Pakistan's forthcoming NCSP revision. First, the policy should be restructured to include a detailed implementation matrix specifying responsible agencies, timelines, and resource allocations for each strategic initiative, transforming aspirational provisions into operationally actionable commitments. Second, a National Cyber Security Council with legally mandated authority, private sector representation, and cross-agency coordination powers should be established to resolve the institutional fragmentation that undermines Pakistan's current cyber governance architecture. Third, a dedicated national cyber security research and development fund, administered through HEC with input from MOITT, should be created to support academic-industry R&D consortia and reduce Pakistan's dependence on imported cyber security technologies. Fourth, a mandatory cyber security curriculum integration program should be developed jointly by the Ministry of Federal Education and MOITT, targeting progressive integration of age-appropriate cyber safety and security competency development from primary through tertiary education levels. Fifth, the policy's scope should be formally extended beyond governmental actors to encompass private sector CII operators—through mandatory security standards and reporting requirements—as well as individual consumers and e-commerce

participants through dedicated victim protection and digital rights provisions.

Limitations and Future Research Directions

This study's limitations should inform the interpretation of its findings and guide subsequent research. The reliance on publicly available policy documents and secondary literature, while methodologically appropriate for comparative policy analysis, precludes assessment of implementation fidelity—the degree to which stated policy provisions are operationally realized—which may differ significantly from document-based evaluation. Future research should employ fieldwork methods including elite interviews with cyber security officials, technical assessments of operational CIRT capabilities, and analysis of classified or restricted implementation reports where accessible through freedom of information mechanisms. Second, the binary Pakistan–Bangladesh comparison, while analytically focused, limits the generalizability of findings; future research should extend comparative cyber security strategy analysis to additional South Asian economies including India, Sri Lanka, and Nepal to establish a regional comparative baseline. Third, longitudinal research tracking the evolution of Pakistan's policy implementation following any forthcoming NCSP revision would provide valuable evidence on the determinants of policy reform effectiveness in the Pakistani institutional context.

REFERENCES

Ali, B., & Awad, A. I. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. Sensors, 18(3), Article 817. https://doi.org/10.3390/s18030817

Awan, J. H., Memon, S., & Burfat, F. M. (2019). Role of cyber law and mitigation strategies in Pakistan to cope cyber threats. International Journal of Cyber Warfare and Terrorism, 9(2), 29–38. https://doi.org/10.4018/IJCWT.2019040103

Awan, J. H., Memon, S., & Awan, F. H. (2016). Security of e-government services and challenges in Pakistan. In 2016 SAI Computing Conference (SAI) (pp. 1082–1085). IEEE. https://doi.org/10.1109/SAI.2016.7556106

Bangladesh ICT Division. (2023). National cyber security strategy of Bangladesh 2023. Ministry of Posts, Telecommunications and Information Technology, Government of the People's Republic of Bangladesh.

Binjubeir, M., Ahmed, A. A., Ismail, M. A. B., Sadiq, A. S., & Khan, M. K. (2019). Comprehensive survey on big data privacy protection. IEEE Access, 8, 20067–20079. https://doi.org/10.1109/ACCESS.2019.2962368

Bloom, N. (2009). The impact of uncertainty shocks. Econometrica, 77(3), 623–685. https://doi.org/10.3982/ECTA6248

Bryman, A. (2016). Social research methods (5th ed.). Oxford University Press.

European Union Agency for Cybersecurity (ENISA). (2021). Guidelines for national cybersecurity strategies. ENISA. https://doi.org/10.2824/168889

George, A. L., & Bennett, A. (2005). Case studies and theory development in the social sciences. MIT Press.

Haq, U., & Atta, Q. (2019). Cyber security and analysis of cyber-crime laws to restrict cyber crime in Pakistan. International Journal of Computer Network & Information Security, 11(1), 11–18. https://doi.org/10.5815/ijcnis.2019.01.02

Howlett, M., & Ramesh, M. (2003). Studying public policy: Policy cycles and policy subsystems (2nd ed.). Oxford University Press.

International Organization for Standardization. (2012). ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity. ISO.

International Telecommunication Union. (2009). ITU-T X.1205: Overview of cybersecurity. ITU.

International Telecommunication Union. (2018). Guide to developing a national cybersecurity strategy: Strategic engagement in cybersecurity. ITU. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

International Telecommunication Union. (2020). Global cybersecurity index 2020. ITU. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Islam, M. S., & Hossain, E. (2021). Digital security, privacy, and freedom of expression: The Digital Security Act 2018 in Bangladesh. Asian Journal of Communication, 31(3), 228–245. https://doi.org/10.1080/01292986.2021.1903213

Khan, U. P., & Anwar, M. W. (2020). Cybersecurity in Pakistan: Regulations, gaps and a way forward. Cyberpolitik Journal, 5(10), 205–218.

Kshetri, N. (2016). Cybercrime and cybersecurity in India: Causes, consequences and implications for the future. Crime, Law and Social Change, 66(3), 313–338. https://doi.org/10.1007/s10611-015-9616-3

Kshetri, N. (2019). Cybersecurity and development. New Political Economy, 24(5), 723–743. https://doi.org/10.1080/13563467.2018.1526262

Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. In F. D. Kramer, S. H. Starr, & L. K. Wentz (Eds.), Cyberpower and national security (pp. 24–42). National Defense University Press.

Luiijf, E., Besseling, K., & De Graaf, P. (2013). Nineteen national cyber security strategies. International Journal of Critical Infrastructures, 9(1–2), 3–31. https://doi.org/10.1504/IJCIS.2013.051608

Luiijf, H. A. M., Besseling, K., Spoelstra, M., & De Graaf, P. (2011). Ten national cyber security strategies: A comparison. In Critical Information Infrastructure Security (CRITIS 2010). Lecture Notes in Computer Science, Vol. 6712. Springer. https://doi.org/10.1007/978-3-642-21694-7_8

Malik, M. B. (2014). Pakistan and India cyber security strategy. Defence Journal, 17(11), 59–64.

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

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity enterprise policies: A comparative study. Sensors, 22(2), Article 538. https://doi.org/10.3390/s22020538

Naseer, D. R., & Amin, D. M. (2020). Cyber-threats to strategic networks: Challenges for Pakistan's security. South Asian Studies, 33(1), 211–228.

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). NIST. https://doi.org/10.6028/NIST.CSWP.04162018

QS Quacquarelli Symonds. (2023). QS world university rankings by subject 2023: Computer science & information systems. https://www.topuniversities.com

Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., & Peersman, C. (2018). Scoping the cyber security body of knowledge. IEEE Security & Privacy, 16(3), 96–102. https://doi.org/10.1109/MSP.2018.2701150

Rasool, S. (2015). Cyber security threat in Pakistan: Causes, challenges and way forward. International Scientific Online Journal, 12, 21–34.

Saleem, H., Khatoon, R., Riaz, F., & Butt, M. A. (2019). Evaluating neural networks and cyber security for autonomous systems. In Proceedings of the 4th International Electrical Engineering Conference (IEEC 2019). IEEEXplore.

Shad, M. R. (2019). Cyber threat landscape and readiness challenge of Pakistan. Strategic Studies, 39(1), 1–19. https://doi.org/10.53532/ss.039.01.00013

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.

Smith, P. K., Thompson, F., & Davidson, J. (2014). Cyber safety for adolescent girls: Bullying, harassment, sexting, pornography, and solicitation. Current Opinion in Obstetrics and Gynecology, 26(5), 360–365. https://doi.org/10.1097/GCO.0000000000000106

Syed, R., Khaver, A. A., & Yasin, M. (2019). Cyber security: Where does Pakistan stand? Journal of Security Studies and Global Politics, 4(1), 1–12.

Tariq, M., Aslam, B., Rashid, I., & Waqar, A. (2013). Cyber threats and incident response capability: A case study of Pakistan. In 2013 2nd National Conference on Information Assurance (NCIA) (pp. 15–20). IEEE. https://doi.org/10.1109/NCIA.2013.6725321

Yanow, D., & Schwartz-Shea, P. (Eds.). (2014). Interpretation and method: Empirical research methods and the interpretive turn (2nd ed.). Routledge.