CYBERSECURITY AND PAKISTAN'S NATIONAL SECURITY: THREAT LANDSCAPE, POLICY GAPS AND STRATEGIC IMPERATIVES

Asif Hussain & Dr Muhammad Fahim Khan*

Abstract

Rapid digital infrastructure growth in Pakistan has made the country more vulnerable to cyber threats, which now threaten its business sector(s) and government institutions. This study investigates Pakistan's escalating cyber security risks through an analysis of three essential theoretical models, which include securitisation theory, deterrence, and hybrid warfare. Qualitative thematic analysis is used for policy documents, cyber incident reports, and academic literature to reveal governance weaknesses, legal framework deficiencies, and institutional capability shortfalls. Evidence indicates Pakistan operates in a complex cyber environment where advanced persistent threats (APTs), ransom ware attacks, cyber-espionage, and disinformation operations persist. Findings reveal that India maintains its position as Pakistan's main external cyber threat actor through its growing offensive capabilities, which also receive support from Israeli partnerships. Sectoral analysis shows that Pakistan faces multiple challenges because of poor inter-agency coordination, insufficient CERT capabilities, excessive dependence on foreign technology, and inadequate legal protections that extend beyond the Prevention of Electronic Crimes Act (PECA) 2016. Current weaknesses in Pakistan's cyber security framework make it extremely difficult to stop or prevent sophisticated cyber-attacks and recover from them quickly. The paper suggests developing an extensive national cyber security plan that combines denial-based deterrence with resilience enhancement strategies. It also advocates for creating a unified cyber security authority, implementing mandatory breach disclosure requirements, supporting local R&D initiatives, and developing cooperative cyber confidence-building initiatives with neighboring countries. Evidence also demonstrates that Pakistan faces economic damage, reputation loss, and strategic instability because of its unaddressed institutional problems during the current hybrid warfare escalation.

Keywords: Cyber security; Hybrid Warfare; Cyber Threats; National Security; Advanced Persistent Threats (APT); Cyber Policy; India–Israel Cyber Cooperation; Critical Infrastructure; PECA 2016.

Introduction

Rapid transformation of Pakistan's digital space brings both new possibilities and perilous security threats to the country. The banking sector, together with

*Mr. Asif Hussain is a PhD Scholar in International Relations, and Dr. Muhammad Fahim Khan is an Assistant Professor in the Department of Humanities and Social Sciences, Bahria University, Islamabad. The authors can be reached at hussainsyedscholar@gmail.com.

telecommunications, government services, and defence operations, depends on extensive digital connections. The nation faces increased dangers because of its extensive network dependencies. The banking sector experienced 114 % increase in cyber incidents during 2024 because of ransom ware attacks and phishing schemes.[1] The attacks against critical infrastructure systems result in service disruptions, which simultaneously damage public confidence and weaken national power.

Security experts worldwide now prioritize cyber security as their primary research subject. According to Denning, security threats now encompass digital intrusions and network disruptions in addition to traditional kinetic warfare. The strategic importance of these threats increases for Pakistan because it operates as a nuclear power in a critical geographic area. The compromise of government databases together with military communications and financial systems threatens to harm national sovereignty while reducing deterrence capabilities and creating unstable decision-making processes.

This article addresses three main questions. First, what are the key cyber threats facing Pakistan's critical infrastructure? Second, how do weak institutions and external factors amplify these vulnerabilities? Third, what essential reforms can fortify Pakistan's cyber resilience?

Qualitative exploratory method is employed, which incorporates secondary data from policy documents, academic studies, and incident reports.[2] The data are organized into thematic categories that separate threats based on their sector and actors' involvement. A detailed analysis connects findings to the theories of securitization, deterrence, and resilience. The study infers how Pakistan frames cyber threats and what measures are needed to build a stronger cyber defence posture. It also delves into facets of cyberspace connecting to hybrid warfare and its impact on the national security paradigm.

Literature Review

The field of cyber security research has become essential for International Relations (IR) and security studies because of its growing importance in recent years. Cyber security is now widely recognised as a domain that affects state sovereignty, strategic competition, and global governance systems. The initial research treated cyberspace as a technical domain, but subsequent studies established its role as a vital arena for power deployment. The security concept of securitisation theory by Buzan, Waever, and de Wilde demonstrates how political leaders transform issues into security threats through their definition of existential threats. This theoretical framework helps Pakistan understand why cyber threats do not receive equal priority to kinetic or nuclear threats.

Scholars have attempted to adapt classical deterrence theory to cyberspace. Nye explains that cyber deterrence faces three major challenges, which include the inability to identify attackers, the problem of matching retaliation to the severity of attacks, and the unbalanced expense structure. Tikk and Kerttunen explain that punishment-based deterrence proves ineffective because cyber attackers remain anonymous. The authors support the use of denial-based deterrence for Pakistan and other states because it focuses on making attacks more difficult to execute. Findings on denial strategies emphasise that organizations need to focus on cyber hygiene practices, develop incident response systems, and build resilience capabilities.[3] Evidence shows Pakistan has weak cyber security capabilities, mainly in healthcare and government sectors, yet its finance and telecommunications sectors show better development because of regulatory needs and private sector funding.

The theory of hybrid warfare extends this analysis by showing how cyber operations function as part of complete statecraft methods. According to Hoffman, hybrid warfare combines cyber operations with propaganda and covert operations and conventional military pressure to create adversary weaknesses without starting open conflict. This concept applies directly to the South Asian region. Multiple researchers have shown that India uses cyber warfare as a component of its long-term security strategy against Pakistan. The authors, Umair and Akhtar, explain that espionage operations have focused on attacking government facilities and defense organizations and essential infrastructure, including power grid systems.[4] The attacks occur in clusters with propaganda operations, which indicate a hybrid warfare strategy for destabilization purposes. Research indicates that India-Israel cyber security cooperation has quickened the development of Indian offensive cyber capabilities.[5] The strategic stability of Pakistan faces challenges because of the technical expertise and malware development, and threat intelligence sharing that result from this alliance.

The literature shows that global powers actively participate in defining the cyber domain while researchers study their influence. Kania explains how China works to achieve cyber dominance through state-backed industrial development alongside military advancements.[6] The United States has established persistent engagement as its standard approach through Cyber Command, which now performs offensive operations that stay below war thresholds.[7] Research thus demonstrates that Pakistan operates within a disputed cyber environment that extends from regional to global levels. The domestic Pakistani literature points to institutional and policy weaknesses as the main obstacles that prevent the country from achieving cyber resilience.

Yamin explains that Pakistan lacks a single authority that can unite different stakeholders for coordination purposes.[8] The Prevention of Electronic Crimes Act (PECA) 2016 receives extensive discussion, but multiple studies show it does not provide sufficient protection. The law contains ambiguous definitions and broad powers that enable illegal activities, yet fails to protect against sophisticated cyber threats, according to Rehman (2019).[9] The authors Imran and Murtaza explain that Pakistan faces a shortage of skilled digital forensics and incident response experts because it does not have enough qualified personnel.[10] RSIL think tank reports show that CERT Rules have established legal definitions, but the process of implementing these rules continues at a slow pace.[11] Evidence indicates that Pakistan creates laws and policies yet struggles to execute them properly.

Specific sectors study provides additional detailed insight. Shaikh and Kiran studied Pakistan's telecom networks to find that PTA regulations failed to protect systems from distributed denial-of-service (DDoS) attacks.[12] Financial sector research demonstrates that banks have established numerous security operations centres (SOCs), yet ongoing breaches prove their security capabilities are not equally distributed.[13] The healthcare sector received minimal research attention until ransom ware attacks on hospital networks demonstrated its weak security position. Global research supports these findings: ENISA notes that healthcare has become one of the top three targeted sectors in Europe, suggesting a global trend likely to affect Pakistan further.[14] Industrial control systems and manufacturing also appear exposed due to supply chain vulnerabilities, a topic raised by Stevens in relation to global industrial espionage.[15]

Over-reliance on foreign technologies is yet another theme in the available literature. Fair and other scholars indicate that importing strategic technologies creates systemic risks because foreign entities can embed vulnerabilities and secret entry points into systems.[16] Pakistan’s telecommunications and IT infrastructure depends heavily on foreign vendors, which continues to threaten national sovereignty. It gets further complicated by geopolitical alignments while Western, Chinese, and other regional actors exert their influence on Pakistan’s digital ecosystem. The development of domestic research capabilities serves as a solution to reduce dependence on foreign technology, according to experts.

Comprehensive resolution of Pakistan's cyber threats requires both regional cooperation and active participation in international standard-setting processes. Greenwald and subsequent research on surveillance operations demonstrate that countries need to establish an equilibrium between their national authority and individual privacy protection.[17] International frameworks such as the Tallinn Manual serve as an

interpretive tool but lack any mechanism to enforce their guidelines. The South Asian region faces minimal cooperation because of ongoing political conflicts between its member states.

Theoretical Framework

This study applies securitisation theory, cyber deterrence and resilience frameworks, and hybrid warfare concepts to analyse Pakistan's cyber challenge. The Buzan-Waever-de Wilde securitisation theory states that political leaders must declare an issue as an existential threat to make it a security concern that warrants special measures.[18] National Cyber Security Policy 2021 of Pakistan identifies cyber defence as vital, yet it does not establish cyber security as a fundamental national security concern.[19] The field of cyber security receives insufficient funding and lacks institutional power to match the level of support dedicated to counterterrorism and nuclear security initiatives.

The traditional approach of deterrence aims to stop attacks through punishment mechanisms. The lack of clear attribution in cyberspace makes retaliation efforts through punishment ineffective, according to Tikk and Kerttunen.[20] According to Kosseff, states with restricted offensive capabilities should adopt deterrence by denial strategies, which enhance system defenses to minimize attack success rates.[21] The concept of cyber resilience builds upon traditional recovery methods by focusing on post-attack adaptation because Pakistan needs this capability to handle ongoing hostile cyber operations.[22]

Hybrid warfare uses conventional and unconventional methods, which include cyber operations and disinformation campaigns.[23] The region of South Asia uses cyber operations as an inexpensive tool to achieve state goals without triggering complete warfare. The activities of Indian state-backed groups who attack Pakistani military and government networks demonstrate this pattern.[24] The analysis of such operations through hybrid warfare principles demonstrates how cyber-attacks aim to weaken Pakistan's ability to make strategic decisions and produce enduring instability.

Major Sectors – Cyber Application in Pakistan
Findings – Finance Sector

The financial sector of Pakistan stands as a prime target for cybercriminals because it offers both high value and weak security defenses. Financial institutions become targets because they manage both monetary assets and protect sensitive customer information.[25] The number of reported cyber bank attacks in Pakistan increased by 114% during 2024 because attackers used ransom ware to disable digital banking operations and execute phishing schemes to obtain customer login information.[26] A combination of banking

trojans and account-draining viruses has resulted in major financial losses and damaged the reputation of affected institutions.

Advanced Persistent Threat (APT) groups such as Lazarus and SideWinder have started to target financial networks through persistent attacks, which experts believe receive backing from state actors.[27] The attacks maintain extended periods of operation while stealing data secretly and threaten to disrupt payment systems. The political nature of these cyber-attacks elevates their impact on national security because financial instability leads to economic instability, which produces broader socio-political effects.

Most Pakistani banks maintain outdated systems because they spend minimal funds on network security measures. The current incident response practices at financial institutions operate on a delayed basis, while most organizations fail to perform penetration testing or red-team simulations.[28] Absence of proper cyber hygiene training makes employees vulnerable to phishing and social engineering attacks, which succeed at high rates.

The financial sector of Pakistan needs to establish multi-layered security systems while improving real-time threat detection and enhancing cooperation with Pakistan Computer Emergency Response Team (PakCERT) and worldwide cyber threat-intelligence organizations to mitigate system weaknesses. The State Bank of Pakistan needs to enforce mandatory breach reporting, conduct risk assessments, and impose regulatory requirements to enhance both system resilience and public confidence.

Findings – Telecommunications Sector

The telecommunications sector functions as a fundamental digital transformation enabler for Pakistan, but cybercriminals and state-sponsored actors focus their attacks on this sector. Fast-growing internet connectivity and mobile penetration rates in Pakistan have made the telecom sector an appealing target for cybercriminals and state-sponsored actors.[29] PTA documented 200 ransom ware attacks on critical systems and 300 DDoS attacks that overloaded networks, 720 malware campaigns for data theft, and 550 phishing attacks that exploited human weaknesses during 2023.[30] A wide range of threats demonstrates the essential role of telecom infrastructure as a strategic target for attackers.

Telecom networks serve dual purposes because they support both civilian communication needs and defense and government operational requirements. The disruption of telecom infrastructure networks disrupts military command systems, public emergency response communications, and economic transaction processes. National telecom Computer Emergency Response Team (CERT) and National telecom Security

Operation Centre (SOC) of Pakistan have made progress, according to Yamin, yet these institutions need more capacity and automated threat detection systems to function effectively.[31]

Security vulnerabilities in telecom networks stem from using outdated equipment and foreign-made network hardware, which present potential security weaknesses and entry points. Difficulties are encountered when trying to establish uniform security protocols that all providers must follow. Shaikh and Kiran state that weak policy enforcement exists because mandatory breach reporting is absent and public-private stakeholder coordination remains insufficient.[32]

Pakistan needs to allocate funds for next-generation intrusion detection systems, SOC capacity expansion, and incident response protocol development to reduce security threats. Real-time threat intelligence sharing between public and private entities should be established through formal public-private partnerships. PTA should establish mandatory security audits and compliance requirements to enhance the overall security posture of telecom establishments.

Findings – Government and Military Sector

The government and military sectors stand as the main targets for cyber espionage operations because their stored information contains highly sensitive data. Multiple instances have shown that high-ranking officials, together with essential state systems, have become victims of cyber-attacks. Federal Board of Revenue (FBR) suffered a major breach in 2021, which exposed millions of taxpayer records and required the agency to shut down its systems temporarily.[33] Stolen information appeared on dark-web marketplaces for sale, which demonstrated the financial value of these attacks and created enduring threats to identity theft and fraud activities.

Advanced Persistent Threat (APT) groups have launched attacks against military networks and strategic assets. The "Confucius group" and other espionage actors alongside this group have been identified by Umair and Akhtar as state-linked Indian hackers who have repeatedly attempted to breach military communications and defence research facilities.[34] Such operations focus on obtaining strategic intelligence while simultaneously targeting command systems to weaken Pakistan's military capabilities.

The state faces difficulties in responding to cyber threats because it lacks a single national cyber security authority and suffers from poor inter-agency coordination.[35] Different ministries operate independently for incident response, while there exists no established system to exchange classified cyber threat intelligence between military and

civilian agencies. Improving Pakistan's cyber security architecture will require learning from established national bodies in the US/UK to design a more cohesive central authority.[36] Protection of sensitive systems requires immediate implementation of red-team exercises and mandatory cyber hygiene training for government personnel and secure communication standards.

Findings – Healthcare Sector

The healthcare industry in Pakistan has proven to be one of the most vulnerable domains for cyber-attacks. Healthcare systems maintain extensive patient data collections while using networked systems to perform diagnostic tests, schedule treatments, and deliver critical care services.[37] A combination of valuable patient data and essential networked systems makes healthcare facilities prime targets for ransom ware attackers and state-sponsored cybercriminals.

Multiple ransom ware attacks have targeted Pakistani healthcare facilities in recent years, which have caused operational disruptions and extended patient treatment times. The attackers prevent healthcare personnel from accessing vital systems through lockouts before they request payment for system access restoration. Research by Ali and Ahmad (2022) shows that healthcare data breaches lead to two major consequences: they compromise patient privacy while creating immediate dangers to human survival through delayed emergency care and treatment delays.[38] Medical record theft enables two major threats to occur because it allows insurance scams and black-market trading of personal health information.

The healthcare sector faces three main cyber security challenges because of its outdated technology infrastructure, insufficient access controls, and insufficient cyber security professionals. The majority of healthcare facilities operate without IT security teams and incident response protocols.[39] Absence of proper security measures makes it easier for attackers to execute phishing schemes and introduce malware into the systems.

Healthcare organizations need official critical infrastructure status to build their cyber resilience. All healthcare organizations need to follow three mandatory requirements, which include security audits, cyber hygiene training for staff, and national CERT system integration. Healthcare organizations need to invest in secure backup systems and encryption technologies to minimize ransom ware attack effects and maintain uninterrupted patient care operations.

Findings – Manufacturing and Industrial Sector

The manufacturing and industrial sector of Pakistan is increasingly dependent on digital systems, which include Industrial Control Systems (ICS) and Operational Technologies (OT). Digitalization has brought productivity growth to these sectors, but it has simultaneously introduced substantial cyber security threats, according to Khan and Rahman (2021).[40] Cyber-attacks on ICS can disrupt production lines, halt supply chains, and cause large-scale financial losses. The number of ransom ware attacks and APT intrusions against manufacturing systems has increased over the past few years. Attackers employ extortion tactics to block control network access and then demand ransom payments for system restoration.[41] Theft of proprietary information and trade secrets during these attacks creates a competitive disadvantage for Pakistani manufacturers.

Manufacturing and industry face security risks because it depends on outdated legacy systems and lack sufficient cyber security infrastructure and specialized ICS security expertise.[42] Lack of system redundancy in organizations makes them vulnerable to extended operational disruptions and damage to their reputation after a single security breach.

Defense against industrial cyber threats requires three essential measures: ICS and OT system modernization, network segmentation, and continuous monitoring for abnormal system behaviour.[43] A defensive strategy against industrial cyber threats requires industry-wide awareness programs and government agency partnerships to establish coordinated protection measures.

External Actors and Hybrid Warfare

External actors also play a critical role in shaping Pakistan's cyber security threat landscape. India, Israel, Iran, China, and the United States maintain active cyber programs that directly or indirectly affect Pakistan. The regional cyber environment becomes unstable because external actors interact with each other through their developing alliances and their implementation of hybrid warfare tactics.

India's Offensive Cyber operations have grown substantially throughout the last ten years. International cyber security firms have documented that Indian state-linked Advanced Persistent Threat (APT) groups ***SideWinder***, ***Confucius,*** and ***Patchwork*** have repeatedly attacked Pakistani government, defense, and financial networks.[44] The operations of these groups include spear-phishing attacks, malware implantation, and extended data extraction operations. The National Cyber Coordination Centre and Defence Cyber Agency of India have developed both defensive and offensive cyber

capabilities, according to scholars who study India's cyber power doctrine.[45] The pattern of attacks against Pakistan indicates that India seeks to gather intelligence while attempting to disrupt decision-making processes and critical system operations when bilateral relations become strained.

Beyond India, regional dynamics also add complexity. The Gulf and South Asia have been targets of Iranian cyber espionage operations that focus on energy infrastructure and telecommunication providers.[46] The number of reported incidents against Pakistan remains low, but Iran's past cyber activities in the region and its current operational capabilities make its cyber operations a possibility. China functions as a dual role entity because it serves as both a strategic ally and a potential security risk. Technical assistance and training provided by China to Pakistan includes cooperation on safe city surveillance systems and joint cyber defense research initiatives. On the other hand, reliance on Chinese hardware and network components raises concerns about potential backdoors and dependency risks.[47]

The United States operates extensive cyber warfare capabilities, which it traditionally uses for counterterrorism and strategic influence operations. The Edward Snowden revelations about U.S. surveillance programs showed that Pakistan's communications were under extensive monitoring by the United States.[48] This creates challenges for trust and complicates Pakistan's alignment in global cyber governance debates.

Cyber security environment also develops through the formation of alliances between nations. *India's growing cyber security cooperation with Israel* is a notable development in this context. Israel is a recognised global leader in cyber offensive and defensive technologies, and its collaboration with India includes joint ventures in cyber security R&D, information sharing, and capacity building.[49] Partnership between India and Israel enables India to execute sophisticated cyber operations, which also affect regional security dynamics, especially its application against Pakistan.

The concept of *hybrid warfare* serves as an effective method to analyse these security dynamics. State actors use hybrid warfare to achieve strategic goals through coordinated conventional and non-conventional methods, which include cyber-attacks, disinformation, and economic disruptions, while avoiding direct military confrontation.[50] State actors launch cyber-attacks during political or military crises to maximize their disruptive effects. For instance, spikes in malicious cyber activity targeting Pakistan have coincided with episodes of cross-border tensions with India, suggesting a coordinated psychological and strategic effect.[51]

The *involvement of external actors* raises several national security concerns. Firstly, continuous cyber espionage by foreign entities threatens to expose vital information, which reduces Pakistan's strategic autonomy. Secondly, the offensive cyber operations against critical infrastructure serve as a potential tool for both coercion and pre-emptive strikes during military conflicts. Thirdly, the involvement of multiple foreign actors in the region makes false-flag operations more likely, which complicates attribution and potentially triggers unintended escalation.

Pakistan needs to improve its threat intelligence operations and develop better attribution systems through technological advancements and international partnerships to protect itself from these security threats. The development of confidence-building measures requires diplomatic efforts between nations to stop accidental conflicts from occurring. The Government of Pakistan needs to establish multiple technology sources to decrease its dependence on foreign suppliers and perform complete security assessments on all imported systems. Pakistan's cyber strategy needs to include hybrid warfare threats as an explicit element, which will enable military and civilian forces to coordinate their responses effectively during defense operations.

Synthesis of Findings - Sectoral Cyber Threat Landscape

Findings from sectoral analysis indicate that Pakistan faces an advanced and diverse cyber threat landscape. Pakistan has not established cyber security as a core national security matter. The government continues to respond to security breaches through reactive measures instead of strategic planning because cyber security has not achieved full securitization status.

From the perspective of deterrence theory, results indicate that Pakistan faces limited success with deterrence through punishment because of difficulties in attributing attacks and restricted offensive capabilities.[52] Implementation of deterrence by denial shows promise, but its effectiveness varies between different sectors. Security operations centres exist in financial and telecom institutions, yet healthcare organizations and government entities have not established similar facilities. Pakistan's Cyber resilience remains weak, as shown by prolonged outages after incidents such as the Federal Board of Revenue breach.[53]

The hybrid warfare framework demonstrates that cyber-attacks function as part of an extensive range of state-to-state competitive activities. Indian-linked APT group SideWinder has conducted attacks on military and government systems to acquire strategic intelligence and disrupt decision-making processes, according to Umair and

Akhtar (2022).[54] These campaigns are deliberately designed to remain below the threshold of conventional conflict, complicating response options for Pakistan.

The systemic nature of vulnerabilities across sectors indicates that Pakistan's cyber weaknesses are structural rather than incidental. A combination of outdated systems, inefficient inter-agency cooperation, and insufficient policy enforcement continues to persist as major issues. Finance and telecom sectors have private sector cyber security programs, but these programs fail to connect effectively with official government response efforts. The healthcare sector and government sector experience delayed response times and poor situational awareness because they lack mandatory reporting requirements and unified response protocols.

Cyber security governance framework becomes more vulnerable to strategic threats because of its fragmented structure. A combination of geopolitical dynamics with cyber-attacks creates a risk of mistaken escalation, which could start an unanticipated crisis. This is particularly dangerous given the fragile escalation control dynamics in South Asia.[55] A National Cyber security Authority with central authority would solve the governance problem by unifying incident response operations and establishing a security protocols uniting civilian and military cyber defense systems.

Finally, capacity building emerges as a crucial requirement. Shortage of cyber security experts in Pakistan prevents the country from deploying advanced defensive measures for its security.[56] Developing a cyber-aware workforce and integrating cyber security into education and training programs are necessary steps to ensure that institutional reforms are sustainable.

Policy and Institutional Gap Analysis

Weak Inter-Agency Coordination

One of the most significant gaps in Pakistan's cyber security framework is weak inter-agency coordination. Cyber security responsibilities are spread across multiple ministries and departments, including the Ministry of Information Technology and Telecommunication (MoITT), Pakistan Telecommunication Authority (PTA), National Telecommunication Corporation (NTC), and military cyber units. Fragmented decision-making structures between agencies create isolated decision systems that prevent the development of a unified national cyber security strategy. Lack of defined incident response protocols between agencies leads to delayed responses during security incidents because no clear authority exists to direct actions.

Lack of a central coordinating body also prevents stakeholders from exchanging threat intelligence data in a systematic manner. Delayed sharing of cyber incident reports from private financial institutions to law enforcement and military cyber defence units enables wider cyber compromise. FBR breach in 2021 demonstrated the importance of early detection through better information sharing between agencies.[57]

A national cyber command or central cyber security agency should be established according to international best practices to achieve government-military-private sector coordination.[58] Absence of coordinated efforts between agencies makes Pakistan's cyber security response slow and uncoordinated. A unified command system enables organizations to make swift decisions and execute joint training exercises, and maintain public confidence through coordinated crisis communications.

Addressing this gap needs proper legislation to create a "lead agency" that will control cyber security policy and operational authority. The agency must have legal authority to compel information sharing, conduct national-level cyber drills, and coordinate cross-sector response. It should function as one window for international stakeholders, thereby enhancing Pakistan's participation in global cyber operations and early warning networks.

Lack of Domestic CERT Capacity

PakCERT functions as the national Computer Emergency Response Team under MoITT, but its operational capabilities, technical resources, and human resources are insufficient to address the current security challenges. The organization focuses on issuing security alerts and conducting basic awareness programs as its main activities. Incident response capabilities of PakCERT remain underdeveloped since it lacks real-time capabilities to detect, analyse, and mitigate complex threats.[59]

In comparison, mature CERTs in other countries operate 24/7 Security Operations Centres (SOCs), which enable them to maintain threat intelligence feeds while coordinating responses to major incidents. PakCERT also faces challenges because it does not have modern forensic labs, lacks malware analysis capabilities, and experts who can reverse engineer APT toolkits. This creates a dependence on foreign cyber security firms for threat analysis, delaying response times and raising sovereignty concerns.

Enhancing CERT capacity will require significant investment in infrastructure, recruitment, and training. A public-private partnership model could be used to share expertise between the private sector and the government. Regional CERT coordination with friendly countries could also provide early warning of cross-border cyber campaigns.

Ultimately, a fully operational PakCERT must serve as the nerve centre of Pakistan's cyber defence posture, capable of detecting and responding to incidents across all critical sectors in real time.

Over-Reliance on Foreign Technology

Foreign technology dependence represents a fundamental weakness in Pakistan's cyber security system. Most of the essential infrastructure equipment, security systems, and software products enter Pakistan through imports, which creates a threat to supply chain security. Dependence on foreign technology systems creates an opportunity for foreign entities to embed backdoors / hidden security weaknesses and conduct surveillance operations.[60] It also exposes Pakistan to export controls and sanctions that could disrupt its access to critical technology during conflicts/crises.

The telecom sector depends on foreign vendors for its infrastructure needs, especially because it uses Chinese-made equipment. Affordable solutions from these vendors create dependency issues, while their control over system vulnerabilities remains a concern. The banking sector also depends on foreign-made core banking software and security platforms for its operations.

Dual strategic risk emerges from these dependencies: first, zero-day vulnerabilities in popular foreign products that adversaries can use for attacks, and second, Pakistan's inability to independently protect its systems because it depends on foreign technical support. Scholars argue that digital sovereignty requires states to build indigenous capability in key technologies such as encryption, authentication systems, and secure hardware.[61]

Policy response should encompass three key measures to address this issue by promoting supplier diversity, conducting security screening on all imported devices, and establishing domestic research and development facilities. Establishment of local cyber security start-ups through incentive programs will help Pakistan decrease its dependence on foreign technology in the long run. Pakistan should also collaborate with friendly nations to develop open-source, transparent security solutions that enhance trust and verifiability.

Legislative Gaps beyond PECA 2016

The Prevention of Electronic Crimes Act (PECA) 2016 serves as Pakistan's main cybercrime law, but it does not comprehensively address modern cyber threats effectively. PECA 2016 mainly criminalizes three specific online offenses, which include hacking, data

theft, and online harassment. The legislation fails to establish a complete system for safeguarding essential information systems, and it lacks requirements for breach disclosure and international cooperation.[62]

The law faces criticism because its ambiguous language enables potential misuse, which threatens both privacy rights and free speech protections.[63] The law also struggles to establish specific roles and duties for different entities that manage cyber security governance. This creates legal uncertainty during incident response, where questions of jurisdiction and liability can delay mitigation efforts.

Various nations across the world have passed updated cyber laws that require organizations to report incidents, establish response protocols, and protect vital infrastructure systems. Pakistan lacks such provisions, leaving gaps in national preparedness. The Government of Pakistan needs to move fast on cyber security legislative reforms, which can protect critical infrastructure. Creation of a central cyber security authority is therefore essential, which can implement privacy standards that match global standards such as GDPR. Such reforms must strike an equilibrium between security needs and civil liberties to establish public trust and stimulate responsible information exchange from private companies.

Summary Table: Sectoral Threats, Impacts, and Policy Gaps

Sectors	Key Threats & Actors	Impact on National Security	Policy Gaps / Suggested Responses
Finance	Ransom ware, phishing, APT groups (Lazarus, SideWinder)	Financial instability, disruption of payment systems	Mandatory breach reporting, stronger CERT-bank coordination
Telecom	DDoS attacks, malware, phishing	Disruption of civilian and military communications	Automated SOC upgrades, standardised security compliance
Government & Military	Espionage, FBR breach, APT infiltration	Loss of classified data, weakened deterrence	Centralised cyber authority, inter-agency intelligence sharing
Healthcare	Ransom ware, APT exfiltration	Risk to patient safety, data privacy breaches	Designation as critical infrastructure, security audits
Manufacturing / ICS	ICS ransom ware, data theft	Supply chain disruption, economic losses	Modernise ICS, network segmentation, and mandatory reporting

Final Thoughts

Based on these findings, several key policy implications emerge. The priority is to establish a National Cyber security Authority with clear legal authority and budgetary

independence.[64] This body should coordinate threat intelligence, standard-setting, and incident response across public and private sectors.

All critical sectors need to establish mandatory breach reporting requirements. Implementation of reporting requirements for incidents has proven successful in other nations because it enables faster threat detection and intelligence collection.[65] The State Bank of Pakistan and Pakistan Telecommunication Authority need to establish time-based incident disclosure requirements for financial institutions and telecom providers.

Cyber operations capacity building is another central pillar. Development of specialized cyber security programs at universities should be accompanied by government funding for professional certification programs to support skill development.[66] Cyber training programs should focus on the healthcare and manufacturing sectors because these industries demonstrate minimal understanding of cyber security threats.

The current level of technical investments needs expansion to achieve the desired results. Organizations need to replace their outdated systems with modern security-focused infrastructure. Security Operations Centres (SOC) need round-the-clock dedicated staff presence for all critical sectors to operate, while these organizations must implement intrusion detection systems and perform penetration testing on a regular basis. Public procurement policies should prefer suppliers compliant with ISO 27001 and similar international standards.

International cooperation also stands as an essential requirement. The country needs to join regional confidence-building initiatives and work with the ITU and other global cyber security organizations to enhance threat attribution and exchange security best practices.[67] Such engagement reduces the risk of miscalculation and enables early warning of emerging threats. A national awareness program needs to start immediately to educate citizens about proper cyber safety practices. The public needs to receive information about secure online practices and multi-factor authentication methods through awareness campaigns.

The current legal framework of Pakistan requires immediate revision. Prevention of Electronic Crimes Act (PECA 2016) needs revision to protect critical infrastructure and establish clear procedures for international cooperation.[68] Implementation of clear regulations will help prevent misuse while protecting privacy and building trust between public entities and private stakeholders. These proposed measures need continuous political backing, effective legislation, and financial support to achieve their long-term advantages, which include enhanced national security, economic stability, and

international credibility. Cyber security must be treated as a national priority on par with traditional defence and economic policy.

Conclusion

Pakistan currently faces a decisive point in its Cyberspace development. National security strategy requires cyber security to become an essential foundation. A complete national effort that unites political direction with institutional changes, technical development, and public education will enable Pakistan to shift from its current defensive stance to a resilient security position. Protecting critical infrastructure and sensitive data through these measures will simultaneously boost Pakistan's strategic stability and digital domain credibility.

References

[1] Shahid Raza and Qamar Abbas, "Financial Cybercrime in South Asia: An Analysis of Trends and Countermeasures," International Journal of Cyber Criminology 17, no. 1 (2023): 89–112.

[2] Babar Aslam and Muhammad Tariq, "Cyber Threats and Incident Response Capability: A Case Study of Pakistan," in Proceedings of the 2nd National Conference on Information Assurance (NCIA) (December 2013).

[3] IBM Security X-Force, X-Force Threat Intelligence Index 2024 (Armonk, NY: IBM, 2024), https://www.ibm.com/think/x-force/2024-x-force-threat-intelligence-index.

[4] Muhammad Umair and Rabia Akhtar, "Cyber-Espionage and the Politics of Information Security in South Asia," Asian Journal of Political Science 30, no. 1 (2022): 89–107.

[5] Pankaj Kumar and Meenakshi Jain, "India–Israel Cooperation in Cybersecurity: Strategic and Technological Implications," Strategic Analysis 44, no. 4 (2020): 311–325.

[6] Elsa Kania, "China's Strategic Thinking on Building Power in Cyberspace," China Brief 19, no. 6 (2019): 12–17.

[7] Jon Lindsay, "The Impact of Persistent Engagement on International Order," International Security 45, no. 3 (2020): 123–163.

[8] Tughral Yamin, "Cyberspace Management in Pakistan," Governance and Management Review 3, no. 1 (2018): 12–17.

[9] Fauzia Rehman, "Legal Analysis of the Prevention of Electronic Crimes Act: Issues and Challenges," Pakistan Law Review 8, no. 1 (2019): 77–94.

[10] Muhammad Imran and Ghulam Murtaza, "The Rise of Cyber Crime in Pakistan: A Threat to National Security," Journal of Development and Social Sciences 3, no. 4 (October–December 2022): 631–640.

[11] Research Society of International Law (RSIL), "Strengthening the Legal Framework for Cybersecurity in Pakistan: The CERT Rules 2023," Policy Brief (Islamabad, 2023).

[12] Hina Shaikh and Rabia Kiran, "Telecommunication Networks and Cybersecurity Risks in Pakistan: Policy and Practice," *Pakistan Journal of Social Sciences* 40, no. 2 (2020): 233–248.

[13] Muhammad Rizwan, "The Cyberthreat in the Contemporary Era: Challenges for the Security of Pakistan," *The Rest Journal* (February 1, 2022).

[14] European Union Agency for Cybersecurity (ENISA), Health Threat Landscape (Athens: ENISA, 2023), https://www.enisa.europa.eu/publications/health-threat-landscape.

[15] Tim Stevens, "Cyberweapons: An Emerging Global Security Challenge," Survival 55, no. 5 (2013): 107–120.

[16] Christine Fair, In Their Own Words: Understanding the Lashkar-e-Tayyaba (Oxford: Oxford University Press, 2020).

[17] Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (New York: Metropolitan Books, 2014).

[18] Barry Buzan, Ole Wæver, and Jaap de Wilde, Security: A New Framework for Analysis (Boulder, CO: Lynne Rienner, 1998).

[19] Government of Pakistan, National Cyber Security Policy 2021 (Islamabad: Ministry of Information Technology and Telecommunication, 2021).

[20] Eneken Tikk and Mika Kerttunen, "Cybersecurity and State-Sponsored Threats: The Case of Advanced Persistent Threats," Journal of Cyber Policy 3, no. 3 (2018): 339–360.
[21] Jeff Kosseff, "Cybersecurity and National Security: The Role of Deterrence," Journal of National Security Law & Policy 9, no. 2 (2018): 123–148.
[22] Mandiant (Google Cloud), *M-Trends 2024: Our View from the Frontlines* (2024), https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2024.
[23] Tim Stevens, "Cyberweapons: An Emerging Global Security Challenge," Survival 55, no. 5 (2013): 107–120.
[24] Muhammad Umair and Rabia Akhtar, "Cyber-Espionage and the Politics of Information Security in South Asia," Asian Journal of Political Science 30, no. 1 (2022): 89–107.
[25] Shahid Raza and Qamar Abbas, "Financial Cybercrime in South Asia: An Analysis of Trends and Countermeasures," International Journal of Cyber Criminology 17, no. 1 (2023): 89–112.
[26] Irfan Ullah and Muhammad Imran, "Cybersecurity Challenges in the Banking Sector of Pakistan: A Rising Concern," Journal of Information Security Research 10, no. 2 (2024): 45–63.
[27] Eneken Tikk and Mika Kerttunen, "Cybersecurity and State-Sponsored Threats: The Case of Advanced Persistent Threats," Journal of Cyber Policy 3, no. 3 (2018): 339–360.
[28] Talha Waqar and Ammar Malik, "Financial Fraud and Cybercrime in Pakistan's Banking Sector: An Analytical Review," South Asian Journal of Business Studies 11, no. 1 (2022): 121–138.
[29] Hina Shaikh and Rabia Kiran, "Telecommunication Networks and Cybersecurity Risks in Pakistan: Policy and Practice," *Pakistan Journal of Social Sciences* 40, no. 2 (2020): 233–248.
[30] Aqdas Malik, "Cyberattacks on Telecommunications Infrastructure: Emerging Trends in Developing Countries," Telecommunications Policy 46, no. 6 (2022): 1–12.
[31] Tughral Yamin, "Cyberspace Management in Pakistan," Governance and Management Review 3, no. 1 (2018): 12–17.
[32] Hina Shaikh and Rabia Kiran, "Telecommunication Networks and Cybersecurity Risks in Pakistan: Policy and Practice," *Pakistan Journal of Social Sciences* 40, no. 2 (2020): 233–248.
[33] Muhammad Rizwan, "The Cyberthreat in the Contemporary Era: Challenges for the Security of Pakistan," *The Rest Journal* (February 1, 2022).
[34] Muhammad Umair and Rabia Akhtar, "Cyber-Espionage and the Politics of Information Security in South Asia," Asian Journal of Political Science 30, no. 1 (2022): 89–107.
[35] Nazish Zafar and Abid Ali, "Cybersecurity Challenges and Prospects for Pakistan: An Analysis," Journal of Security Studies 12, no. 2 (2021): 45–63.
[36] International Bar Association, "Improving Pakistan's Cybersecurity Architecture Using US-UK Insights" (2024), https://www.ibanet.org/Improving-Pakistans-cybersecurity-architecture-US-UK-insights.
[37] Katherine Nicholas and Sherri Greenberg, "Ransomware in Hospitals: Emerging Threats to Patient Safety," *Journal of Medical Internet Research* 23, no. 10 (2021): e26575.
[38] Arshad Ali and Saeed Ahmad, "Cybersecurity Challenges and National Security in Pakistan: An Emerging Threat Landscape," Pakistan Journal of International Affairs 5, no. 2 (2022): 55–74.
[39] Hamid Asmat, Pakistan and Cyber Crime: Problems and Preventions (2019).
[40] Fawad Khan and Nadia Rahman, "Industrial Control Systems and Cybersecurity Challenges in South Asia," International Journal of Critical Infrastructure Protection 32 (2021): 100409.
[41] Talha Waqar and Ammar Malik, "Financial Fraud and Cybercrime in Pakistan's Banking Sector: An Analytical Review," *South Asian Journal of Business Studies* 11, no. 1 (2022): 121–138.
[42] Nadia Rahman and Imran Ullah, "Critical Infrastructure Protection in Pakistan: Energy and Transportation under Cyber Threats," International Journal of Critical Infrastructure Protection 34 (2021): 100427.
[43] Dragos, 8th Annual OT Cybersecurity Year in Review (2025), https://www.dragos.com/blog/dragos-8th-annual-ot-cybersecurity-year-in-review-is-now.
[44] Mandiant, "APT Trends Report 2023: South Asia Focus," Threat Intelligence Report (Reston, VA: Mandiant, 2023).
[45] Arindrajit Basu, "Foreign Cyber Espionage and Sovereignty: South Asian Perspectives," Journal of International Cybersecurity 3, no. 1 (2021): 44–61.
[46] FireEye, "Iran-Linked Cyber Espionage Campaigns Targeting the Middle East and South Asia," Threat Intelligence Report (March 2022).
[47] Elsa Kania, "China's Strategic Thinking on Building Power in Cyberspace," China Brief 19, no. 6 (2019): 12–17.
[48] Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (New York: Metropolitan Books, 2014).
[49] Pankaj Kumar and Meenakshi Jain, "India–Israel Cooperation in Cybersecurity: Strategic and Technological Implications," Strategic Analysis 44, no. 4 (2020): 311–325.
[50] Frank Hoffman, "Hybrid Warfare and Challenges," Joint Force Quarterly 80 (2018): 34–39.
[51] Hina Shaikh and Rabia Kiran, "Telecommunication Networks and Cybersecurity Risks in Pakistan: Policy and Practice," *Pakistan Journal of Social Sciences* 40, no. 2 (2020): 233–248.

[52] Eneken Tikk and Mika Kerttunen, "Cybersecurity and State-Sponsored Threats: The Case of Advanced Persistent Threats," Journal of Cyber Policy 3, no. 3 (2018): 339–360.

[53] Muhammad Rizwan, "The Cyberthreat in the Contemporary Era: Challenges for the Security of Pakistan," *The Rest Journal* (February 1, 2022).

[54] Muhammad Umair and Rabia Akhtar, "Cyber-Espionage and the Politics of Information Security in South Asia," Asian Journal of Political Science 30, no. 1 (2022): 89–107.

[55] Christine Fair, In Their Own Words: Understanding the Lashkar-e-Tayyaba (Oxford: Oxford University Press, 2020).

[56] Muhammad Imran and Ghulam Murtaza, "The Rise of Cyber Crime in Pakistan: A Threat to National Security," Journal of Development and Social Sciences 3, no. 4 (October–December 2022): 631–640.

[57] Muhammad Rizwan, "The Cyberthreat in the Contemporary Era: Challenges for the Security of Pakistan," *The Rest Journal* (February 1, 2022).

[58] European Union Agency for Cybersecurity (ENISA), Health Threat Landscape (Athens: ENISA, 2023), https://www.enisa.europa.eu/publications/health-threat-landscape.

[59] Tughral Yamin, "Cyberspace Management in Pakistan," Governance and Management Review 3, no. 1 (2018): 12–17.

[60] Elsa Kania, "China's Strategic Thinking on Building Power in Cyberspace," China Brief 19, no. 6 (2019): 12–17.

[61] Arindrajit Basu, "Foreign Cyber Espionage and Sovereignty: South Asian Perspectives," Journal of International Cybersecurity 3, no. 1 (2021): 44–61.

[62] Babar Aslam and Muhammad Tariq, "Cyber Threats and Incident Response Capability: A Case Study of Pakistan," in Proceedings of the 2nd National Conference on Information Assurance (NCIA) (December 2013).

[63] Fauzia Rehman, "Legal Analysis of the Prevention of Electronic Crimes Act: Issues and Challenges," Pakistan Law Review 8, no. 1 (2019): 77–94.

[64] Government of Pakistan, National Cyber Security Policy 2021 (Islamabad: Ministry of Information Technology and Telecommunication, 2021).

[65] European Union Agency for Cybersecurity (ENISA), Health Threat Landscape (Athens: ENISA, 2023), https://www.enisa.europa.eu/publications/health-threat-landscape.

[66] Jeff Kosseff, "Cybersecurity and National Security: The Role of Deterrence," Journal of National Security Law & Policy 9, no. 2 (2018): 123–148.

[67] Tim Stevens, "Cyberweapons: An Emerging Global Security Challenge," Survival 55, no. 5 (2013): 107–120.

[68] Babar Aslam and Muhammad Tariq, "Cyber Threats and Incident Response Capability: A Case Study of Pakistan," in Proceedings of the 2nd National Conference on Information Assurance (NCIA) (December 2013).