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

STRATEGIC AND STRUCTURAL CHALLENGES OF CYBER WARFARE IN PAKISTAN

Rimsha Malik[*1], Dr. Raziq Hussain[2]

[*1]*Associate Research Officer, Center for International Strategic Studies, AJK, Pakistan*
[2]*Assistant Professor, Department of International Relations, Muslim Youth University, Islamabad, Pakistan*

[*1]rimsham156@gmail.com

DOI: https://doi.org/10.5281/zenodo.20024801

Keywords

Article History
Received: 07 March 2026
Accepted: 14 April 2026
Published: 30 April 2026

Corresponding Author: *
Rimsha Malik

Abstract

The emergence of cyberspace as a strategic domain has transformed the nature of conflict, deterrence, and sovereignty. Unlike conventional warfare, cyber conflict operates through informational disruption, cognitive influence, and infrastructural penetration, often below the threshold of physical violence. For Pakistan, rapid digital expansion has not been matched by corresponding evolution in strategic thinking or institutional preparedness. This mismatch between traditional security paradigms and the non-linear dynamics of cyberwarfare creates structural vulnerabilities. This article examines the strategic and institutional gaps that hinder Pakistan's ability to establish a credible cyber deterrence posture. It addresses the absence of a coherent national cyber doctrine, fragmented governance structures, reactive policymaking, and limited inter-agency coordination. Grounded in cyber deterrence theory and strategic studies, the article employs qualitative analysis of documented cyber incidents, policy frameworks, cybersecurity indicators, and publicly reported influence operations targeting Pakistan. The findings suggest that Pakistan's cyber insecurity stems less from isolated technical weaknesses and more from systemic structural immobility. Recurrent data breaches, disinformation campaigns, and exploitation of unregulated digital platforms reveal a deterrence vacuum shaped by doctrinal ambiguity and weak institutional integration. The blurred boundary between domestic and foreign cyber threats further complicates strategic response mechanisms. The article concludes that cybersecurity must be reconceptualized as a core pillar of national security and strategic autonomy. Developing a unified cyber doctrine, strengthening institutional coordination, and embedding societal resilience into deterrence strategy are essential for reducing asymmetric vulnerabilities. More broadly, the analysis demonstrates that states unable to adapt structurally to the evolving logic of digital conflict risk gradual erosion of sovereignty in the contemporary security environment.

INTRODUCTION

Not only is modern combat distinct, but so is the very definition of risk. Power in this expanding field is based less on overt military might and territorial dominance and more on psychological sway, coded manipulation, and computational dominance. An ontological issue arises for Pakistan in the face of cyberwarfare, given the

country's ideological differences, rapid technological growth, and ongoing geopolitical instability. The problem, therefore, becomes how to comprehend war in general, not only how to fight, because deterrence is based on credibility, readiness, and perception rather than on force alone.

Instead of focusing on obvious issues like inadequate funding or weak firewalls, this chapter delves into the conceptual divide between the state's traditional strategic thinking and the demands of the digital era. Far more perilous than foreign penetration or data theft is Pakistan's reliance on security concepts from the 20th century, despite living in the technologically unpredictable 21st century. A lot worse is this structural immobility. In contrast to conventional conflict, which often ends in bloodshed, cyberwarfare rarely does. Rather, it ambushes society from behind, wreaking havoc by capitalizing on informational weaknesses and the opacity of established institutions. The loss of infrastructure and imagination is at the heart of Pakistan's most significant challenge.

It is not retaliation but rather the transmission of messages of cost, resilience, and uncertainty that constitute cyber deterrence. Reactions, rather than planning, continue to take precedence in Pakistan's strategic culture. The government fails to address the wider civil-societal, psychological, and economic consequences of digital incursions due to its sluggish threat recognition, disjointed regulatory frameworks, and cybersecurity policy that mainly targets military gear. Consequently, the main objective of this chapter is to shed light on a more fundamental strategic dilemma: the lack of a doctrine that can handle the uncertainty, non-linearity, and asymmetry that are hallmarks of cyberwarfare.

The porous border between Pakistani and foreign cyber threats makes an already difficult situation much worse. The weaponization of information ecosystems distorts the facts and threatens to manipulate the public's trust, a nation's most valuable security asset. Espionage, cybercrime, infrastructure destruction, and influence operations are all problems in Pakistan. But it still prioritizes reactive measures above proactive planning and continues to respond strategically in isolation. This school of thought argues that cyber insecurity is not just the result of technology failures, but rather is the result of a state's structural issues in adapting to the new reality of digital vulnerability rather than physical sovereignty.

Pakistan is at a crossroads in light of the growing competition for control of cyberspace as a strategic domain. Cyberattacks on government websites continue, exposing security flaws in the system. One such incident was in 2023, when sensitive information from the Federal Board of Revenue (FBR) was leaked on the dark web due to a cyberattack (ARY News, 2024). Such events reveal systemic flaws that endanger the state's digital sovereignty and stability, in addition to exposing technical vulnerabilities.

Since the 1990s, thanks to the proliferation of ICTs in Pakistan's government, businesses, and public services, the country's integration into the global information economy has picked up speed. But national cybersecurity capabilities have not evolved in tandem with this digital boom. Pakistan is vulnerable to numerous cyber threats, including espionage, data theft, disinformation, and digital sabotage, due to its lack of a thorough cybersecurity framework, even as the country is becoming more dependent on digital platforms. The spread of Trojanized mobile applications has further complicated the threat landscape. In 2021, Sophos Labs discovered phony copies of the Pakistan Citizen Portal, which secretly collect user data, spy on communications, and undermine national digital confidence (Sophos, 2021).

The fact that hostile foreign networks are actively taking advantage of Pakistan's unregulated cyber environment only makes the situation worse. The coordinated influence tactics against Pakistan have been continuously exposed in the EU DisinfoLab reports from 2020 to 2024 (EU DisinfoLab, 2020). These campaigns have made use of bogus media, forged NGO platforms, and algorithmic manipulation of internet narratives. This is a prime example of how hybrid warfare has taken over cyberspace, with enemies using tactics below the line of physical confrontation to undermine the legitimacy of states and destabilize them.

Examining the institutional, regulatory, and strategic gaps that have prevented Pakistan from establishing a credible cyber deterrent posture, this article delves into the structural and strategic obstacles that Pakistan is encountering in its quest to safeguard the cyber realm. Pakistan is still not prepared for cyber threats, as it does not have a cohesive national cyber doctrine, does not have specific coordination organizations, and relies on reactive measures instead of a proactive strategy.

Pakistan now has a deterrent vacuum, which its enemies are happy to fill by launching ongoing cyberattacks on government websites, phone networks, and public opinion polls.

Cyberspace has shifted from an afterthought to the center of strategic competition in this setting. This article delves into how Pakistan's present stance undermines its capacity to project deterrence and protect its national interests in the digital realm. It highlights how institutional fragmentation, technological limitations, and legal stagnation characterize Pakistan's current position. This article provides a solid groundwork for comprehending Pakistan's disproportionate vulnerability by drawing attention to these structural and strategic shortcomings. Cybersecurity is much more than just a technological concern; it is a cornerstone of national security and strategic autonomy.

Here we take a look at some important indexes, showcasing Pakistan's dedication to different digital frameworks, breaking down the impact of each framework's sub-pillars, and seeing what the country may do within each.

THEORATICAL FRAMEWORK

This article relies on the Cyber Deterrence Theory as its conceptual basis. It is based on the deterrence theory which was originally based on the classical nuclear strategy, where the deterrence theory focuses on preventing an act of hostility using credible threats of retaliation, proving capable, and exhibiting a will to such action. In the digital realm, cyber deterrence is applied to the sphere of cyberspace, which is low-visibility, visually changing technology, and blurry lines between government and non-governmental forces. Cyber Deterrence Theory postulates that three fundamental mechanisms, namely, capability, resilience and signaling, make an actor able to avert adversarial cyber acts.

Capability is defined as the defensive and offensive technical capabilities, such as the capability to identify, assign, and act in response to cyber intrusions. A state should have evident equipment, qualified human resources, and powerful infrastructure to demonstrate that any evil activities will be very expensive. Resilience is the ability to take, recover, and adjust to cyberattacks to reduce the possible strategic, economic, and social impact. A strong system will lessen the motive of the enemies as the attacks will not have a decisive benefit. Signaling involves communicating intention, norms and consequences to the potential aggressors. It can be done by use of policy statements, attending international cybersecurity forums, and apparent incident responses. The combination of these three pillars constitutes the core of cyber deterrence that allows the state to manipulate the cost-benefit analysis of adversaries and avoid escalation in the cyber sphere.

The Cyber Deterrence Theory is especially applicable to the situation of cybersecurity in Pakistan. Pakistan is a sophisticated threat environment with consistent state-sponsored attacks, non-state cybercrime, and advanced influence operations. Pakistan has a low level of strategic and institutional preparedness to counter the technological growth, despite high digital adoption. Cyber Deterrence Theory offers a systematic viewpoint to examine these loopholes and offers a framework through which gaps in capability, resilience, and signaling can be assessed in relation to the deterrence vacuum. Examples of these include repeated breaking of government websites, financial institutions, and digital infrastructure, which suggest the lack of technical infrastructure and human capacity, which diminishes deterrence by ability. Likewise, disjointed governance and poor inter-agency communication restrain the nation to overcome attacks and implement temporal policies on resilience. Besides, the lack of a single national cyber doctrine and inadequate presence in international cybersecurity forums reduces

legitimate signaling to adversaries, opening possibilities to perpetual cyber aggression.

The strategic aspect of cyber deterrence is also highlighted in this framework. In comparison with traditional deterrence that is based on the observable military capabilities, cyber deterrence has to exist in an opaque space where the effects of action are indirect and attribution is difficult. This is the case of Pakistan as it is through legal gaps, fragmentation in policies, and institution that cyber threats are used to the disadvantage. Using Cyber Deterrence Theory, this paper will place the technical and policy failures of Pakistan in a larger strategic framework that demonstrates how the structural and institutional immobility negatively affects the security of the country. It emphasizes the fact that cyber insecurity is not only a product of the lack of technology but also of the lack of clarity in doctrine, lack of development in the governance, and lack of the inclusion of cyber strategy in the national security architecture.

The theory also gives a normative reform guidance. Pakistan can enhance deterrence by taking proactive policy actions, according to its principles: the formation of a single cyber command unit, formalization of the inter-agency coordination framework, investment in qualified cyber professionals, and development of effective national response plans on incidents. Improvements to legal systems, the adoption of data protection laws and also involvement in regional and international cyber diplomacy efforts also help support signaling. Through the combination of these efforts, Pakistan will be able to develop a more plausible and holistic cyber deterrence stance that will mitigate exposure to asymmetric warfare, protect the digital sovereignty of the country, and harmonize national policy with emerging cyber conventions.

As discussed abow, the Cyber Deterrence Theory can be used as both an analytical and prescriptive approach to this study. Analytically, it can be made to analyze how the weaknesses in the structure of Pakistan, technological constraints and strategic environment interact to explain the deterrence deficit. In its prescriptive version, it implies taking practical measures to build capability, resilience, and signaling that will address vulnerabilities and improve national cybersecurity. Using Cyber Deterrence Theory as a foundation, this research places the cyber problems faced in Pakistan in a theoretical context, applying the technical, institutional, and strategic aspects of cyberspace in connection to the issue of national security.

1.1 Digital and Cybersecurity Index Assessment: Pakistan's standing

Table 1. List of Indexes and Pakistan's ranking

Serial No	Index / Indicator	Ranking of Pakistan
1	The ICT Development Index 2023	48.7 / 100
2	E-Government Development Index (EGDI) 2024	136/193
3	The Network Readiness Index Report 2023	90/121
4	Global Cybersecurity Index 2024	94/194
5	Global Digital Readiness Index 2021	120/146

Source: *Drawing data from the ICT Development Index 2023, E-Government Development Index 2024, The Network Readiness Index Report 2023, Global Cybersecurity Index 2024, and Global Digital Readiness Index 2021*

The exponential rise of internet accessibility and the information and communication technology (ICT) revolution are causing a fundamental upheaval in the present global scene. Although these innovations have brought about many new possibilities, they have also brought about many new complicated problems, the most prominent of which is an increase in highly sophisticated cyber threats. They vary from simple attempts at hacking to more sophisticated forms of criminality and, most concerning, the rise of cyberwarfare. Governments' economic and administrative

landscapes have been changed by the increasing reliance on digital technologies, which has also changed the security paradigms that sustain national stability.

There has been a meteoric rise in the usage of online service platforms and digital tactics for government and business in Pakistan. However, this transformation is occurring in the midst of a highly precarious security environment marked by internal vulnerabilities and regional hostility. This implies that there are still cyber threats that Pakistan could face. The absence of robust cybersecurity systems and the escalating geopolitical tensions have created a critical vulnerability window. This has been borne out by the multiple cyberattacks on official and institutional websites in Pakistan. Indian cybercriminals often coordinate their efforts to accomplish a common aim. The long-standing animosity and ongoing geopolitical dispute between Pakistan and India have further increased the stakes in the cyber realm.

Attacks on Pakistan's banking industry have been on the rise, which is concerning because hackers are increasingly looking for ways to profit from weak digital infrastructures. The situation is already critical, and terrorist groups' threats to exploit cyber capabilities for vengeance or asymmetric warfare are making it much worse. Cyberspace has joined land, sea, air, and space as the fifth domain of warfare in this ever-changing setting. This shows a shift in thinking about how to handle disputes and the idea of deterrence.

Overall, despite considerable advances in legislative reform, Pakistan's cybersecurity posture remains inadequate. Pakistan is a rapidly developing cyber power, as evidenced by the country's ranking of 66th in the 2017 Global Cybersecurity Index (GCI) released by the International Telecommunication Union (ITU), a UN specialized agency. While there has been improvement in Pakistan's organizational architecture, institutional capability, and the establishment of technical institutions, the country's legislative efforts to address cybersecurity concerns have made little success. These problems stem from cybersecurity initiatives that aren't coordinated and don't have a strategy for the future.

Pakistan needs to quickly refocus its national policy on cyber preparedness because of how important it is. In this strategy, creating an all-encompassing cybersecurity and e-governance plan should be the central focus. Cohesive achievement of economic, administrative, and national security goals requires alignment of interests among all key players in the cyber ecosystem. The lack of cooperation between Pakistan's intelligence and security agencies in the fight against cybercrime is another issue that needs addressing. Overall, national cybersecurity plans have failed because of ineffectiveness and duplication of effort brought about by disjointed institutional frameworks.

Pakistan must address this structural gap by establishing a centralized and coordinated framework that improves service delivery, connects vital infrastructure nodes, and promotes inter-agency collaboration. Institutional synergy is the nation's greatest bet for protecting itself from evolving cyber threats. It is equally critical to promote digital literacy and increase public understanding regarding cybersecurity.

We must vigorously pursue curriculum revisions that center on digital hygiene and cyber ethics, as well as targeted public education campaigns and capacity-building programs, because humans are typically the weakest link in cybersecurity.The development of a resilient and innovative cybersecurity ecosystem depends on an educated and trained human capital base. Pakistan may take use of its demographic dividend to create a safer and more tech-savvy society by raising awareness and training cyber professionals.

In recent years, numerous worldwide indices have been developed to assess a country's level of digital advancement. These indices have yielded valuable insights into Pakistan's cyber capacity and digital readiness. A composite measure that employs seven criteria to evaluate the progress of information and communication technology (ICT), the ICT Development Index (IDI) is published annually by the International Telecommunication Union (ITU). Considering that nearly 60% of Pakistan's population is under the age of 35, the nation's 48th position out of 169

economies in the 2023 IDI (ITU, 2024a) demonstrates its tremendous unrealized potential. One way to help Pakistan's youth take charge of the country's IT advancements is to equip them with the necessary digital skills and ensure they have inexpensive access to communication tools. In the meanwhile, the E-Government Development Index (EGDI) 2024 from the UN assesses countries based on three factors: HCI, OSI, and TII, which stands for telecommunications infrastructure. According to the United Nations (2024a), Pakistan made its debut in the "High EGDI" category in 2024 after dropping to 136th rank in 2022. Reasons for this accomplishment include a large user base (including 77 million internet users and 165 million mobile customers) and a rise in teledensity (75%). However, across several departments, there is a clear absence of G2C and C2G service delivery; thus, a systematic effort is necessary to improve digital governance's reach and quality.

Similarly, Pakistan is in the 90th spot out of 134 nations on the Network Readiness Index (NRI) 2023. This index assesses how nations utilize ICTs for long-term development across four domains: Technology, People, Governance, and Impact. According to the Portulans Institute (2023a), Pakistan ranks 117th in Governance and 49th in Technology, thus the country needs to change its laws and make regulators more watchful. According to the NRI, Pakistan could become a big player in the digital ecosystem if the problems caused by bad leadership were to be addressed.

Also, according to CISCO's Global Digital Readiness Index 2023, Pakistan is at the "Accelerate" stage and ranks 120th out of 146 nations. Overall, Pakistan scored 7.77 out of 25 (CISCO, 2023), with disparities observed in three critical areas: Basic Needs (0.64/4), Business and Government Investment (0.37/3), and Technology Infrastructure (0.88/4). According to these figures, Pakistan must make substantial investments and execute wise policies if it aspires to achieve the "Amplify" level of digital readiness. Nevertheless, the essential building blocks have already been assembled.

In addition, the Global Cybersecurity Index (GCI) 2024, put out by the International Telecommunication Union, assesses the level of commitment of governments to cybersecurity by analyzing their steps in five domains: legislation, technological infrastructure, companies, and cooperation. With a rise from 79th to 40th place and admission to the Tier-1 "Role Modeling" category, Pakistan has clearly made significant strides in strengthening its cybersecurity posture (ITU, 2024b). Instead of using simple numerical rankings, the GCI's tier-based methodology encourages regional comparison and mutual learning among nations in the same performance tier.

This shift is greatly appreciated by developing countries such as Pakistan, who are achieving growth despite systemic limitations. Pakistan and other low-income governments face challenges in allocating resources, implementing laws, and safeguarding vital infrastructure, in contrast to high-income nations that have robust national cybersecurity strategies and response teams (ITU, 2024b). The GCI emphasizes this as a worldwide imbalance. Improvements in Pakistan's performance on these metrics indicate that the country's authorities are beginning to recognize the latent potential of its people and infrastructure. Without targeted changes in leadership, skill development, and public-private partnerships, the digital divide will prevent cybersecurity from expanding sustainably.

The legal framework underpinning Pakistan's cybersecurity ecosystem includes the Pakistan Telecommunication Act (1996), the Electronic Transaction Ordinance (2002), and the Prevention of Electronic Crimes Act (PECA) (2016). The primary features of Pakistan's cybersecurity ecosystem are illustrated in the table below.

Table 2.Overview of Existing Cybersecurity Ecosystem in Pakistan

National Strategy Documents	• National Cybersecurity Policy 2021 • Personal Data Protection Bill 2021 (*Under Review*)
National Computer Emergency Response Teams (CERTs)	No
National Cybersecurity Agency	No
National Cybersecurity Guidelines / Standards	No
Data Security, Data Integrity, and Data Localization Requirements	No
Cybercrimes Prosecution Agency	NR3C (works under FIA)
National Cybersecurity Coordinator	No
Cyber Threat Intelligence Agency	No
Capacity Building Institutions	National Cybersecurity Center, Islamabad
Foreign Collaborations	No

A detailed investigation of Pakistan's cybersecurity landscape reveals significant systemic deficiencies that hinder the development of a strong and comprehensive national framework. Several essential components are absent or in preliminary development, including a cohesive national cybersecurity organization, operational computer emergency response teams (CERTs), definitive protocols for data protection, and established cybersecurity procedures. Although legislation such as PECA 2016 addresses cybercrimes, it fails to encompass the broader strategic necessities required for national cybersecurity and resilience.

To rectify these shortcomings, Pakistan's Federal Cabinet enacted the inaugural National Cyber Security Policy on 27 July 2021, marking a pivotal point in the nation's endeavor to institutionalize cybersecurity. The objective of this strategy is to establish a secure, well-coordinated, and responsive public-private cyber ecosystem. The Ministry of Information Technology and Telecommunication (MoITT) is currently evaluating the Personal Data Protection Bill (2020). Upon its enactment, it will establish a foundation for a more secure digital economy in Pakistan by tackling critical concerns related to data privacy, integrity, and localization.

1.2 Evolving Cyber Warfare: Constraints and Challenges for Pakistan

Despite rising dangers and increased reliance on technology, Pakistan's cyber strategy is still in its early stages and poorly coordinated. A lack of a coherent national doctrine, poor coordination among agencies, and insufficient deterrent mechanisms are some of the most pressing strategic issues the country faces in this age of ubiquitous cyberwarfare. The already precarious geopolitical climate, the prevalence of border conflicts, and the technology gap between India and its regional rivals only make matters worse.

1.2.1 Absence of a National Cyber Warfare Doctrine

Without a thorough national cyber warfare strategy, Pakistan faces a significant strategic challenge. Although the country's National Cyber Security Policy was published in 2021, it mostly provides an overview of the policy's principles and objectives rather than a detailed plan for how to implement them (Ministry of IT & Telecom, 2021). With no officially stated doctrine for offensive or defensive cyber operations in place as of 2024, Pakistan's intelligence and military branches are at a loss as to how to respond to the ever-changing cyber threat landscape.

In contrast, the Indian Ministry of Defense (MoD) has announced plans to establish a tri-service command called the Defense Cyber Agency (DCA)

in 2019 to handle offensive and defensive cyber operations (HEIDER, 2024). When crises turn into digital conflicts, Pakistan is at a strategic disadvantage due to this disparity. Delays in responding to assaults and continued division of labor among civilian and military agencies are consequences of not having a cyber doctrine.

1.2.2 Weak Strategic Deterrence and Attribution Capabilities

Strategic cybersecurity relies on digital deterrence, however Pakistan does not have effective cyber deterrence measures. Attributing attacks, projecting retaliatory capability, and signaling intent to adversaries are all necessary for effective deterrence, in addition to strong defensive capabilities. A Carnegie Endowment for International Peace assessment indicated that only 11% of cyber events against Pakistan between 2015 and 2022 could be plausibly linked to a source, highlighting Pakistan's inadequate cyber attribution capability (Lewis, 2022).

In addition, Pakistan lacks the necessary infrastructure and has not publicly stated a policy regarding proportional or retaliatory cyber strikes. Because of the lack of clear consequences, enemies are encouraged to launch cyber assaults without worrying about retaliation, leading to strategic ambiguity. Evidence of this was found following the 2019 Pulwama-Balakot incident, in which Indian cyber teams allegedly breached Pakistani networks for surveillance purposes without facing direct reprisal (Kaplan, 2021).

1.2.3 Resource Constraints and Technological Asymmetry

Allocating resources and enhancing technological capacity are two other significant obstacles. According to the Ministry of IT & Telecom Pakistan (2023) and the Indian Ministry of Defense (2023), Pakistan's national cybersecurity projects received less than USD 15 million in the fiscal year 2022–2023. In comparison, India's received USD 62 million and China's estimated USD 1.4 billion. Due to strategic underinvestment, Pakistan is unable to build its own cybersecurity tools, hire qualified cybersecurity experts, or fund R&D.

According to the World Economic Forum (2023), there is a significant disparity between the number of trained cybersecurity professionals in Pakistan (less than 2,000) and India (more than 100,000). The lack of human resources has a significant effect on the nation's ability to withstand cyberattacks, which can have catastrophic effects in industries such as banking, energy, and defense.

1.2.4 Fragmentation of Strategic Institutions and Command Structure

A number of Pakistani ministries and departments are involved in cybersecurity initiatives, including as the Pakistan Telecommunication Authority (PTA), the Inter-Services Intelligence (ISI), NADRA, the Pakistan Telecommunication Authority (FIA Cybercrime Wing), and ISPR. Nevertheless, the planning of strategic cyberwarfare is not coordinated by any single command body. More than 70% of Pakistan's vital digital assets do not belong to a single command structure, according to an internal audit conducted by the National Security Division in 2022. This leaves monitoring and incident response vulnerable (NSD, 2022).

Decisions cannot be made quickly, strategies cannot be planned, and risks cannot be adequately assessed due to this structural fragmentation. Additionally, it makes it harder for the military and civilian sectors to work together, which is particularly problematic in situations when cyberattacks are a component of hybrid warfare involving both conventional and information operations.

1.2.5 Strategic Vulnerability to Information Warfare

Pakistan is at risk not just from system-level attacks but also from cyber-enabled information warfare, which encompasses narrative manipulation, psy-ops, and propaganda. A report from the Stanford Internet Observatory (2023) states that coordinated inauthentic behavior (CIB) efforts, with many of the operations originated in Indian networks, sought to undermine Pakistani institutions online, making Pakistan the second most targeted South Asian country.National discourse and democratic institutions are

undermined by this type of psychological warfare. According to Bradshaw and Howard (2023), disinformation operations can cause long-term strategic instability by undermining public trust in the government, military, and judiciary, particularly during elections or national crises.

1.3 Structural Gaps in Pakistan's Cybersecurity Infrastructure

Although Pakistan has been working on the "Digital Pakistan" strategy for twenty years, the country's cybersecurity remains in a terrible state. Even though the country has updated its information technology policy multiple times since its inception in the year 2000 to cover a wide range of topics, including legal frameworks, digitalization of certain sectors, infrastructure improvement, and innovation promotion (Ministry of IT, 2020), the country's approach to cybersecurity is severely lacking. The lack of a unified national cybersecurity framework continues to be a barrier to the gradual transition toward a knowledge-based economy that is intended to be accomplished through digital policy.

Major structural vulnerabilities include, but are not limited to, delays in the implementation of data protection legislation, unequal institutional coordination, inadequate establishment of Computer Emergency Response Teams (CERTs), and the absence of a unified cybersecurity agency. Even though the Electronic Transactions Ordinance (ETO) was passed in 2002 and the Prevention of Electronic Crimes Act (PECA) was put into effect in 2016, these measures are not sufficient on their own to construct an effective cybersecurity regime (CISS Insight, 2023).

In July 2021, the federal cabinet of Pakistan gave its approval to the first National Cyber Security Policy of Pakistan. As stated in the MoITT's 2021, its objective is to establish a cybersecurity ecosystem that is not only secure but also well-coordinated and flexible. Nevertheless, significant supplemental laws, such as the Personal Data Protection Bill 2020, are still being considered at this time. If this measure is ratified, it is envisaged that it will solve significant concerns regarding the integrity, localization, and security of data (MoITT, 2020).

Despite the implementation of digital policies aimed at promoting e-governance and adhering to global data protection standards in provinces like Punjab and Khyber Pakhtunkhwa, there is a significant lack of policy coordination and operational synergy between the federal and provincial levels. The Punjab Digital Policy (2018) aims to initiate structural transformation without explicitly outlining cybersecurity regulations, but the KP Digital Policy (2018) incorporates cybersecurity protocols that align with the General Data Protection Regulation (GDPR) (KPITB, 2018; PITB, 2018).

Originally established in 1959 as the National Communications Security Board (NCSB), the National Information Technology Security Board (NTISB) today oversees cybersecurity problems arising from emerging technologies. However, the enforcement of cybersecurity standards across many sectors is obstructed by the NTISB's deficiencies in strategic authority, technological proficiency, and overlapping jurisdictions (Cabinet Division, 2023).

Both nation-state and non-state cyber attackers are intensifying their assaults on Pakistan's critical infrastructure. The Pakistan Tribune (2024) reported over 16 million cyberattacks in 2023, reflecting a 17% rise from the prior year. It affected around 25% of Pakistan's internet customers. Rewterz (2018) observes alarming trends, including a 59% rise in banking malware, a 35% increase in Trojan attacks, and a 24% escalation in ransomware threats.

Hacktivist and state-sponsored threats persist. For instance, as reported by Norman Shark and the Shadowserver Foundation (2013), Indian APTs have executed intricate espionage operations targeting Pakistani governmental entities. The predominant cyber intrusions focus on HTTPS Port 443, with the United States and Russia being implicated in these violations (Kaspersky, 2024).

Between 2015 and 2024, a series of cyberattacks targeted Pakistani banks and government entities. In 2018, assaults on Pakistani banks compromised almost 150,000 credit card details on the dark web, resulting in losses exceeding $6 million (Zaidi,

2018). The ransomware assault on K-Electric in 2020 sought a ransom of $38 million. Resecurity (2024) indicates that a significant smishing scam masqueraded as Pakistan Post to defraud clients. The scam exhibited operational parallels to the notorious Smishing Triad outfit.

Cyber threats possess a geopolitical aspect, evidenced by past incidents such as the breach of the Ministry of Foreign Affairs website following the Pulwama incident in 2019 and the spyware assault aimed at Pakistani officials via the Israeli NSO Group (Kirchgaessner, 2019). Dawn (2015) asserts that the 2013 Snowden revelations further substantiated that the U.S. NSA employed malware such as SECONDATE to infiltrate Pakistan's civil and military digital infrastructures. The urgent necessity for robust cyber capabilities is underscored by these repeated occurrences, which expose significant vulnerabilities in Pakistan's digital defenses. State sovereignty and institutional integrity are severely threatened by unpreparedness regarding the increasing intertwining of cyber power with national security. Cybersecurity firms such as Symantec identify Pakistan as one of the ten most targeted countries for cyberattacks worldwide. Consequently, Pakistan must promptly revise its cybersecurity policy (CISS Insight, 2023).

It is imperative that significant policy texts, such as the Personal Data Protection Bill, be implemented and that national initiatives are aligned with international frameworks like the Global Cybersecurity Index. Moreover, to enhance resilience and mitigate vulnerabilities in the digital world, it is essential to invest in technical human resources, establish real-time threat intelligence capabilities, and centralize cybersecurity responsibilities under a single authority.

1.4 Geopolitical and External Challenges in Cyber Space for Pakistan

Pakistan and other states in crucial geostrategic positions are especially vulnerable to the growing influence of geopolitical rivalry and external strategic threats on the cyberwarfare battlefield. Pakistan faces constant challenges from both state-sponsored and non-state entities in the realm of cybersecurity, which necessitates both internal and external resilience. Pakistan is even more exposed online due to the global spread of cyber capabilities, asymmetrical hostilities, and the intricacy of regional politics.

1.4.1 Cyber Threats from State and Non-State Actors

India and Pakistan are antagonistic states whose geopolitical tensions frequently translate into cyberspace, posing a persistent cyber danger to Pakistan. Pakistan was the target of more than 65% of APT assaults on South Asia in 2022, with many of these attacks being associated with state-sponsored organizations, according to a report by Group-IB. The persistent targeting of Pakistani military, diplomatic, and government establishments by cyber espionage groups located in India, such as "APT36" (or Mythic Leopard) (Group-IB, 2022).

Hacktivist groups and transnational criminal organizations are among the non-state entities that have attacked Pakistan online. State-sponsored threats are not the only ones that have done this. From 24,000 incidents in 2018 to more than 100,000 instances in 2022, the Cyber Crime Wing of Pakistan's Federal Investigation Agency (FIA) recorded a 400% surge in cybercrime complaints (FIA, 2022). These groups frequently attack both public and private infrastructure by taking advantage of lax cyber laws and enforcement capabilities.

1.4.2 Geopolitical Pressures and Strategic Vulnerabilities

In terms of geopolitics, Pakistan is still caught up in the cyber weapons competition in the region. Compared to Pakistan, India has poured a lot more money into its cybersecurity and offensive cyber capabilities. According to the Indian Ministry of Electronics & IT (2022) and the Ministry of IT & Telecom Pakistan (2023), the cybersecurity budget for 2022–2023 in Pakistan was roughly three times lower than the 515 crore (about USD 62 million) allotted to the same area by the Indian government. Despite Pakistan's attempts to update its cyber defense posture, deterrence is hindered by this disparity, which generates a strategic asymmetry.

In addition, the narrative surrounding the regional conflict, especially after Pulwama (2019), has further highlighted the cyber component of hybrid warfare. Both countries participated in low-level cyber sabotage, disinformation efforts, and digital propaganda during and after the Pulwama-Balakot incident. India asserted that it successfully warded off many cyberattacks that threatened vital digital assets, while Pakistani cyber teams allegedly launched counter-narratives against Indian social media networks and surveillance systems (Kaplan, 2021). The merging of conventional geopolitical animosity with cyber hostilities is borne out by these occurrences.

1.4.3 International Norms, Isolation, and the Need for Cyber Diplomacy

Pakistan is still not actively participating in international efforts to establish cyber norms. International channels for legal cooperation in cyber investigations are less accessible to it because it has not signed the Budapest Convention on Cybercrime. In addition, the ITU Global Cybersecurity Index 2020 rates Pakistan at 79 out of 182 nations, highlighting the country's serious shortcomings in institutional response, technical capabilities, and regulatory frameworks (ITU, 2021).Because of its marginalization, Pakistan is unable to work with other countries and implement cybersecurity standards that are recognized worldwide. More and more, rival nations like India's have been involved in cyber diplomacy, aligning themselves with cyber cooperation blocs in the Indo-Pacific and the West. Taking part in international conferences, where regulationsCyber norm-building is frequently influenced by the development of setting and strategic narratives, as stated by Tikk and Kaska (2020). Two strategic fallouts of Pakistan not being present in these arenas include a dearth of shared intelligence networks and slow access to best practices in implementing cybersecurity policies. These geopolitical and external threats need that Pakistan increase its regional cooperation efforts and cyber diplomacy. Participating in United Nations cyber conferences, building strategic alliances with allies skilled in cyberwarfare, and bolstering the capacities of regional organizations like the Shanghai Cooperation Organization and the Organization of Islamic Cooperation are all viable next steps. The many cyber risks that Pakistan faces can be better managed with the use of digital deterrence strategies that include attribution capabilities, incident response protocols, and norms-based signaling.

1.4.4 Enhancing Pakistan's Cyber Resilience

Strategic indifference could jeopardize Pakistan's digital sovereignty and national security at a critical point in its cybersecurity framework. A nation can deter cybercriminals, according to the digital deterrence paradigm, by bolstering its cyber defenses, sending trustworthy signals, and being resilient. Unfortunately, Pakistan does not yet have the institutional maturity to adequately defend itself against complex attacks due to its immature cyber architecture. Despite the fact that programs like the National CERT and bills like the Personal Data Protection Bill appear to be moving in the right direction, studies show that there are still holes in the system, problems with cooperation, and insufficient capabilities to discourage.

1.4.5 Institutional and Legal Disparities

The country's structure is greatly affected by its disjointed judicial system. Protecting Pakistan's digital economy and e-commerce is crucial, but the Data Protection Bill is too limited and doesn't cover everyone. Protective measures for marginalized groups, such as religious and ethnic minorities, transgender people, children, and women, are severely absent. Little can be done to prevent the exploitation and digital harm of children in the absence of explicit legislative safeguards and classifications that designate their data as sensitive. Digital deterrence models stress the need of a robust legal framework in conveying the consequences of bad actors' actions.

Though it remains the foundation of modern cybersecurity enforcement, the Prevention of Electronic Crimes Act (PECA) of 2016 has grown obsolete as a result of the dynamic nature of cybersecurity threats. The Ministry of Information

Technology's National CERT has very little institutional autonomy and operational freedom when it comes to sector-wide response coordination. To successfully deploy deterrence by denial and resilience, it is essential to establish a separate cybersecurity authority that is responsible for maintaining national security mandates and enabling proactive defense measures.

1.4.6 Technical Deficiencies and Cyber Readiness

When it comes to Pakistan's technology, there are still significant readiness issues. Integral to any effective deterrent posture are networks for Cyber Threat Intelligence (CTI), SIEM systems for security information and event management, and operational SOCs. Pakistan is missing out on real-time threat data and collaboration opportunities thanks to its non-participation in globally networked systems like FIRST, which impacts strategic situational awareness. Furthermore, without a publicly enforced National Information Security Policy, Pakistan is unable to set deterrence through credible signaling and a strong defensive baseline.

It is difficult to formulate long-term strategies and establish attainable targets for cyber maturity because the cyber policy is in its infancy. The essential components of a strategic deterrent architecture—a transparent governance model, risk assessment methodologies, capacity requirements, and a compliance mechanism—are not well-defined or enforced. According to Libicki (2021), countries that have used digital deterrent mechanisms, such as the United Kingdom and Estonia, have achieved this through well-defined governance structures that place an emphasis on scalability and interoperability in incident response, beyond only technological methods.

1.4.7 Organizational Fragmentation and Sectoral Gap

While the establishment of PAK NCERT, Pakistan's National Cyber Emergency Response Team, is a positive step in the right direction, it is insufficient on its own. It is challenging to accomplish its extensive goals, such as threat detection and response, awareness-building, and policy formation, due to a lack of institutional authority and insufficient inter-agency cooperation. An essential component of digital deterrence is the integration of command and information flows across different organizational units. Due to the lack of a unified standard or real-time interoperability framework, many industry-specific CERTs (e.g., those dealing with energy, healthcare, and finance) operate autonomously.

Deterrence is most effective when a central authority is responsible for regulating the complete nation's infrastructure, coordinating the efforts of the private sector, and checking for compliance at every stage. The National Cyber Directorate in Israel and the National Cyber Security Centre (NCSC) in the UK are two international models that Pakistan's CERTs could learn from. Cyber command centers with localized R&D units, simulation centers, and crisis coordination mechanisms should evolve from reactive actors into strategically empowered cyber command centers.

1.4.8 Capacity Building and Digital Sovereignty

Pakistan also faces a structural limitation in the form of its human capital and institutional capacity. Neither a national accreditation system nor a uniform framework for cybersecurity certifications exist in the nation. The result is a cyber-workforce that lacks organization, education, and proactive thinking. Human knowledge acts as a multiplier and essential component of "deterrence by denial" in the concept of digital deterrence, which is crucial for cyber resilience because it depends on how quickly and accurately humans react (Kello, 2022). To bridge this knowledge gap, it is essential to obtain certifications that align with international standards and academic curriculum, such as UK Cyber Essentials or ISO 27001.

With cloud infrastructure, you may achieve scalability, flexibility, and top-notch security. Encryption, identity management, and disaster recovery options offered by cloud systems are more cost-effective and nimble than those offered by more conventional arrangements. Coordinated deterrence postures are made possible by the

ability to improve real-time threat detection and public-private collaboration through the use of cloud-based technologies. Instead than continuously depending on foreign solutions, which come with their own sovereignty difficulties, this position needs investment in indigenous cloud capabilities if it wants to be sustained. This promise is highlighted by Pakistan's current Tier 1 "Role-Modelling" ranking in the ITU Global Cybersecurity Index (2024).

CONCLUSION

The three pillars of a credible cyber deterrence posture are capability, resilience, and signaling. In all of these domains, Pakistan's cybersecurity measures remain inconsistent. Because it lacks the necessary institutional procedures, it cannot demonstrate its ability to punish crime. From a technical perspective, it is lacking sufficient defensive depth. There is still a lack of harmony and cooperation among its national cyber command structure. The absence of a qualified cybersecurity workforce undermines efforts to fortify defenses and prevent breaches.

To address these systemic and strategic issues, Pakistan must pass the Personal Data Protection Bill, create a unified cyber governance ecosystem, activate sectoral CERTs, and speed up the creation of a National Information Security Policy. Without these changes, the state will be vulnerable to cyber espionage, dislocation of strategy, and cyber coercion. Their absence will render digital deterrence a mere abstraction.

There are new digital threats that go beyond the limits of conventional warfare, and they are putting a burden on Pakistan's cybersecurity infrastructure. The lack of a unified national strategy that incorporates cyber defense into the larger security apparatus is a significant strategic challenge. Strategic Pakistan has been sluggish to acknowledge the significance of cyberspace, leading to reactive rather than preventive responses to cyber events, even though cyberspace has emerged as a crucial arena for power projection and statecraft. Vulnerabilities have been created as a result of the delay in prioritizing institutional matters, and both state and non-state actors take advantage of this.

There is, unfortunately, no deterrence in online. Owing to its inadequate offensive and defensive cyber capabilities, Pakistan is more susceptible to persistent attacks and suffers a loss of confidence. The more common and sophisticated cyberattacks are, examples include data breaches, website defacements, and targeted disinformation efforts, which are frequently associated with malevolent foreign actors. Reactions, which are at most symbolic, reveal the unfortunate strategic gap between threat perception and capability growth. Without a formalized digital deterrent stance, Pakistan faces the danger of escalatory actions that could harm national morale and institutional trust.

Inadequate technical infrastructure, fragmented governance, and inadequate policies exacerbate problems structurally. Due to duplication of effort and unclear instructions, the several agencies engaged in cyber operations are unable to collaborate efficiently. Further evidence of the serious underfunding of cybersecurity is the fact that less than half of Pakistan's national budget goes toward cyber resilience and digital infrastructure initiatives. The existing legal frameworks governing cyber operations are antiquated and poorly implemented because of a lack of competent staff and essential technical expertise.

Finally, Pakistan's cybersecurity trajectory is further complicated by geopolitical issues. As a result of regional rivalry, particularly with India, cyber hostility has recently shifted gears. The absence of trust-building efforts and global standards has turned the internet into a battleground for low-intensity wars, making attribution difficult and escalation forecasting harder. Pakistan isn't actively participating in global cybersecurity coalitions, so it can't take advantage of collective defense mechanisms or share intelligence. This is not only about making technological adjustments; we must have visionary leaders and the political resolve to fix our nation's structural and strategic flaws immediately.

Unless cybersecurity starts to be viewed as a priority rather than a technicality, the threats to the national stability and digital sovereignty are going to be even further. To deal with these

challenges it is necessary not only some technological improvements, but also institutional reform, clarity in its doctrines, workforce, and long-term political dedication. Cyber resilience should be incorporated as part of the larger national security architecture and cannot be run separately.

Future studies can examine parallels between cyber deterrence models across states that sit at similar positions, evaluate channels through which civil-military integration could be achieved to govern cyberspace, and determine regional confidence-building efforts in cyberspace. More empirical focus on institutional reform and capacity-building mechanisms would also enhance the policy development in this area. The direction Pakistan follows in its cyberspace will eventually be decided by its readiness to strategically adjust to the digital conflict. Lack of such adaptation will mean this vulnerability will continue; the presence of it will mean credible deterrence is possible.

REFERENCES

ARY News. (2024, November 7). FTO orders FBR to improve security as data breach causes Rs 81.43 billion tax fraud. https://propakistani.pk/2024/11/07/fto-orders-fbr-to-improve-security-as-data-breach-causes-rs-81-43-billion-tax-fraud/

Bradshaw, S., & Howard, P. N. (2023). *The global disinformation order: 2022 update*. Oxford Internet Institute. https://oii.ox.ac.uk/

Cabinet Division. (2023). *National Communication Security Board (NCSB)*. https://cabinet.gov.pk/Detail/OWYxZTYxMWQtNDZhMC00M2IyLTk1NDgtODNmNTMxNmNlNGU0

CISS Insight. (2023). Pakistan's cybersecurity landscape. *Journal of Strategic Studies*, 118–119.

CISCO. (2023). *Global digital readiness index 2023*. Computer Information Data System Company. https://www.cisco.com

Dawn. (2015, May 20). Cyberattacks against govt expose fatal cracks on Pakistan's digital fence. https://www.dawn.com/news/1182856

EU DisinfoLab. (2020, December 9). *Indian chronicles: Deep dive into a 15-year operation targeting the EU and UN to serve Indian interests*. https://www.disinfo.eu/publications/indian-chronicles-deep-dive-into-a-15-year-operation-targeting-the-eu-and-un-to-serve-indian-interests/

Federal Investigation Agency (FIA). (2022). *Cybercrime statistics 2018–2022*. Government of Pakistan. https://fia.gov.pk/

Group-IB. (2022). *APT trends report 2022/2023: Overview of cyber threats in South Asia*. https://group-ib.com/

HEIDER, U. (2024, July 8). Indian military's embrace of cyber warfare. CASS. https://casstt.com/indian-militarys-embrace-of-cyber-warfare/

Indian Ministry of Defence. (2023). *Defence expenditure and cyber warfare developments*. Government of India.

Indian Ministry of Electronics & Information Technology. (2022). *Budget allocation for cybersecurity 2022–23*. https://meity.gov.in/

International Telecommunication Union. (2021). *Global cybersecurity index 2020*. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

International Telecommunication Union. (2024a). *Measuring digital development – ICT development index 2024*. https://www.itu.int/hub/publication/D-IND-ICT_MDD-2024-3/

International Telecommunication Union. (2024b). *Global cybersecurity index 2024*. https://www.itu.int/pub/D-HDB-GCI.01-2024

Kaplan, F. (2021). *Cybersecurity and cyberwar: What everyone needs to know* (2nd ed.). Oxford University Press.

Kaplan, F. (2021). *Cybersecurity and cyberwar: What everyone needs to know* (2nd ed.). Oxford University Press.

Kaspersky. (2024). Cyber threats increased by 17% in 2023. *Pakistan Tribune*. https://tribune.com.pk/story/2457021/cyber-threats-increased-by-17-in-2023

Kirchgaessner, S. (2019, December 19). Israeli spyware allegedly used to target Pakistani officials' phones. *The Guardian*. https://www.theguardian.com/world/2019/dec/19/israeli-spyware-allegedly-used-to-target-pakistani-officials-phones

KPITB. (2018). *Khyber Pakhtunkhwa digital policy 2018–2023*. https://kpitb.gov.pk/sites/default/files/Khyber%20Pakhtunkhwa%20Digital%20Policy%202018-2023.pdf

Lewis, J. A. (2022). *Cyber operations in South Asia: Attribution and deterrence*. Carnegie Endowment for International Peace. https://carnegieendowment.org/

Maheem, H. (2021). *Statecraft and cybersecurity in South Asia: Emerging threats and regional challenges*. University of Oxford.

Ministry of IT & Telecom Pakistan. (2021). *National cyber security policy 2021*. Government of Pakistan.

Ministry of IT & Telecom Pakistan. (2023). *Annual budget report on digital security*. Government of Pakistan.

Ministry of Information Technology. (2020). *Pakistan digital policy*. https://moib.gov.pk/Downloads/Policy/DIGITAL_PAKISTAN_POLICY%2822-05-2018%29.pdf

MoITT. (2021). *National Cyber Security Policy 2021*. Government of Pakistan.

National Security Division (NSD). (2022). *Internal audit report: Critical digital asset security in Pakistan*.

Norman Shark & Shadowserver Foundation. (2013). *Unveiling an Indian cyberattack infrastructure*.

PITB. (2018). *Punjab digital policy*. https://pitb.gov.pk/punjab-digital-policy

Portulans Institute. (2023a). *Network readiness index 2023*. https://networkreadinessindex.org/

Rewterz. (2018). *Threat intelligence report 2018*. https://www.rewterz.com/threat-intelligence-reports/2018-threat-intelligence-report

Resecurity. (2024, June 11). Smishing Triad is targeting Pakistan to defraud banking customers at scale. https://www.resecurity.com/blog/article/smishing-triad-is-targeting-pakistan-to-defraud-banking-customers-at-scale

Sophos. (2021, January 12). New Android spyware targets users in Pakistan. https://news.sophos.com/en-us/2021/01/12/new-android-spyware-targets-users-in-pakistan/

Stanford Internet Observatory. (2023). *South Asia CIB trends: Pakistan under digital siege*. Stanford University. https://cyber.fsi.stanford.edu/

Tikk, E., & Kaska, K. (2020). *International cybersecurity law and policy: Building global norms*.

United Nations. (2024a). *UN e-government survey 2024: Accelerating digital transformation for sustainable development*. https://desapublications.un.org/publications/un-e-government-survey-2024

World Economic Forum. (2023). *Global cybersecurity outlook 2023*. https://www.weforum.org/

Zaidi, E. (2018, November 17). Cyber attackers steal 150,632 plastic cards data of three banks. *The News*. https://www.thenews.com.pk/print/394589