Pakistan's Cybersecurity Landscape: Information and Communication Technology Readiness, Challenges and Opportunities

Zaheema Iqbal[*] and Rafi us Shan[*]

Abstract

There is a direct correlation between digital adoption and the prevalence of cyber threats; likewise, digital readiness and cybersecurity rankings are closely intertwined. Pakistan's Information and Communication Technology (ICT) posture is directly tied to its commitment to cybersecurity. With the increased use of the internet and the growing sophistication of cyber-attacks by both state and non-state actors, cybersecurity has become a significant challenge for policymakers in Pakistan in the commercial domains. This paper examines Pakistan's ICT index ranking, and patterns of cyber threats landscape. By assessing Pakistan's cybersecurity standing based on the Global Cybersecurity Index (GCI) published by the International Telecommunication Union (ITU), this paper provides actionable recommendations for national policymakers to address the gaps in the cybersecurity framework and improve national position in global cybersecurity rankings.

Keywords: Cyber threats, cybersecurity rankings, ICT, ITU, GCI, Pakistan's Cybersecurity Strategy.

* Zaheema Iqbal is a non-resident researcher at the Global Foundation for Cyber Studies and Research in Washington, D.C. She holds a degree from the National Defense University, Pakistan.

* Rafi us Shan (PhD) is a technologist and educator with over two decades of experience in digital transformation, cybersecurity, privacy and data protection, and cloud security. He is currently on the faculty of the Higher Colleges of Technology (HCT) in the UAE.

Introduction

Information systems are one of the fundamental pillars of knowledge-based economies.[1] Over the past decade, the nature and volume of information managed and delivered through ICT have grown exponentially. ICT-based systems are now a key enabler for service delivery in Pakistan, government departments and service providers have been actively designing and deploying various applications and services to deliver public services through ICT. However, despite these efforts, Pakistan's overall ICT ranking in various global indexes has not shown significant improvement.[2]

While government ministries and autonomous bodies at both federal and provincial levels are advancing the agenda of digital transformation, in return, the uneven growth of digital technologies has led to a widening digital divide. Additionally, the health and resilience of digital systems and processes have not been prioritized under any existing digital transformation policy. This lack of focus has contributed to a decline in the country's overall information security posture, posing risks to the progress of its digital transformation initiatives.[3] To ensure inclusive and sustainable digital transformation for all, consistent and well-structured efforts are essential.

This paper provides an overview of Pakistan's ICT posture, examining its alignment with various established ICT indexes and offering a detailed breakdown of the parameters and their coverage used in these indexes. There is a clear linkage between a country's ICT posture and its commitment to information security. The paper assesses Pakistan's current cybersecurity performance based on the Global Cybersecurity Index and offers actionable recommendations for national policymakers to improve its standing in ICT-related rankings in general and the GCI of the International Telecommunication Union in particular.

1. Shahrazad Hadad, "Knowledge Economy: Characteristics and Dimensions," *Management Dynamics in the Knowledge Economy* 5, no. 2 (2017): 203–225. https://www.researchgate.net/publication/318005213_Knowledge_Economy_Characteristics_and_Dimensions

2. Asif Javed, "The Scope of Information and Communication Technology Enabled Services in Promoting Pakistan Economy," *Asian Journal of Economics, Finance and Management*, no. 4 (2020): vol. 2, pp. 1–9.

3. Usama Nizamani, "Internet Governance and Pakistan's Digital Economy," *Journal of Current Affairs*, no. 2, vol. 3 (2019): 23–49.

Assessing National ICT Landscape

The digital landscape of Pakistan is analyzed through the lens of various indexes, examining current postures, identifying reasons for shortcomings, and providing recommendations. These indexes evaluate the progress of ICT development, the evolution of digital transformation across multiple factors, cross-sector and regional comparisons in the adoption of digital technologies, the extent of the digital divide, and overall ICT development. Additionally, they offer valuable insights into policy formulation and, most importantly, highlight the potential for ICT development within various affiliate sectors that influence ICT adoption. This section is divided into two sub-sections. The first sub-section analyzes Pakistan's performance in ICT indexes, while the second sub-section reviews the efforts made by Pakistan to strengthen and complement its digital ecosystem.

To achieve this, the study has examined benchmarked ICT-related indexes, focusing primarily on Pakistan's performance and potential in these frameworks, including the ICT Development Index (IDI), the E-Government Development Index (EGDI), the Network Readiness Index (NRI), and others. Additionally, the study provides an analytical review of Pakistan's performance in the Global Cybersecurity Index by the ITU, evaluated against the benchmarks set by these ICT indexes.

The following section assesses key indexes, highlighting Pakistan's commitment to various established digital frameworks, analyzing the impact of their sub-pillars, and exploring the country's potential within these sub-pillars.

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

Table 1: List of Indexes and Pakistan's Ranking.
Source: Compiled by the authors (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 ICT Development Index

The ICT Development Index (IDI) tracks progress toward an information society. As a composite index, it combines multiple indicators into a single benchmark and has been published annually by the ITU since 2009.[4] The 2023 IDI incorporates seven indicators and covers 169 economies. Its core objectives are to measure the level, evolution, and progress of ICT development, assess the digital divide, and evaluate how effectively countries can leverage ICT for growth based on their existing skills and capabilities. Pakistan ranks 48th on the index and possesses significant ICT potential. With a population exceeding 220 million, a median age of 22, and around 35% of its population under 15 years of age (and approximately 60% under 35 years of age), Pakistan has a young and dynamic demographic profile.[5] Empowering this youth bulge with appropriate digital skill sets, along with providing affordable access to digital platforms and communication technologies, could substantially improve Pakistan's standing in the ICT index.

E-Government Development Index (EGDI) 2024

The EGDI evaluates the use of ICT systems to deliver public services across countries. It is based on three main components: the Human Capital Index (HCI), the Online Service Index (OSI), and the Telecommunication Infrastructure Index (TII). The 2024 EGDI provides a comprehensive assessment of the digital landscape across 193 economies.[6] The overall index reflects significant progress, with the proportion of the population less engaged in digital development decreasing from 45.0% in 2022 to 22.4% in 2024.[7] Pakistan has made significant progress, rising to the 136th position in the 2024 EGDI by uplifting its status from the 151st rank in the 2022 survey. This marks Pakistan's first-ever entry into the "High EGDI"

4. "Measuring Digital Development – ICT Development Index 2024," *International Telecommunication Union* (ITU), June 2024. https://www.itu.int/hub/publication/D-IND-ICT_MDD-2024-3/
5. "Measuring Digital Development – ICT Development Index 2024."
6. "UN E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development," *United Nations*, 2024. https://desapublications.un.org/publications/un-e-government-survey-2024
7. "UN E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development."

category, representing a notable leap from its previous standing in the "Middle EGDI" category.[8] Pakistan has a teledensity of 75%, with 165 million mobile phone subscribers and 77 million internet users. The country holds significant growth potential if the population is empowered with affordable communication technologies and digital literacy. Such efforts could dramatically enhance Pakistan's standing in the Telecommunication Infrastructure Index and Human Capital Index.

Moreover, focused efforts are needed for government entities to enhance service delivery through information and communication technologies. Despite the promotion of ICTs for digital service delivery—such as Government-to-Government (G2G), Government-to-Citizen (G2C), and Citizen-to-Government (C2G) interactions—many government departments in Pakistan should focus on developing strategies to expand the use of ICT for efficient public service delivery.[9]

The Network Readiness Index Report (NRI) 2023

The NRI Report 2023 focuses on enhanced ICT competitiveness and development. It evaluates the policies, factors, and institutions that enable countries to leverage ICTs for sustainable growth and well-being. The NRI provides a holistic framework for assessing the multi-dimensional impact of ICT on society while identifying aspects that will become critical for adopting new technologies in the coming decades.[10]

The latest NRI report maps the network-based readiness of 134 countries, analyzing four key factors: Technology, People, Governance, and Impact. Pakistan ranks 90th out of 134 economies in the NRI 2023. Its primary strength lies in the Technology pillar, where it has shown notable improvement. However, the greatest scope for further progress remains in the Governance pillar, which continues to be a concern.

8. "UN E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development," *United Nations*, 2024. https://desapublications.un.org/publications/un-e-government-survey-2024
9. J, Clement. "E-Government Development Index (EGDI) 2020, by Country," *Statista*, August 26, 2020. https://www.statista.com/statistics/421580/egdi-e-government-development-index-ranking/.
10. Network Readiness Index, Portulans Institute, 2023. https://networkreadinessindex.org/countries/

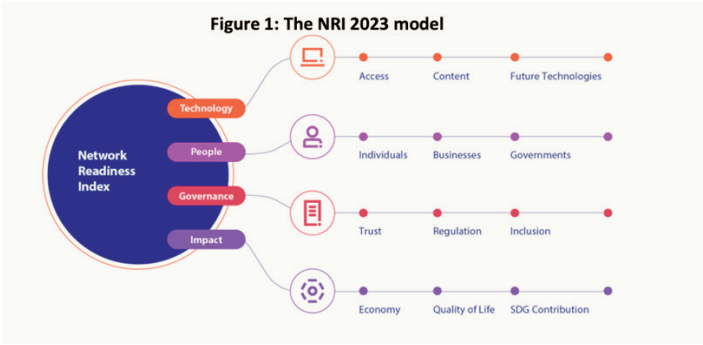

Figure 1: NRI 2023; Source: Network Readiness Index 2023[11]

Specifically, Pakistan is ranked 49th in the Technology pillar, 89th in the People pillar, 117th in the Governance pillar, and 93rd in the Impact pillar, as shown in Figure 2.

Figure 2: Pakistan's global ranking, overall and by pillar.
Source: Network Readiness Index 2023.[12]

As discussed earlier, with 60% of its population under the age of 35 and a median age of 22.8—8 years younger than the global average—Pakistan possesses immense human potential. By equipping its youth with the right skills, particularly digital skills that align with the digital ecosystem, the country can develop a trained workforce to serve as a cornerstone of the knowledge economy. Currently, over 100 universities in Pakistan produce more than 25,000 ICT graduates annually. However, it is crucial for Pakistan to not only improve the quality of these graduates but also significantly increase the number of ICT graduates to at least 100,000 per year to meet the demands of a rapidly evolving digital economy.

11. Network Readiness Index, Portulans Institute.
12. Network Readiness Index.

Global Digital Readiness Index 2023

The Global Digital Readiness Index 2023, published by Computer Information Data System Company (CISCO), evaluates global economies based on their digital readiness across three stages: Activate, Accelerate, and Amplify. The index ranked 146 countries, with Pakistan positioned at 120th. A country's digital readiness is assessed through several factors, including basic needs, business and government investments, ease of doing business, human capital, the start-up environment, technology adoption, and technology infrastructure.

Singapore ranked the highest on the Global Digital Readiness Index 2023 with a score of 2.37, followed by Luxembourg and Iceland. Pakistan, with a score of 7.77 out of 25, was placed in the "Accelerate" stage. Its performance across the sub-pillars was as follows: 0.64 out of 4 in Basic Needs, 0.37 out of 3 in Business and Government Investment, 0.85 out of 4 in Ease of Doing Business, 1.89 out of 4 in Human Capital, 0.62 out of 3 in Start-Up Environment, 1.19 out of 3 in Technology Adoption, and 0.88 out of 4 in Technology Infrastructure.

Global Cybersecurity Index 2024

The GCI 2024, published by the ITU, aims to promote cybersecurity awareness and evaluate countries' commitment to cybersecurity across various sectors and applications.[13] The GCI evaluates countries based on five key pillars: legal, technical, organizational, capacity building, and cooperation. The 2024 report ranks countries by region and highlights global leaders in cybersecurity readiness. Singapore is recognized as the most committed nation globally, achieving a perfect index score of 100. It is followed by Switzerland with a score of 97.55, and Denmark in third place.[14] The 2024 GCI ranks Pakistan at 40th, marking a significant improvement from its previous 79th position. This advancement has elevated Pakistan to the Tier-1 (Role Modeling) rating. A detailed discussion of each GCI-ITU pillar is provided in Section 2.

13. "Global Cybersecurity Index 2024," *International Telecommunication Union*, 2024. https://www.itu.int/pub/D-HDB-GCI.01-2024.
14. "Global Cybersecurity Index 2024."

The GCI 2024 utilizes a robust and comprehensive framework laid down below to evaluate the cybersecurity readiness of countries globally. While the assessment strategy is well-structured, there are still areas where further refinements could enhance its effectiveness.

Comprehensive Cybersecurity Framework: The GCI evaluates cybersecurity readiness across five key pillars: Legal, Technical, Organizational, Capacity Development, and Cooperation. It assesses countries' commitment to cybersecurity initiatives, with a particular focus on legislative frameworks, technical preparedness, and cooperative measures to address cyber threats.

Tier-Based Evaluation: The GCI 2024 employs a tier-based system, categorizing countries into five performance tiers, ranging from Tier 1 (Role-Modeling) to Tier 5 (Building). This shift from a purely numerical ranking to a tier-based approach helps highlight regional leaders and pinpoint areas for improvement. It also enables countries to benchmark their progress more effectively against peers.

Regional Disparities and Capacity Gaps: The report underscores significant regional disparities in cybersecurity capabilities. High-income countries typically have well-established national cybersecurity strategies and functional Computer Incident Response Teams (CIRTs). In contrast, lower-income countries often struggle with resource allocation and capacity development, particularly in safeguarding critical infrastructure and advancing child online protection initiatives.

The next section encompasses a critical analysis of the GCI pillars to evaluate the benchmarks—examining their relevance, effectiveness, and the key areas they cover—before analyzing Pakistan's performance in detail.

Critical Analysis of GCI – 2024 – Areas of Strength

Holistic Approach: The GCI's assessment strategy encompasses five key pillars—Legal, Technical, Organizational, Capacity Development, and Cooperation—offering a comprehensive evaluation of a country's cybersecurity posture. This approach ensures that countries are assessed not only on their technical capabilities but also on their legislative frameworks,

institutional support, and international cooperation, all of which are vital for achieving holistic cybersecurity.

Tier-Based System: By implementing a tier-based structure (spanning Tier 1 to Tier 5), the GCI transitions away from a simplistic ranking system, which can often feel limiting or reductive. This approach clusters countries with others at comparable levels of cybersecurity development, shifting the focus from competition over numerical rankings to promoting collaboration and knowledge-sharing within each tier. Additionally, it provides a platform to recognize regional champions—countries that may not yet rank among the global leaders but are making noteworthy progress in advancing their cybersecurity capabilities.

Inclusivity and Global Perspective: The assessment evaluates cybersecurity readiness across a wide range of geopolitical regions, ensuring the index represents both advanced economies and developing nations. This inclusive approach promotes a global dialogue on cybersecurity, enabling countries at various stages of development to learn from each other. The document's focus on capacity-building in under-resourced regions is particularly vital for pursuing equitable global cybersecurity progress.

Critical Analysis of GCI – 2024: Weaknesses and Areas for Improvement

Heavy Emphasis on Policy and Strategy: While the focus on legal and organizational measures is undoubtedly important, the strategy risks placing too much weight on the existence of policies and frameworks, potentially overlooking their actual effectiveness. Simply having a cybersecurity policy or law in place does not ensure proper implementation. The assessment could be strengthened by incorporating a more detailed analysis of how these policies are enforced and their tangible impacts, such as through case studies or post-implementation evaluations.

Overgeneralization in Regional Tiers: While the tier-based system offers several advantages, it may inadvertently lead to overgeneralization within the tiers. For example, two countries in the same tier could face vastly different challenges and possess distinct strengths. One country might excel in capacity building but struggle with technical infrastructure, while anoth-

-er might have advanced technical tools but lack international cooperation. Adding further granularity within the tiers could provide more nuanced insights into each country's unique situation, enabling policymakers to address localized challenges more effectively.

Limited Focus on Emerging Threats: The strategy may face criticism for not adequately addressing emerging cybersecurity threats, such as AI-driven attacks, deepfakes, and nation-state-sponsored cyber warfare. The existing GCI pillars do not explicitly measure how well countries are prepared to tackle next-generation cyber threats, which are likely to become increasingly critical in the coming years. Expanding the technical pillar to include specific metrics on resilience to these emerging threats would create a more forward-looking and comprehensive assessment.

Reliance on Self-Reported Data: The index's heavy reliance on self-reported data introduces potential biases, as countries might overstate their cybersecurity readiness to appear more secure or underreport due to insufficient data collection infrastructure. Incorporating third-party audits or leveraging verifiable cybersecurity incident data could improve the reliability of the assessment and mitigate the subjectivity inherent in self-reported responses.

Lack of Weighting and Prioritization: The five pillars of the GCI are not explicitly weighted, leaving ambiguity about which areas are most critical for a country's overall cybersecurity posture. For instance, technical readiness may be more vital for a country's immediate security than international cooperation, yet both are evaluated as if they carry equal importance. Introducing a weighting system based on factors such as risk exposure or national priorities could make the index more representative of real-world cybersecurity challenges and better aligned with individual country needs.

The previous section provided an overview of prominent international indexes, highlighting the benchmarks Pakistan should aim for and its ranking in each index to assess the country's current standing. The next section examines Pakistan's ICT landscape, its commitment to cybersecurity, current levels of preparedness, and the cyber threats facing the country.

ICT Landscape and Cybersecurity Commitment of Pakistan

The Digital Pakistan agenda has been in place for over two decades. Pakistan's first IT policy was introduced in 2000 and subsequently reviewed in the following years to address areas such as legislation, sectoral digitalization, standardization, infrastructure development, women's empowerment, human resource development, innovation promotion, local hardware manufacturing, research and development, increased software exports, and the establishment of software technology parks.[15] Pakistan's digital policy envisions becoming a strategic enabler for an accelerated digitalization ecosystem, aiming to expand the knowledge-based economy and drive socio-economic growth. However, the policy lacks substantial progress in information security initiatives, with efforts primarily limited to legal measures. These include the legalization of electronic transactions under the Electronic Transactions Ordinance (ETO-2002) and the enactment of cybercrime laws, along with the establishment of a few supporting bodies.

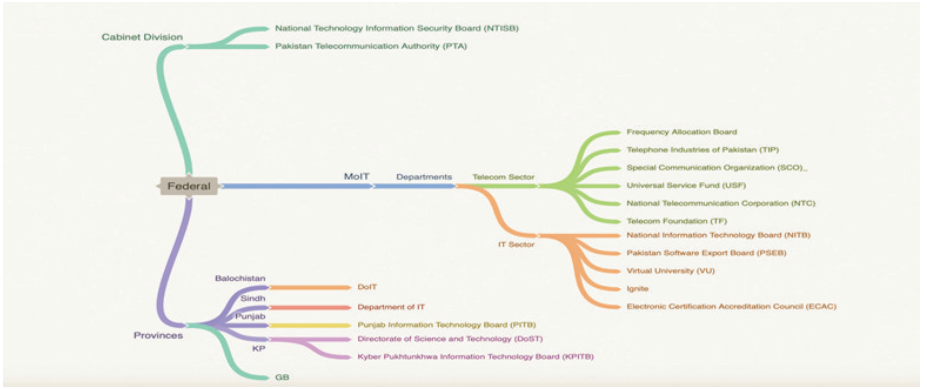

Figure 3: List of Government Departments dealing with Information Technology.
Source: Compiled by the authors (The data is open source and taken from each department's website including the Ministry of Information and Telecommunication website, Punjab Information Technology Board, Directorate of Science and Technology, KP Information Technology Board, National Technology Information Security Board, Universal Service Fund, National Telecommunication Corporation, Telecom Foundation, National Information Technology Board, Pakistan Software Export Board, Ignite, Virtual University, and Electronic Certification Accreditation Council).

The KP Digital Policy, launched in 2018,[16] introduced key initiatives aimed at aligning with Global Data Protection Regulations (GDPR) and implem-

15. "Pakistan Digital Policy," *Ministry of Information Technology*, (2020). https://moib.gov.pk/Downloads/Policy/DIGITAL_PAKISTAN_POLICY%2822-05-2018%29.pdf
16. "Khyber Pakhtunkhwa Digital Policy," *Khyber Pakhtunkhwa Information Technology Board*, (2018).https://kpitb.gov.pk/sites/default/files/Khyber%20Pakhtunkhwa%20Digital%20Policy%202018-2023.pdf

-enting standardized cybersecurity protocols across government departments. The policy also outlined regulations to safeguard data of the citizens, establish appropriate cybersecurity frameworks, and enhance transparency and accountability in digital governance. Similarly, the Punjab Digital Policy also launched in 2018,[17] aimed to transform the province into a knowledge-based economy. While the policy broadly addressed information security, it lacked a specific focus or detailed measures to tackle cybersecurity challenges effectively.

Under the Digital Pakistan policy,[18] Component one focuses on protecting personal data and ensuring online privacy to enhance transparency, security, and confidentiality of information through the implementation of a Data Protection Act. The policy also emphasizes incorporating security and privacy considerations into subsequent frameworks, such as cloud computing, e-government solutions, and the promotion of digital signatures to strengthen data security and authentication.

The National Information Technology Security Board (NTISB)[19] was renamed from the National Communication Security Board (NCSB) to address the needs of emerging technologies. The NCSB was originally established in 1959 under the Ministry of Defense, with the Cabinet Secretary serving as its chairman. The primary objective of the NTISB is to advise the Government of Pakistan on matters related to information and communication technologies and associated initiatives. Although various ministries, departments, and organizations have occasionally followed information security initiatives, however, the digital ecosystem lacks a unified approach or a dedicated body to ensure the security of Pakistan's cyberspace comprehensively.

Imminent Cybersecurity Threat

This section highlights the major cyber threats facing Pakistan, underscor-

17. "Punjab Digital Policy," *Punjab Information Technology Board*, (2018). https://pitb.gov.pk/punjab-digital-policy
18. "Pakistan Digital Policy," *Ministry of Information Technology*, (2020). https://moib.gov.pk/Downloads/Policy/DIGITAL_PAKISTAN_POLICY%2822-05-2018%29.pdf
19. National Communication Security Board (NCSB). https://cabinet.gov.pk/Detail/OWYxZTYxMWQtNDZhMC00M2IyLTk1NDgtODNmNTMxNmNlNGU0..

-ing the country's current state of vulnerability. It not only emphasizes the growing importance of cyber power in modern statecraft but also demonstrates the critical need for robust cybersecurity measures as part of an effective defense mechanism. By including this section, the authors aim to present both the strengths and weaknesses of Pakistan within the digital realm.

Patterns of Cyber Attacks against Pakistan

This section examines the volume of cyberattacks targeting Pakistan, revealing a significant rise in cyber threats. In 2023, the country experienced a 17% increase in cyber threats compared to 2022. One cybersecurity firm reported 16 million cyberattacks in 2023, with 24.4% of internet users in Pakistan affected by these threats.[20] The study further highlighted a 59% surge in banking malware, a 35% increase in trojan attacks, and a 24% rise in ransomware attacks, indicating a worrying trend in the cybersecurity landscape.[21]

Moreover, the US and Russia are reported to be responsible for the highest number of cyberattacks targeting Pakistan, with 40% of these attacks focusing on Port 443 (HTTPS). Ransomware continues to be one of the most frequently used types of malwares in these attacks.[22] Additionally, Indian hackers are often implicated in cyber espionage activities. According to a report by Norman Shark and the Shadow Server Foundation, Indian Advanced Persistent Threats (APTs) consist of small yet highly organized and nationally aligned groups that carry out coordinated attacks on Pakistan's government infrastructure.[23]

20. "Cyber threats increased by 17% in 2023," *Pakistan Tribune*, February 20, 2024. https://tribune.com.pk/story/2457021/cyber-threats-increased-by-17-in-2023#:~:text=Kaspersky%20blocked%2016%20million%20cyberattacks,the%20scale%20of%20modern%20threats.
21. "Cyber threats increased by 17% in 2023."
22. "Threat Intelligence Report," *Rewterz Information Security*, p:11, 2018. https://www.rewterz.com/threat-intelligence-reports/2018-threat-intelligence-report
23. Fagerland, S., M. Krakvik, J. Camp, and A. S. Norman, "Unveiling an Indian Cyberattack Infrastructure," *Norman Shark and Shadowserver Foundation*, 2013.

Major Cyberattacks Targeted Pakistan's Public Infrastructure for the period 2015-2024

Year	Targeted Infrastructure	Technique/Method	Impact
2015	Gateway Exchange[24]	Limited DOS	Service of International Trunk call
2016	Pakistani Websites[25]	Defacement as revenge for the Pathankot incident	Reputation Loss
2017	Top civil-military Leadership[26]	Espionage and spying through malware	Identity theft, loss of data privacy
2018	Banking System across Pakistan[27]	Ransomware	Reputation loss, security breach, data hacked, money stolen of more than $6 million
2019	Ministry of Foreign Affairs, Pakistan Army[28]	Website Defacement	Post-Pulwama Reaction / Reputation Loss
2020	K-Electric[29]	Netwalker Ransomware attack	Reputation loss
2023	Pakistan International Airline (PIA)[30]	DDos Attack	Online operations were stopped, and passengers could not access the website
2024	Pakistan Post[31]	Smishing	Stolen thousands of people personal and financial information

Source: Compiled by authors (drawing data from sources mentioned against each threat)

In October 2018, Pakistani banks across the country fell victim to major cyberattacks, suffering losses exceeding $6 million, along with significant data breaches and damage to their reputation.[32]

24. Ghumman, Khawar, "Cyberattacks against govt expose fatal cracks on Pakistan's digital fence," *Dawn Newspaper*, May 20, 2015. https://www.dawn.com/news/1182856
25. "Hacktivism: India vs. Pakistan," *Recorded Future*, February 11, 2016. https://www.recordedfuture.com/india-pakistan-cyber-rivalry/.
26. Khattak, I. "Pakistan Top Target for Foreign Espionage," *Dawn Newspaper*, January 19, 2017. https://www.dawn.com/news/1309413.
27. Qarar, S. "Almost All' Pakistani Banks Hacked in Security Breach," *Dawn Newspaper,* November 6, 2018. https://www.dawn.com/news/1443970.
28. "Pulwama Attack: Pakistani Websites Hacked," *The Times of India*, February 18, 2019. https://timesofindia.indiatimes.com/gadgets-news/pulwama-attack-pakistani-websites-hacked-heres-the-list/articleshow/68042727.cms
29. "K-Electric Services Hit by Cyberattack." *Express Tribune*, September 10, 2020. https://tribune.com.pk/story/2263343/k-electric-services-hit-by-cyberattack
30. Khaitan, Ashish. "Pakistan Cyber Attack, Team UCC Claims to Take Down Pakistan International Airlines," *The Cyber Express,* April 4, 2023. https://thecyberexpress.com/pakistan-cyber-attack-international-airlines/
31. "Smishing Triad Is Targeting Pakistan to Defraud Banking Customers at Scale." *Resecurity*, June 11, 2024. https://www.resecurity.com/blog/article/smishing-triad-is-targeting-pakistan-to-defraud-banking-customers-at-scale.
32. Qarar, S. "Almost All' Pakistani Banks Hacked in Security Breach, Says FIA Cybercrime Head," November 6, 2018. [Online]. Available at: https://www.dawn.com/news/1443970

A month later, in November 2018, over 150,630 payment cards from Habib Bank of Pakistan and 12 other banks were stolen and sold on the dark web.[33] In April 2019, following the Pulwama incident, Indian hackers compromised the official website of Pakistan's Ministry of Foreign Affairs, rendering it inaccessible from several countries outside Pakistan In January 2020, during a cyber-espionage campaign, the Israeli NSO Group targeted numerous Pakistani government officials' mobile phones using spyware. The intended victims included journalists, attorneys, political dissidents, senior foreign government officials, diplomats, and human rights activists.[34]

More recently, K-Electric experienced a severe ransomware attack demanding $38 million, marking one of the most significant cyber incidents. In 2024, the country faced its largest scam of the year, involving a smishing campaign by a cybercriminal group. The attackers sent malicious messages via iMessage and SMS, posing as Pakistan Post, to mobile carrier customers. Their goal was to steal financial and personal information. The templates and codes used in this scam showed clear similarities to those from earlier incidents attributed to the Smishing Triad group.

These patterns illustrate the wide range of cyberattacks targeting Pakistan from both state and non-state actors. According to leading global cybersecurity firms such as Symantec, Pakistan ranks among the top ten most targeted countries globally. This claim is further substantiated by the Snowden documents released in 2013 and 2014, which revealed that the U.S. National Security Agency (NSA) had been spying on Pakistan's civil and military leadership using malware codenamed SECONDATE.

Considering these trends, coupled with the objectives outlined in the Digital Pakistan vision, it is critical to prioritize Pakistan's cybersecurity commitment. Strengthening the core cybersecurity pillars in alignment with the Global Cybersecurity Index is essential for improving resilience and preparedness.

33. Zaidi, E. "Cyber Attackers Steal 150,632 Plastic Cards Data of Three Banks," *The News,* November 17, 2018. https://www.thenews.com.pk/print/394589-cyber-attackers-steal-150-632-plastic-cards-data-of-three-banks.
34. Kirchgaessner, Stephanie, "Israeli Spyware Allegedly Used to Target Pakistani Officials' Phones," *The Guardian*, December 19, 2019. https://www.theguardian.com/world/2019/dec/19/israeli-spyware-allegedly-used-to-target-pakistani-officials-phones.

The next section offers targeted recommendations to address these challenges and strengthen Pakistan's cybersecurity framework.

Pakistan's Cyber Wellness Profile and Policy Recommendations

Pakistan is positioned in the Tier 1 – Role-Modelling category, signifying that it has demonstrated strong cybersecurity measures. Other countries in this tier include Singapore, the US, and the United Kingdom. Countries in this category excel across all five pillars: legal, technical, organizational, capacity development, and cooperation, setting a benchmark for global cybersecurity standards.

When comparing Pakistan with five other countries in Tier 1, Singapore and the United Kingdom stand out due to their strong capacity development initiatives and well-established cybersecurity organizations. Malaysia and India, also in Tier 1, show growing commitments but are still in the process of developing certain technical measures. Turkey, another Tier 1 nation, emphasizes improving its cybersecurity cooperation efforts, particularly about international agreements. Pakistan's progress in implementing foundational cybersecurity regulations and strengthening cooperation mechanisms places it on par with other leading nations in the tier. However, compared to countries like Singapore and the US, Pakistan would benefit from further advancements in technical and organizational measures to achieve a more robust cybersecurity posture.

The GCI 2024 assessment strategy takes a comprehensive approach to evaluating global cybersecurity readiness by focusing on three key elements: *Multi-Pillar Assessment Approach:* Cybersecurity commitments are assessed across five pillars: Legal, Technical, Organizational, Capacity Development, and Cooperation. This multidimensional framework offers a holistic perspective on a country's cybersecurity maturity and highlights strengths and areas needing improvement.

Tier-Based Performance Model: Instead of relying on rank-based systems, the index categorizes countries into tiers (e.g., "Role-Modeling" to "Building"). This approach emphasizes performance trends while minimizing misinterpretation caused by minor score differences often seen in ranking systems.

Capacity Development and Cooperation: The strategy prioritizes raising cybersecurity awareness, skill-building initiatives, and fostering global partnerships. It acknowledges that human expertise and international collaboration are critical to advancing cybersecurity measures worldwide.

Pakistan's response to cyber incidents is largely reactive and impulsive, which stands in contrast to globally established best practices that emphasize proactive and strategic approaches. The country has not actively developed comprehensive information or cybersecurity policies and strategies to safeguard its information assets. This section evaluates Pakistan's existing cybersecurity preparedness based on the GCI of the International Telecommunication Union. It also provides recommendations and actionable strategies tailored for developing countries, focusing on improving Pakistan's cybersecurity posture. These recommendations aim to help Pakistan and similar nations strengthen their information security frameworks and move toward a more robust and proactive cyber defense strategy.

Recommendations

Legal Measures

The Government of Pakistan has taken a few notable legislative steps to address cybersecurity and online safety. Key initiatives include the ETO of 2002 and the Prevention of Electronic Crimes Act (PECA) of 2016. Pakistan also has specific legislation addressing child online protection, though enforcement often relies on broader laws like Section 293 of the Criminal Code. Furthermore, Pakistan is among the countries that have ratified international treaties prohibiting the sale of children, child prostitution, and child pornography, obligating the state to prevent the sexual exploitation and abuse of children. However, the country faces significant challenges in implementing and enforcing these laws. Pakistan lacks a dedicated authority responsible for online child protection, as well as a proper mechanism for reporting such incidents. This institutional gap hinders the effective execution of these legislations and undermines efforts to ensure the safety and security of children in the digital space.

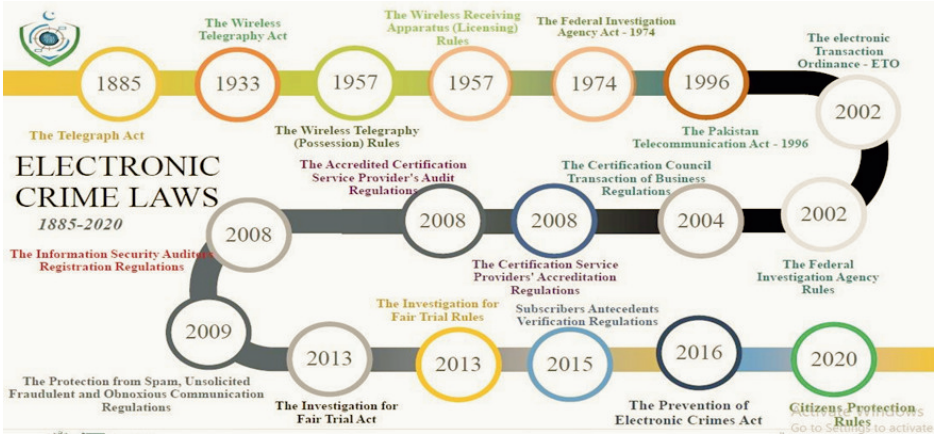

Figure 4: List of Cyber Laws in Pakistan Source: Compiled by Author [35]

The Data Protection Bill holds significant potential for shaping Pakistan's digital IT and e-commerce strategy by fostering economic competitiveness. It seeks to balance creating an enabling environment for Pakistani digital exporters to access foreign markets while safeguarding against the risks of data colonization. However, the bill currently overlooks vulnerable segments of society, such as minors, women, transgender individuals, and minorities. To ensure equitable protections, it is critical to explicitly address these groups within the legislation. Moreover, personal data for minors should be classified as sensitive to provide additional safeguards against exploitation and harm, ensuring their rights and privacy are adequately protected in the digital sphere

In this regard, a constitutional body or independent organization should be created to oversee cybersecurity matters at the national level. Currently, the National CERT operates under the Ministry of Information Technology (MoIT) and derives its authority from CERT rules under the Prevention of Electronic Crimes Act (PECA) 2016. However, a separate legal entity is required to better empower national, sectoral, and regional CERTs, ensuring a more comprehensive and coordinated cybersecurity framework. The Personal Data Protection Bill should be passed on a priority basis to build a robust data protection ecosystem in Pakistan. This legislation is critical for addressing privacy concerns, safeguarding personal information, and enabling the growth of Pakistan's digital economy in alignment with global data protection standards.

35. Zahoor, Rashida and Razi, Naseem, "Cyber-Crimes and Cyber Laws of Pakistan: An Overview," *Research Journal of Arts and Humanities,* Vol.2, o. 2, 2020. https://www.prjah.org/index/php/prjah/article/download/43/27

Technical Measures

Technology is widely regarded as the first line of defense against cyber threats, and in its absence, nation-states remain vulnerable and susceptible to cyberattacks. To mitigate these risks, countries should establish and enforce minimum security criteria and accreditation mechanisms to ensure a baseline level of cybersecurity readiness. These measures should be supported by the establishment of a dedicated national body tasked with focusing on cyber incidents and a centralized framework designed to coordinate responses to such incidents effectively. At present, Pakistan lacks an officially recognized National Information Security Policy, which is a critical gap in its cybersecurity infrastructure. While a cybersecurity policy does exist, it remains in the development phase and has not been fully implemented, leaving the country exposed to growing digital threats. Accelerating the implementation and enhancement of this policy is essential for building a robust national cyber defense framework.

The government or National CERT should develop the capacity to implement technical measures like Security Operations Centers (SOC) and Security Information and Event Management (SIEM) systems at both national and sectoral levels. These measures should ensure the delivery of proactive and reactive cybersecurity services across all critical sectors, enhancing the nation's ability to detect, prevent, and respond to cyber threats.

Building effective cyber threat intelligence (CTI) and situational awareness requires active participation in local and international cyber threat-sharing networks. Platforms like the Forum for Incident Response and Security Teams (FIRST) provide advisory services to protect cyberspace, making them critical for advisory sharing, collaboration, and incident response. Interaction with such networks can strengthen Pakistan's overall security posture.

Information security objectives should be aligned with national security goals while fostering an environment that promotes innovation, free data exchange, and a thriving technology ecosystem. Given the strategic overlap with national security, the defense sector should be treated as a key stakeholder. Many nations have structured their governance models around

the defense sector to ensure better coordination and security integration.

Pakistan should develop a well-defined cybersecurity policy and strategy with clear objectives, a roadmap, and actionable steps. This should include a governance model and defined milestones, a cyber strategy maturity model to track progress, a compliance framework with accountability and responsibility matrices, standards for compliance, quality assurance, and capacity building, a detailed list of services, their impact on sectors, and their timelines for implementation.

Regulating cyberspace should become a priority, with adherence to information security laws, regulations, standards, and guidelines. Compliance efforts will improve data management capabilities, reduce vulnerabilities, and build a stronger security posture across government departments and critical industries. Effective governance, management, enforcement, capacity building, and risk assessment require a comprehensive suite of software and hardware tools. To reduce dependency on foreign technologies, promoting the local electronic industry and encouraging indigenous manufacturing of cybersecurity tools and systems must be prioritized.

This approach will build self-reliance and improve national resilience against external threats. In this regard the is a need to equip national and sectoral Computer Emergency Response Teams (CERTs) with indigenous technologies and capabilities to reduce dependency on foreign tools and solutions. Additionally, the development of a robust policy, technology, and operational mechanism is required to ensure seamless collaboration between CERTs and other organizations responsible for safeguarding digital assets. The creation of a comprehensive cyber governance framework that empowers and enables the broader cybersecurity ecosystem is needed. Furthermore, the formulation of national information assurance (IA) policies and frameworks based on international best practices are needed i.e., UAE IA Regulations, UK Cyber Essentials, and ISO 27001.

Organizational Measures

Organizational measures play a pivotal role in the effective execution of national initiatives, especially those aimed at achieving strategic goals in cyb-

-ersecurity. To ensure success, it is imperative to establish dedicated national agencies tasked with implementing strategies, monitoring progress, and evaluating outcomes. Without a cohesive national-level strategy, a supervisory body, and a clear governance framework, efforts to bolster cybersecurity will remain disjointed, making it impossible to achieve harmony and progress in this critical domain. In Pakistan, the establishment of the Pakistan National CERT (PAK NCERT) marks a significant step in safeguarding the country's digital assets, critical infrastructure, and sensitive information from cyberattacks, cyber terrorism, and cyber espionage. PAK NCERT's core functions include detecting, preventing, and responding to cyber threats; raising national awareness about cybersecurity; promoting research and development in the field; formulating cybersecurity policies and strategies; and fostering international cooperation to tackle cross-border cyber threats.

Operating under the National CERT framework are specialized CERTs designed to address specific areas of cybersecurity. Government CERTs focus on securing government systems and data, while Sectoral CERTs are responsible for protecting key industries such as finance, healthcare, and energy. Provincial CERTs cater to region-specific cybersecurity needs, and Critical Infrastructure CERTs are tasked with safeguarding vital infrastructure, including power grids, telecommunications, and transportation systems. Together, these entities form a comprehensive approach to fortifying Pakistan's cybersecurity landscape.

This body should be formally mandated to lead the development and implementation of the national information security policy and strategy, as well as to devise supporting frameworks, policies, and directives to ensure a secure cyberspace in Pakistan. Additionally, the body should coordinate with all stakeholders involved in the national information security policy and ensure that all key deliverables are achieved. It should also develop technologies, processes, and capacities to plan, monitor, identify, detect, and respond effectively to information security-related activities. The national body can formulate a comprehensive national information and cybersecurity policy, along with a supporting strategy, aligned with national security needs, international norms, and global benchmarks. Thus, a central body should be established to take ownership of the cybersecurity mandate in Pakistan.

While the National CERT is an excellent initiative, it requires robust organizational support and a framework for long-term sustainability. Establishing a legal entity to prioritize the cybersecurity agenda in Pakistan would provide the National CERT with a solid legal and institutional foundation, enabling it to operate effectively and address the country's cybersecurity challenges.

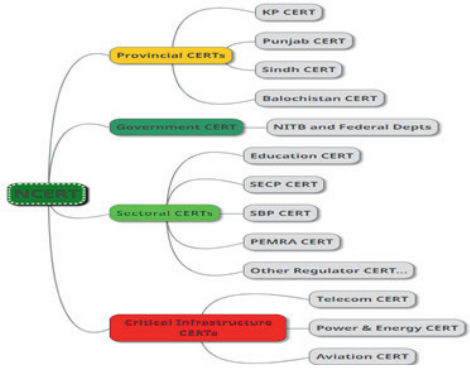

Figure 5: National Computer Emergency Response Team and departments under it. Source: Compiled by authors[36] data drawing from CERT Rules, Ministry of Information Technology and Communication, October 3, 2023).

Capacity Building Measures

Human and institutional capacity building is indispensable for highlighting the significance of cybersecurity, raising awareness, fostering knowledge for systematic solutions, and enhancing the professional human resource pool. Effective capacity building is assessed through key factors such as research and development, training programs, education, certified professionals, and the effectiveness of public sector agencies. However, Pakistan currently lacks a national-level framework for implementing cybersecurity certifications and accrediting national agencies, leaving a critical gap in its ability to systematically develop and sustain a robust cybersecurity ecosystem.

Cloud infrastructure can significantly enhance a country's cybersecurity posture by offering scalable, resilient, and cutting-edge security measures. For Pakistan, which has achieved Tier 1 "Role-Modelling" status in the

36. "CERT Rules," *Ministry of Information Technology and Communication*, October 3, 2023. https://moitt.gov.pk/Detail/MTBmMGQ3NDItOWM2Mi00N2M0LWE1ZGUtMjRlNWJlOGYwZGU0

ITU's GCI 2024, leveraging cloud infrastructure presents an opportunity to further fortify its cybersecurity framework in several keyways:

Scalability and Flexibility: Cloud services provide the ability to scale resources up or down based on demand, ensuring that security measures remain responsive and adaptive to varying threat levels. This eliminates the need for significant capital investment in infrastructure, allowing for a cost-effective and efficient approach to cybersecurity.

Advanced Security Features: Leading cloud providers offer built-in security tools, including encryption, identity and access management, and continuous monitoring. These features are often more robust and comprehensive than traditional on-premises solutions, providing enhanced protection against evolving cybersecurity threats.

Regular Updates and Patch Management: Cloud providers ensure timely management and deployment of security patches, minimizing vulnerabilities associated with outdated software and enhancing overall system security.

Disaster Recovery and Business Continuity: Cloud infrastructure provides robust disaster recovery solutions, ensuring data integrity and availability even during cyber incidents.

Cost Efficiency: Utilizing cloud services allows organizations to reduce expenses associated with maintaining physical hardware, enabling them to allocate resources more effectively toward enhancing security protocols.

For Pakistan, integrating cloud infrastructure aligns seamlessly with its ongoing cybersecurity initiatives while addressing critical areas for improvement. One, Cloud platforms can support training and development programs, contributing to the creation of a skilled cybersecurity workforce capable of addressing emerging threats; Two, Cloud-based security solutions can significantly improve incident response capabilities and enable real-time threat detection, bolstering Pakistan's cybersecurity framework; Three, Cloud services facilitate enhanced collaboration between public and private sectors, promoting information sharing and coordinated responses to cyber threats, which are essential for a

resilient cybersecurity ecosystem. By strategically adopting cloud infrastructure, Pakistan can significantly strengthen its cybersecurity defenses, maintain its prestigious Tier 1 "Role-Modelling" status in the ITU's GCI, and set an example for other nations aspiring to enhance their cybersecurity frameworks.

Thus, a comprehensive framework to address the cyber skill gap is essential and should be adopted by the Higher Education Commission (HEC) and other skill development bodies, such as NAVTTC and similar organizations. The National Institute of Standards and Technology (NIST) has developed an effective model for capacity building in cybersecurity, known as the National Initiative for Cybersecurity Education (NICE), which can serve as a valuable reference for such efforts. In addition to institutional initiatives, public awareness campaigns play a vital role. PAK-CERT actively engages in disseminating cybersecurity awareness through advertisements and special promotional campaigns, ensuring that the public is educated about cybersecurity risks and best practices.

Pakistan should prioritize the dynamic nature of technology and its implications for national security. Recognizing the ever-evolving threat landscape, efforts are underway in research and development (R&D) to stay ahead of these challenges. A significant step in this direction is the establishment of the National Cybersecurity Center (NCCS) under Air University, Islamabad, which has set up 12 advanced laboratories across the country. These labs aim to strengthen Pakistan's cybersecurity capabilities through innovative research and skill development. Additionally, further initiatives are expected to foster indigenous solutions through collaboration with the local industry, ensuring that Pakistan develops a self-reliant and robust cybersecurity ecosystem.

The Cloud Policy approved three years ago, requires further operationalization through the establishment of policies and an enabling framework for cloud operators to effectively conduct business in Pakistan. This step is crucial for the public sector to harness the full potential of regulated public clouds and thrive in a cloud-powered digital ecosystem. Adopting agile technology models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) in the public sector can only be achieved if the Public Procurement Regulatory Author-

-ity (PPRA) simplifies and streamlines cloud procurement processes for government entities. Such reforms would not only lower technology adoption costs by 70-80% but also significantly reduce deployment timelines, enabling faster and more efficient technology integration across the public sector.

Cloud computing enhances cybersecurity by enabling organizations to develop, deploy, and operate secure technology solutions more efficiently. To maximize these benefits, the proposed centralized cyber body should take the lead in facilitating and promoting the adoption of cloud-based cybersecurity solutions. The demand and supply gap in the digital skills market, particularly in the cybersecurity industry, is widening. To address this challenge, the HEC and the proposed cybersecurity body must collaborate closely to promote local talent and foster indigenous research and development.

Cooperation Measures

Dealing with cybercrime necessitates a multi-stakeholder approach, both domestically and internationally, with active input from all relevant parties. These efforts are assessed based on the effectiveness of cooperative frameworks, partnerships, and information-sharing networks. A key objective of the recently established PAK-CERT is to foster international cooperation with other global CERTs, enhancing Pakistan's ability to address cross-border cybersecurity challenges. Pakistan is also a member of the ITU-IMPACT initiative, providing quick access to its cybersecurity-relevant services. Additionally, the country secured a four-year term (2018-2022) on the ITU Administrative Council, becoming one of the thirteen nations elected to this trans-governmental body from the Asia and Australia regions. Pakistan is also a member of the Asia Pacific Security Incident Response Coordination Working Group (ASPIRC-WG). These memberships and partnerships contribute significantly to strengthening Pakistan's cybersecurity profile, particularly in cooperative measures and international collaboration.

The Government of Pakistan is actively working to engage in various international mechanisms related to cybersecurity. However, a more focused effort is required to align these initiatives with international bodies

and standards. By channeling its potential effectively, Pakistan can address capacity-building and cooperation challenges, thereby enhancing its global standing and readiness in the cybersecurity domain.

Pakistan should prioritize the initiation of bilateral and multilateral agreements with countries and entities that hold and process data belonging to Pakistani citizens. To strengthen its cybersecurity framework, Pakistan could also collaborate with China to launch capacity-building programs focused on training research and development. Furthermore, the government should foster public-private partnerships with locally established companies to enhance capacity in the cybersecurity domain. Notably, the approval of the Mutual Legal Assistance (Criminal Matters) Act in 2020 provides a robust legal foundation for facilitating cooperation and coordination with both domestic and international stakeholders.

The government should actively pursue inter-agency partnerships and agreements among various governmental bodies to strengthen coordination and collaboration in the realm of cybersecurity. Such partnerships are vital for creating a unified approach to addressing cyber threats and enhancing national resilience. Under PAK-CERT, fostering international cooperation is a key objective. This initiative not only facilitates the development of advanced cybersecurity capabilities but also supports the sharing of cyber threat intelligence.

Pakistan should establish strong linkages with other countries and international bodies to facilitate the exchange of information on cyber threats and collaborate on cybersecurity and data protection initiatives. In this way, Pakistan can leverage its cybersecurity and data protection capabilities as key tools for cyber diplomacy.

Conclusion

Pakistan's geopolitical situation presents unique challenges, having been at the center of various disruptive events over the past three to four decades. Despite these challenges, the emergence of information technology as a critical driver of national development provided an opportunity for Pakistan to leverage its potential to its advantage. Unfortunately, this potential has not been fully realized.

Cybersecurity, recognized globally as the fourth dimension of warfare, remains an area of concern for Pakistan. The country's information security posture is not encouraging, given the increasing threats tied to digital transformation, data sovereignty, and digital access. Pakistan is frequently targeted by cybercriminals, facing challenges such as financial losses. These threats underscore the urgent need to establish core information security capabilities to protect the country's critical assets.

The cyberwarfare landscape is intensifying, and without a long-lasting and comprehensive mechanism to safeguard its CIs and other high-value assets, Pakistan remains vulnerable. This paper reviews the reasons behind Pakistan's current information security challenges and explores its potential to improve its cybersecurity ranking in global indexes.

As the fifth most populous nation, with an average age of around 22 years, Pakistan has significant potential to expand its ICT sector and address the digital divide. Focusing on information security as a national priority will enable Pakistan to strengthen its ICT commitment, build capacity, and drive socio-economic growth. Currently, Pakistan lags its regional competitors in both ICT growth and information security rankings. Prioritizing ICT development and integrating key economic growth indicators into its strategic vision will ensure a smoother digital transition and help Pakistan compete on the global stage.