Article

A Hybrid Analytical Framework for Enhancing Cybersecurity in Underdeveloped Countries

Sardar Muhammad Ali * , Abdul Razzaq , Haider Abbass , Muhammad Yousaf , Rafi us Shan

Posted Date: 18 October 2024

doi: 10.20944/preprints202410.1442.v1

Keywords: Cybersecurity; Global Cybersecurity Index; Data Envelopment Analysis; Benchmarking

Article

A Hybrid Analytical Framework for Enhancing Cybersecurity in Underdeveloped Countries

Sardar Muhammad Ali [1,*], Abdul Razzaque [2,†], Haider Abbass [3,†],Muhammad Yousaf [4,†] and Rafi Us Shan [5,†]

[1] Information Security, National University Of Sciences and Technology,Sector H-12, Islamabad, 44000, Islamabad, Pakistan.

[2] Head of Department for Quantum Information Sciences, National University Of Sciences and Technology, Sector H-12, Islamabad, 44000,Islamabad, Pakistan; abdul.razzaq@mcs.edu.pk

[3] Head of Information Security Department, National University Of Science and Technology, H-12, Islamabad, 44000, Islamabad, Pakistan; haider@ mcs.edu.pk

[4] Head of Department, Department of Cybersecurity and Data Science,Riphah Institute of Systems Engineering (RISE), Riphah International University, H-12, Islamabad, 44000, Islamabad, Pakistan; muhammad.yousaf@riphah.edu.pk

[5] Faculty member of Computer Information Science, Higher Colleges OfTechnology, D54, Academic City, 97154, Dubai, United Arab Emirates; rshan@hct.ac.ae

* Correspondence: smali79@yahoo.com

† These authors contributed equally to this work.

Abstract: This paper presents an approach to assess and improve the cybersecurity infrastructure of developing countries. We have highlighted and addressed the critical gaps through a hybrid approach encompassing SWOT analysis, benchmarking using Data Envelopment Analysis (DEA) and, Root Cause Analysis (RCA). This approach has provided a strong basis for evaluating cybersecurity performance by combining qualitative insights with quantitative metrics. As a case study, we have compared an underdeveloped country's (Pakistan) cybersecurity posture to five highly developed countries (Lithuania, Estonia, Singapore, Spain, and Norway). Our analysis has identified cybersecurity shortcomings and provided actionable recommendations within a flexible framework, applicable for all developing countries to identify and address vulnerabilities, and align their cybersecurity infrastructure with international standards.

Keywords: cybersecurity; global cybersecurity index; data envelopment analysis; benchmarking

1. Introduction

International Telecommunications Union (ITU) defines cybersecurity as "A set of parameters and collection of tools, policies, security concepts, security measures, guidelines, risk management approach, training, best practices, technology that can be used to safeguard the cyberspace and organization along with user assets"[1]. This broad term emphasizes how crucial it is to secure not just the technological domain of cyberspace but organizational and personal aspects as well. Broad repercussions result from a cybersecurity breach that jeopardizes an information system's availability, confidentiality, integrity, or security policies.[2]

Cybercrimes transcend borders, causing billions of dollars in global damages. Ransomware, phishing, DOS attacks, and unauthorized access continue to rise, exacerbating the threat to international security[3] With increased digital transformations, developing nations are facingcyber threats that may hamper their economic development and disrupt thefinancial system on a global scale. Developing nations have crossed the Internet penetration threshold of 10% [4]. The global cost of cybercrime is projected to reach more than $10.5 trillion annually by2025, a significant increase from $3 trillion in 2015. A few developing nations are now taking the required actions to fortify the global cybersecurity ecosystem bysystematically tackling related threats.[5]The Least Developed

Countries (LDCs), recognized by the UnitedNations since 1971 as economically themost vulnerable nations are least prepared for cyber threats. The LDCs, witha substantial population of about 13% ofthe world population, show the biggestgap in cybersecurity not only due totheir limited access to the internet andinadequate cybersecurity strategies butalso due to their overall economic performance where they only contribute1.3% to the global GDP and less than1% to the global trade. To date (2024),there are 46 Least Developed Countries(LDCs), comprising 33 countries from Africa, 8 from Asia, 3 from Oceania, andone country from Latin America and the Caribbean[5].

Despite significant progress, these countries face a substantial digital divide. In 2022, approximately 407 million people, or 36% of the population in LDCs, were using the internet, compared to theglobal average of 66%. This still leaves 720 million people offline, representing27% of the global offline population, despite LDCs accounting for only 14%of the world's population. Use of the internet in LDCs has increased exponentially from 4% to 36% of the population,with an impressive annual growth rate (CAGR) of 22% much higher than the global average of 7.2%. Since the internet security penetration has increased, therefore, the rate of growth has slowed.Between 2019 and 2022, growth rates ranged from 13 to 17% and decreased from 23% to 39%observed between 2011 and 2018. The data underscores both the significant strides made in internet access across LDCs and the ongoingchallenge of bridging the digital divide, as a large portion of the population remains disconnected from the internet. With limited access to the internet and insufficient cybersecurity strategies, thesenations are highly susceptible to cyber threats. The Committee for Development Policy (CDP) uses indices such as thegross national income (GNI) per capita, Human Assets Index (HAI), and Economic and Environmental Vulnerability Index (EVI) to assess the progress and challenges faced by LDCs, highlighting the gaps in their preparedness for cyber threats.[6]

A country's cybersecurity ecosystemis shaped by its reliance on ICT infrastructure and its vulnerability, which is caused by both technological and social factors.[7]

The rapid digitization of each sector has added to these threats, necessitating cybersecurity as a top priority for both enterprises and governments.[8–10] Although it encouraged innovation and expansion, digital transformation has also made systems more vulnerable to cyberattacks. This change was accelerated by the COVID-19 epidemic, which forced governments and businesses to reconsider their methods of operation and, as a result, raised awareness of the significance of digital security [11–15]

The need to enhance data security measures at the international level is underscored by the rise in sophisticated cyberattacks against private enterprises, government agencies, and key infrastructure that the world has observed. [16]

Cybersecurity indices are compiledto assess the state of information security, cybersecurity, as well as the levelof protection from the threats. Global cybersecurity indices include cybersecurity indices that are related tothe assessment (indexing, ranking) ofcountries on the activities of state institutions. Global cybersecurity indicesinclude the Digital Economy and SocietyIndex (DESI), the Global Cybersecurity Index (GCI), the National Cybersecurity Index (NCSI), and the National Cyber Power Index (NCPI). The developers of global cybersecurity indices are usually global and international organizations such as; the European Commission (EC) and ITU. This diverse representation highlights the multifaceted nature of cybersecurity challenges and the tailored approaches adopted, underscoring the importance of international collaboration, knowledge-sharing, and leveragingthe policies, practices, and initiatives of leading nations to enhance global cyber resilience and address evolving threats[17–19].

GCI is an authentic resource thatevaluates cybersecurity readiness across the world including 194 member states using five types of criteria as given below[20]:

1. Organizational Measures

- National coordination institutions
- Cybercrime management policies
- Cybersecurity development strategies

2. Legal Measures

- Cybersecurity laws and regulations
- Cybercrime laws and regulations

3. Technological Measures

- Technical institutions for cybersecurity
- Cybersecurity standards and frame-works
- Cybercrime prevention technologies

4. Capacity Development Measures

- Research and development programs
- Awareness-raising campaigns
- Education and training programs
- Certified cybersecurity professionals
- Public sector agencies for capacitydevelopment

5. Collaboration Measures

- National partnerships
- Regional cooperation frameworks
- Global information-sharingnetworks
- International partnerships and agreements

The methodology used in the 5th edition of GCI(2024) is a Tier-based modelas given below:

- Tier 1 (T1) Role-modelling $95 \leq x \leq 100$
- Tier 2 (T2) Advancing $85 \leq x \leq 95$
- Tier 3 (T3) Establishing $55 \leq x \leq 85$
- Tier 4 (T4) Evolving $20 \leq x \leq 55$
- Tier 5 (T5) Building $0 \leq x \leq 20$

GCI is being increasingly used as a benchmark to enable countries to identify areas of improvement, alongside incorporating best practices and simultaneously enhancing awareness among stakeholders.

The current analysis of the GCI revealsstark differences between various regionswhen it comes to cybersecurity readiness.The readiness levels from the highest tothe lowest are as follows: At the top ofthe list is Europe with the highest GCIranking, second is the Asia-Pacific region,while Africa and North America are atthe bottom of the list with the lowestrankings. It exhibits their vulnerabilitythat demands targeted interventions[20].We proposed a three-layered novel Hybrid Analytical Framework forEnhancing cybersecurity in Underdeveloped Countries. We used the DataEnvelopment Analysis (DEA) model; amodel that assesses relative efficiencyin this context by comparing one ofthe underdeveloped countries (Pakistan)against the best-practicing countries of cybersecurity including Lithuania, Estonia, Singapore, Spain, and Norway acrossfive GCI pillars model. The research willprovide robust and targeted interventions using the DAE model to strengthenoverall cybersecurity and safe global cyberspace [21–23].

Our unique and robust framework is the best suited to improve cybersecurity in underdeveloped countries, with specialemphasis on Pakistan which is categorized as an LDC. The remainder of thepaper is organized as follows: Section 2 reviews the related work. We described the Research Methodology in Section 3, and a case study on Pakistan to expound the application of our framework is presented in Section 4. We presented ourResults in Section 5, in Section 6 we conducted a discussion, and in Section 7, We presented recommendations. We summarised our conclusion in Section 8 and indicated directions for the future work in9.

2. Literature Review

In the literature on national cybersecuritystrategies (NCSSs), selected countries have developed comprehensive frameworks to address cybersecurity threats.

Lithuania's cybersecurity framework is comprehensive and well-aligned withEU directives. These legal foundations are overseen by the Ministry of National Defence which ensures compliance with the EU's Network and Information Security (NIS) Directive. However, there is room for improvement in stakeholderinvolvement during the preparation of strategic documents. In terms of capacity building, Lithuania has initiated university-level cybersecurity programs and conducts regular national cybersecurity exercises. The demand for cybersecurity specialists remains high, and public awareness campaigns are not widely reported. Internationally, Lithuania maintains strong cooperation with the EU, NATO, the UN, and the organizations of the Baltic[24,25]. Lithuania has established technical institutions such as the National Cyber Security Centre (NCSC) along with the National Computer Emergency Response Team (CERT-LT) to manage cybersecurity incidents, though the integration of cybersecurity research and education remains a challenge due to the country's relatively late entry in the EU[26,27]. Organizationally, the Ministry of National Defence collaborates with other governing bodies, and the Cyber Security Council fosters PublicPrivate Partnerships (PPPs), although specific incentives for these collaborationsare lacking [28]. GCI 2024 ranking of Lithuania is shown in Figure **??**.

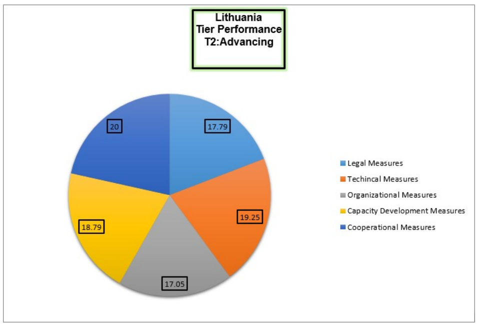

Figure 1. Lithuania performance in GCI 2024.

Estonia's cybersecurity framework is robust in the Cybersecurity Law. It issupported by the data protection and cybercrime policies, and the policy provided by the Ministry of Economy and Communications. At the international level, Estonia is prominent as it hosts theNATO Cooperative Cyber Defense Center of Excellence (CCDCOE) and participates in the EU's cybersecurity efforts. However, dependence on foreign IT products and fragmented efforts to raise publicawareness are cited as challenges [29].Estonia uses advanced technologies such as the X-Road platform and relies on theEstonian Information Systems Authority(RIA) for coordination amongst publicand private sectors[30]. Capacity building is emphasized through the Cyber Defence Unit and educational initiatives at Tallinn University of Technology. GCI 2024 ranking of Estonia is shown in Figure 2.

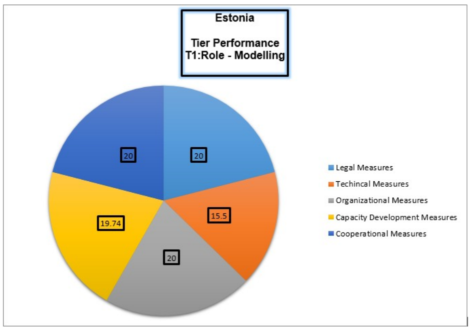

Figure 2. Estonia performance in GCI 2024.

Singapore emphasizes quick identification and required actions to contain the damages caused by cybersecurity incidents, with the National Computer Emergency Response Team (CERT) playing acritical role in managing such incidents. Key initiatives like GoSafeOnline and the Public Cyber Outreach & Resilience Programme (PCORP) are in place toraise public awareness and understanding of cybersecurity issues. Singapore stresses more on research and development (R&D) in cybersecurity, particularly through its universities. Singapore University of Technology and Design (SUTD) leads the way in state-of-theart cybersecurity research. The specialized curricula developed at these institutions help to ensure that Singapore remains at the forefront of cybersecurity education and innovation[26–28].Cybersecurity Act of 2018, which mandates protections for vital information infrastructure serves as the foundation of Singapore's cybersecurity architecture.Leading national efforts, the Cyber Security Agency (CSA) of Singapore employs cutting-edge AI-driven threat detection technologies and promotes R&D. The objective of capacity-building programs like SG Cyber Talent and the Cybersecurity Development Program is to producea workforce with the necessary skills. Singapore participates in international cybersecurity partnerships and collaborations, such as the ASEAN Cyber Capacity Program (ACCP), and alliances with international institutions such as TheEuropean Union Agency for Cybersecurity (ENISA). In addition to enforcing rules and regulations, CSA coordinates the national plan that was created in 2016 [31]. GCI 2024 ranking of Singapore is asshown in Figure 3.

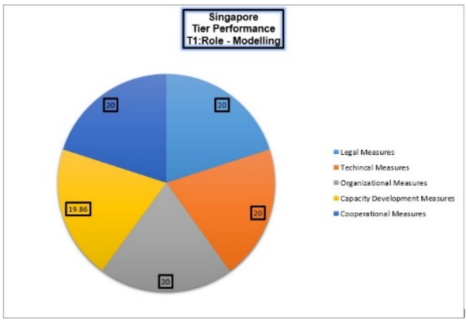

Figure 3. Singapore performance in GCI2024.

Spain aims to strengthen cybersecurity Research and development through initiatives in universities and businesses, supported by incentive mechanisms to foster innovation, especially in small businesses. Internationally, Spain maintains multilateral and bilateral cooperation with the UN, EU, NATO, and other entities Public-private partnerships (PPPs) are a key part of Spain's strategy, as shown by the National Cybersecurity Forum, which improves collaboration between the public and private sectors. While Spain emphasizes training and education in its strategy, specific actions are less detailed comparedto other nations[26,27]. However, public awareness initiatives are not extensively detailed[29]. Spain's cybersecurity is based on the National Security System (ENS) and the General Data Protection Regulation (GDPR) for fortifying its cybersecurity system. Furthermore, there is a National Cybersecurity Council which coordinates the National Cybersecurity Institute (INCIBE) and The National Cryptologic Centre (CCN). The INCIBE mainly supervises the threat intelligence and cyber defense in the country. Capacity-building initiatives in Spain include professional training and public awareness campaigns, although these efforts lack detailed descriptions[32,33]. Spain is actively engaged in European and international cybersecurity cooperation, participating in the NIS Cooperation Group and collaborating with NATO. Spain developed its cybersecurity strategies in 2013 and 2019, led by the National Security Council, with broad stakeholder involvement from government, academia, and business sectors [34]. GCI 2024 ranking of Singapore is as shown in Figure 4.

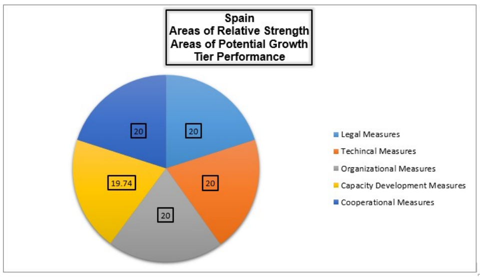

Figure 4. Spain performance in GCI 2024.

The Norwegian National Security Authority (NSM), along with a nationalCERT, is tasked with managing technical infrastructure and responding to cyber incidents. Norway's approach involves engaging private and public sector stakeholders through workshops and conferences, but specific public awareness campaigns and educational programs are not detailed. Despite its proactive cybersecurity stance, the available literature does not specifically mention Research and Development programs or incentive mechanisms[26,27].

Norway's cybersecurity strategy, encapsulated in its National Cyber Security Strategy, focuses on safeguarding critical infrastructure and adhering to international standards, including the GDPR. NSM coordinates cybersecurity efforts across various governmental ministries and the private sector, ensuring effective policy enforcement. Capacity-building efforts are driven by the National Cybersecurity Centre, which provides training and resources to enhance Norway's cybersecurity capabilities. Since its first cybersecurity strategy in 2003, Norway has produced four strategies, with updates in 2007, 2012, and 2019, developed in collaboration with the United States and other international partners. Internationally, Norway engages in bilateral and multilateral collaborations, including partnerships with NATO, the UN, the EU,the OECD, and the OSCE. Although public-private partnerships (PPP) are acknowledged, there are no detailed references to current or future PPP initiatives. [35]. GCI 2024 ranking of Norway is as shown in Figure 5.

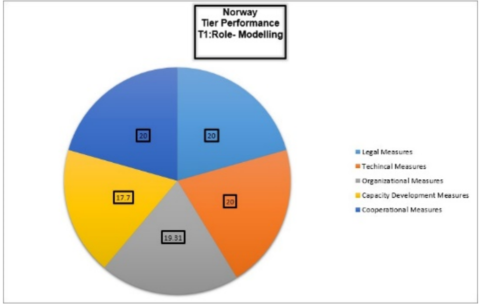

Figure 5. Norway performance in GCI 2024.

Pakistan's cybersecurity cybersecurity strategy is based on the Prevention of Electronic Crimes Act (PECA) 2016and the National Cyber Security Policy (NCSP) 2021. PECA 2016 Provideslegal measures to combat cybercrimes,cyber terrorism, and data breaches.NCSP 2021 Primarily Focuses on securing digital infrastructure and fostering a safe online environment. NR3C is a key institution used for the Investigation of cybercrimes and the development of technical expertise. PakCERT deals with incident response and coordinates cybersecurity efforts. PTA is responsible for internet governance and enforcement of cybersecurity regulations.

The Ministry of IT and Telecommunications plays a crucial role in implementing and enforcing cybersecurity measures. Capacity building is a priority for Pakistan. Training programs are designed for law enforcement and cybersecurity professionals to improve their skills and effectiveness in addressing cyber threats. In terms of cooperation, Pakistan emphasizes regional partnerships, particularly within the South Asian Association for Regional Cooperation (SAARC), to address cross-border cyber threats and collaborate on cybersecurity initiatives [36]. Computer Emergency Response Team (CERT) or Computer Incident Response Team (CIRT) is essential for dealing with cyber incidents. These teams are responsible foridentifying and responding to security incidents, which is critical to minimizingdamage and mitigating risk.[26,36] GCI2024 ranking of Pakistan is as shown in Figure 6.

Previous studies on NCSSs havemainly focused on cross-comparisonsurveys and thematic analysis like [37] reviewed ten NCSSs, in 2013, further reviewed expanded to nineteen strategies from eighteen countries. These are inconsistencies in cybersecurity definitions, action plans, and international cooperation[38]. Lehto in [39]carried out research that analyzed eight nations'threats, definitions, and objectives using the five-fold classification model of cybercrime, cyber espionage, cyber activism,cyber terrorism, and cyber warfare. The research found significant variance inthe depth and scope of the cybersecurity strategies and the differences in the emphasis and priorities placed on the private sector, citizen perspective, and public administration. Similarly, a comparative analysis of the NCSS of six nations was carried out, and the outcome observed was in variations in the nations' focus ranging from the economicimpact of cyber incidents to cyberattack prevention on critical sectors. A lack of methodology in evaluating the strategies was outcome[40]International comparative study on cyber security strategy was carried out with an emphasis on public-private partnerships and how the institutional framework ofthe partnership was established. The study noted that public-private partnerships are strengthened under the Government's authority to respond effectively to cyber security accidents. A paradigm shift in government intervention in the private sector was observed, stating a change from voluntary to enforced self-regulation. The scope of the research was, however, limited to three nations[41]. The NCSS review of fifty-four countries focused on nationalsecurity, jurisprudence, and politics was carried out. It was observed that theNCSS supports national security considering the benefits and risks associated with internet usage[42]. A comparative analysis of twenty countries based on technical, policy-related, legal, and operational measures was carried outusing the ITU's cyber security ranking. The research found that although there were common aims and objectives, therewere also considerable differences in the scope and approach of the strategies. The study gave detailed recommendations to consider when developing an NCSS and concluded that three of the nations' strategies were better than the rest[43]. Sixty NCSS were analyzed and the authors, who used a hierarchical clustering method, noticed similarities between NCSS developed by EU and NATO members. A common focus of the majority of the NCSS was criticalinfrastructure protection, public-private partnership, and defending the IT system of the wider society[44]. Regardless of an increasing volume of research on National Cyber Security Strategies(NCSSs), there remains a critical gap in the literature when it comes to a comprehensive, data-driven analysis that assesses the efficiency of these strategies, particularly using a systematic step-bystep Data Envelopment Analysis (DEA) approach. Much of the work is basedon descriptive or comparative analysis of cybersecurity frameworks but fails to systematically quantify the inefficiencies in these frameworks.

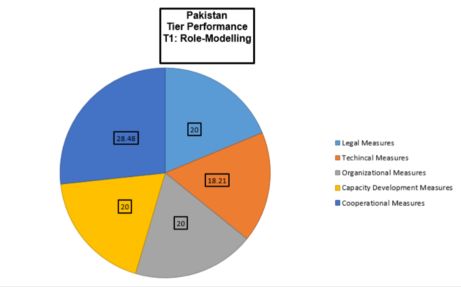

Figure 6. Pakistan performance in GCI2024.

3. Research Methodology

We present a three-layered, model that compares NCSSs from developednations and identifies actionable gaps and inefficiencies in the cybersecurity strategies of developing countries. By combining qualitative benchmarkingwith quantitative DEA, this research provides a targeted focus on the root causes of low-ranked GCI. Furthermore,the integration of SWOT analysis andRoot Cause

doi:10.20944/preprints202410.1442.v1

Analysis (RCA) into the DEA model offers a detailed, structuredapproach for developing nations to targetonly weaknesses in their cybersecurity frameworks. Our framework not onlycompares but provides practical, actionable recommendations, tailored to the geopolitical and economic contexts of least-developed countries. We present a novel framework such comprehensive, efficiency-focused one that empowersunderdeveloped nations to align theircybersecurity ecosystems with global best practices, addressing the void inthe literature for a robust model that improves not just GCI rankings but the overall effectiveness of national cybersecurity strategies. Our proposed model incorporates three key analytical techniques—SWOT analysis, Benchmarking using Data Envelopment Analysis (DEA), and Root Cause Analysis (RCA)—to assess and improve cybersecurity strategies in underdeveloped low-ranked GCI countries as follows.

- SWOT Analysis: We carried outa comprehensive SWOT analysis toidentify the Strengths, Weaknesses, Opportunities, and Threats within Pakistan's cybersecurity ecosystem.
- Benchmarking using DEA: we used DEA for benchmarking Pakistan's cybersecurity framework against best practicesfrom tier-3 countries such as Lithuania, Estonia, Singapore, Spain, and Norway. DEA is used to identify gaps in the five (GCI) pillars—Legal, Technical, Organizational, Capacity Building, and Cooperation—between Pakistan and developed tier-1 countries, thus targetinginefficiencies in the current cybersecurityecosystem.
- Root Cause Analysis (RCA): Inthe final step, we used a Fishbone diagram to conduct RCA, to identify thefundamental reasons behind inefficiencies. We then calculated an Adjustment Factor, which we applied to get a Comprehensive Cybersecurity Effectiveness Score (CCES). This score providesa quantifiable measure of Pakistan's cybersecurity effectiveness and guiding targeted improvements.

The main Contributions of our threelayered Hybrid Analytical Framework inthe Paper are as follows:

- Identification Of Inefficiencies: In underdeveloped nations like Pakistan identify inefficient cybersecurity strategies by comparing them with best practices of the top-ranked Tier 1 countries.
- Quantitative Gap Analysis: To reveal accurate quantitative scores and identify targeted gaps in the five GCI pillars (Legal, Technical, Organizational, Capacity Building, and Cooperation).
- Tailored Recommendations: for improving cybersecurity strategies by aligning with Tier 1 countries, while considering geographical, political, and financial constraints specific to underdeveloped nations.
- Realistic Impact Assessment: Our proposed model provides analysis and assessing a country's cybersecurity posture through the Comprehensive Cybersecurity Effectiveness Score (CCES), helping governments to measure and track improvement effectively.
- GCI Ranking Improvement: By Incorporating the recommendations, underdeveloped countries can improve their cybersecurity ranking in the Global Cybersecurity Index (GCI).

Our proposed research methodology is composed of the following six phases. as shown in Figure 7. A detailed description of each phase is given below.

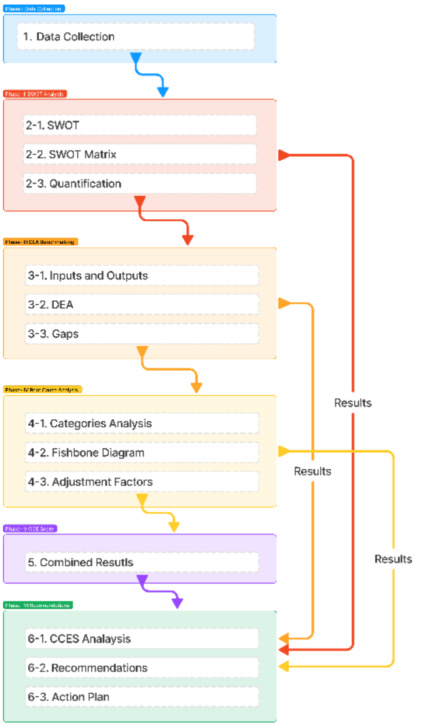

Figure 7. Proposed model methodology and discussed subsequently phase-wise indetails as follows.

3.1. Phase I: Data Collection

With a focus on South Asia, this study primarily uses qualitative methods to better understand the environment around cybersecurity practices in the area. Qualitative research techniques,such as focus groups, in-depth interviews,observations, and document reviews, were employed to produce subjective knowledge pertinent to the study's goals [32,33]. To conduct a holistic assessment of our proposed framework, the primary Data source used in this research is mainly based on ITU's Publications, and the countries are selected from the 2020 GCI normalized scores and declaredas the most committed to cybersecurity in 2018[20]. Secondary data is collected from government publications, websites, books, newspapers, magazines, Google Scholar and government websites wereamong the other sources of secondarydata used for the research review. The countries along with their tier-rating are as shown in Table 1, Pakistan is classifiedas Tier 1 (T1) in cybersecurity. This part is covered in Phase I. As a case study, Pakistan is selected as an underdevelopedcountry as discussed in our introduction, ranked 164th out of 194 nations globally that has a Human DevelopmentIndex (HDI) score of 0.540, placing it in the "low" human development category according to the 2023–2024 study[6,33].Pakistan's cybersecurity ranked 79th in the GCI 2020 after the introduction of Tier tier-based system in GCI 2024 now improved its ranking and is placed on Tier 1 (T1) – Role-Modelling. Estonia, Singapore, Spain, and Norway wereselected since being declared as RoleModels in the 5th edition of GCI 2024 and are developed countries, Lithuania as a developed country was placed in the 6thranked country in GCI 2020 on a normalized score-based system but due to the tier system introduced in 2024 is nowplaced on Tier 2 as discussed in[20,45].

Table 1. Cybersecurity Tier RankingGCI 2024.

Country	Abbreviation	Tier Ratings
Lithuania	LTU	Tier 2 (T2) – Advancing
Estonia	EST	Tier 1 (T1) – Role-Modelling

Singapore	SG	Tier 1 (T1) – Role-Modelling
Spain	ESP	Tier 1 (T1) – Role-Modelling
Norway	NOR	Tier 1 (T1) – Role-Modelling
Pakistan	PAK	Tier 1 (T1) – Role-Modelling

3.1.1. Inclusion Criteria

We used the following inclusion criteria:

1. Language: Articles that matched our search string in English were selectedfor our research.
2. Authenticity: Peer-reviewed literature was taken for Integrity purposes.
3. Privacy: Studies included having privacy protections in their methodologies.

3.1.2. Exclusion Criteria

We used the following exclusion criteria Researchers used the following exclusion criteria.

1. Articles Without Peer Review: Articles without peer review were eliminated from our research.
2. Irrelevant Studies: Irrelevant studies other than cybersecurity in developing nations were eliminated.
3. Lack of Privacy: Research lacking clear privacy guarantees was excluded.

3.2. Phase II: SWOT Analysis

For the implementation of our framework, we conducted a thorough SWOTanalysis to assess and identify Strengths, Weaknesses, Opportunities, and Threats affecting the cybersecurity Eco System of Pakistan as our case study. We compiled information into a matrix to visualize asa SWOT Matrix. The information in the matrix is quantified by assigning scores toidentify strengths and weaknesses as the SWOT Index.

3.3. Phase III: Benchmarking(Data Envelopment Analysis DEA)

We assess Performance and efficiency byidentifying and defining the Input and Output that are relevant to Cybersecurity. We applied the DEA model to measure the efficiency of selected developed countries' strategies by comparing these inputs and output. DEA results are used for identification of efficiency gaps in the cybersecurity ecosystem, these results areused subsequently for highlighting areas where performance can be improved.

3.4. Phase IV. Root CauseAnalysis (RCA)

We analyzed the root causes of the Inefficiencies in underperforming strategies. We created a Fishbone diagram for visualization of root causes and connections between causes and effects. We then used Root cause analysis to calculate an adjustment factor to determine how much change or improvement is required to address the identified gaps.

3.5. Step V: Calculate Comprehensive Cybersecurity Effectiveness Score(CCES)

doi:10.20944/preprints202410.1442.v1

We combined the results from the SWOTanalysis, DEA, and RCA to calculate a Comprehensive Cybersecurity Effectiveness Score (CCES). CCES score reflects the overall effectiveness of the cybersecurity strategy.

3.6. Step VI: Recommendations

The CCES components are broken down to identify specific areas of improvement and insights. Based on the CCES results, specific, actionable recommendations aredeveloped to address the inefficiencies and capitalize on strengths. Finally, a strategic action plan is formulated, outlining steps to improve the cybersecurity ecosystem based on the tailored recommendations.

4. Case Study

In this section, we demonstrate the useof a three-layered efficiency-based framework to assess the efficiency of Pakistan'scybersecurity ecosystem across the fivepillars of the GCI. Pakistan is compared with five developed countries (Lithuania, Estonia, Singapore, Spain, and Norway), and this leads us to identify areas where Pakistan's strategies are underperforming. We use SWOT analysis to gauge internal factors, DEA Benchmarking to measure efficiency, and Root Cause

Analysis (RCA) to address inefficiencies. Finally, a Comprehensive Cybersecurity Effectiveness Score (CCES) is calculated, leading to tailored recommendations for improving Pakistan's cybersecurity strategies and bridging the gap with the developed nations.

4.1. SWOT EvaluationProcedure

Factor Identification: Factors are identified as follows.

4.1.1. Strengths

Resources including infrastructure and a trained labor force.

4.1.2. Weaknesses

Internal shortcomings such as outdated technology

4.1.3. Opportunities

External factors like possible alliances and cutting-edge technologies.

4.1.4. Threats

External threats include increasing cyberattacks and unstable geopoliticalconditions.

4.2. Quantifying the Qualitative Insights

The insights obtained from this investigation are necessary to translate the findings into quantifiable parameters. These findings are converted into quantifiable components that direct the developmentof focused plans for improving cybersecurity in Pakistan by identifying critical features in each sector.

4.3. Benchmarking Using DEA

Using the DEA model, the results of the SWOT analysis were compared to thoseof five developed nations to evaluate cybersecurity measures even more. Usingthe same pillars as the chosen countries, the DEA model makes it easier to compare the effectiveness of Pakistan's cybersecurity activities. Establishing a model that incorporates institutional benchmarking into decision-making is essential, especially when addressing preexisting difficulties and quickly advancing developments in technology. This model groups together a range of parametersbased on predetermined goals, including emergency response capabilities, national cybersecurity risk management, policiesand regulations, governance structure, involved parties, information transfer mechanisms, strategy, and priorities [22,23].

Using the DEA model, the results of the SWOT analysis were compared to thoseof five developed nations to evaluate cybersecurity measures even more. Usingthe same pillars as the chosen countries, the DEA model makes it easier to compare the effectiveness of Pakistan's cybersecurity activities.

4.4. Data Envelopment Analysis (DEA) in Cybersecurity EfficiencyAssessment:

The DEA method is one of the most effective ways to assess relative efficiency when applied in tandem withbest practice models within a reporting group.DMU inputs and outputs arecompared using the non-parametric DEA technique to determine how effective theDMUs are. This study uses the selected countries from Table 1 as DMUs with the growth of cyber defense capabilities performing as the major outcome and other cybersecurity measures servingas inputs.DMU inputs and outputs are compared using the non-parametric DEA technique to determine how effective the DMUs are. This study uses the selected countries from Table 1 as DMUs with the growth of cyber defense capabilities performing as the major outcome and other cybersecurity measures serving as inputs [23].

4.5. Selection of Inputs andOutputs

Inputs and Outputs are selected in accordance with the GCI cybersecurity pillarsas shown in Table 2.

4.6. Scale of Comparison OfSelected Countries

Six countries are compared in the analysis having diverse and rich cybersecurity development levels and geographical regions. The comparison is based on pillars as described in Table 2. The following scale is used for converting qualitative scores into quantitative values. Very High: 4 High: 3 Moderate: 2 Low: 1.

4.7. Input and Output Matrices

The input matrix (X) represents the resources and efforts invested in various cybersecurity pillars. The input scores for each country across the five cybersecurity pillars are shown in the Table 3.

The output matrices used in our Data Envelopment Analysis (DEA) for comparing cybersecurity development across the selected countries are shown in Table 4. The output matrix (Y) reflects the observed outcomes or effectiveness in each area. These matrices are constructed based on the qualitative-to-quantitative conversion.

4.8. Data Envelopment Analysis (DEA) Model

To Find out the comparative efficacy of cybersecurity measures in the selected countries we employed the DEA methodology. The mathematical formulation for this is as follows: For each Decision Making Unit (DMU) j (j = 1,..., K), whereK is the total number of DMUs (selectedcountries in our study), the efficiency score DEA is calculated by

$$E_{\text{DEA}} = \frac{\sum_{m=1}^{M} y_m^j u_m^j}{\sum_{n=1}^{N} x_m^j v_m^j} \tag{1}$$

Subject to

$$E_{\text{DEA}} = \frac{\sum_{m=1}^{M} y_m^j u_m^j}{\sum_{n=1}^{N} x_m^j v_m^j} \leq 1 \text{ for } k = 1, \ldots, K \tag{2}$$

$$u_1, u_2, \ldots, u_M \geq 0 \tag{3}$$

doi:10.20944/preprints202410.1442.v1

$$\text{and } v_1, v_2,\dots, v_N \geq 0 \quad (4)$$

Where:

- y^j is the mth output of the jth Decision Making Unit (DMU)
- x^j is the nth input of the jth DMU
- u_m is the weight given to the $m$thoutput
- v_n is the weight given to the nth input
- M is the number of outputs
- N is the number of inputs

Table 2. Inputs & Outputs based on cybersecurity pillars.

Pillars	Inputs	Outputs
Legal	Legal Framework Development Regulatory Compliance	Effectiveness of Legal Framework Enforcement and Compliance
Technical	Investment in Infrastructure Technical Skill Development	Technical Capabilities Innovation and Upgrades
Organizational	Organizational Structure Coordination Efforts	Efficiency of Organizational Structure Coordination Effectiveness
Capacity Building	Training Programs Public Awareness Campaigns	Skill Development Public Awareness
Cooperation	International Partnerships Collaborative Projects	Strength of International Cooperation Impact of Collaborative Projects

Table 3. Inputs Matrix (X).

Country	Legal	Technical	Organizational	Capacity Building	Cooperation
Lithuania	2	2	2	2	3
Estonia	4	4	4	3	4
Singapore	4	4	4	4	4
Spain	3	3	3	1	3
Norway	4	4	4	1	4
Pakistan	2	1	1	2	2

Table 4. outputs Matrix (Y).

Country	Legal	Technical	Organizational	Capacity Building	Cooperation
Lithuania	3	2	2	2	3
Estonia	4	4	4	3	4
Singapore	4	4	4	4	4
Spain	3	3	3	1	3
Norway	4	4	4	1	4
Pakistan	2	1	1	2	2

In our analysis:

Each country represents a DMU (j = 1,..., 6)

We have five GCI, each with an input andan output (M = N = 5)

The inputs (x^j) and outputs (y^j) are the quantified scores derived from our qualitative assessments, ranging from 1 to 4.

The DEA model searches to maximize the efficiency score E DEA for each country, subject to the constraint that no efficiency score exceeds 1 when the same set of input and output weights is applied to all countries.

4.9. DEA Analysis of National Cybersecurity Strategies Organizational Pillar

The graph represents a (DEA) applied to the organizational infrastructure of national cybersecurity strategies for six countries: Lithuania, Estonia, Singapore, Spain, Norway, and Pakistan. The horizontal and vertical axes represent the Organizational Infrastructure Maturity

Indicators Levels (MILS) of the Strategy, which are used as both the input and output variables in this model.

I. Countries on the Efficiency Frontier:Estonia, Singapore, and Norway have efficiency scores of 4, placing them on the Ro-Le Curve (red dashed line), which represents the efficiency limit. These countries are considered to be utilizing their organizational resources optimally for their cybersecurity strategies.

II. Countries Below the Efficiency Frontier: Lithuania, Spain, and Pakistan fall below the efficiency frontier, indicating inefficiencies in their organizational infrastructure. Their actual performance is compared to projected performance onthe curve (green dashed lines). For example, Pakistan's actual score of 1 is projected to be a score of 2 on the efficiency frontier, illustrating the gap that needs tobe bridged to reach optimal efficiency.

4.9.1. Broad Contours of theEfficiency Frontier

:

I. Pakistan has the lowest organizational infrastructure score (1), indicating significant inefficiencies. To improve, Pakistan would need to centralize its cybersecurity efforts under a unified authority, enhance coordination amongvarious agencies, and streamline decisionmaking processes.

II. Lithuania and Spain are closer to the efficiency frontier but still fall short. Lithuania, with a centralized structure, faces potential bottlenecks in coordination, while Spain, despite good interagency coordination, could benefit from more centralized management to enhance efficiency.

III. Estonia, Singapore, and Norway set benchmarks for cybersecurity organizational effectiveness. These nations' highly collaborative or centralized organizational models enable excellent coordination and efficient cybersecurity policy implementation. The significance of a coordinated, centralized, or integrated approach to conducting national cybersecurity initiatives is emphasized by this report. To increase organizational efficiency, nations such as Pakistan should concentrate on enhancing coordination mechanisms and unifying duties under a single effective leadership.

1. Countries on the Efficiency Frontier: Estonia, Singapore, and Norway with input and output values of 4, aresituated on the efficiency frontier (RoLe Curve). This suggests that they are making the most of their coordination and organizational structures to ensureefficient cybersecurity.

2. Countries Below the Efficiency Frontier: Lithuania, Spain, and Pakistan fall below the efficiency frontier, exhibiting inefficiencies in their organizational structure and fall below the efficiency frontier. Pakistan, for instance, has thelowest score (1), which indicates severe inefficiency.

4.9.2. Detailed Examination ofInefficiencies

:

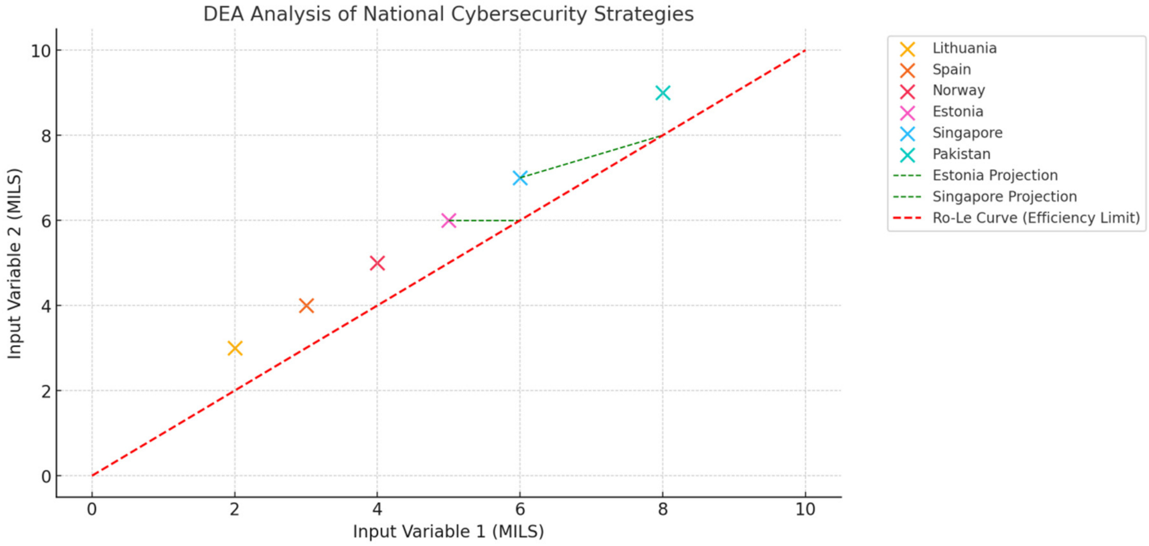

Figure 8. DAE analysis of Cybersecurity Strategies.

Pakistan: Inefficient cybersecurity methods result from a decentralized organization with coordination issues, as seen by the low input and output values. Pakistan must strengthen inter-agency collaboration and centralize its efforts to improve.

Lithuania and Spain: Although these nations are getting closer to the efficiency frontier, they still need to workon strengthening their coordination and organizational structures to achieve the same optimal levels of efficiency as Estonia and Singapore.

Estonia, Singapore, and Norway: Set the standard for organizational efficiency in cybersecurity, due to well-organized systems that support effective cybersecurity processes.

4.10. RCA Process and Fishbone DiagramConstruction

To find inefficiencies in the Five Pillars of GCI, the Root Cause Analysis (RCA) process was used. The process includes:

i. Finding inefficient by examining the DEA output scores.

ii. Identifying probable inefficienciescaused by reviewing the literature.

iii. By Grouping the causes according to their relevance. Creating a Fish-bone Diagram to show the connections andinterdependence between categories andpossible reasons.

4.11. Comprehensive Cybersecurity Effectiveness Score(CCES)

The DEA efficiency ratings, the RCA results, and the quantifiable outputs from the SWOT analysis can all be combined to create the Comprehensive Cybersecurity Effectiveness Score (CCES).

4.11.1. SWOT Index

: The DEA efficiency assessments, the RCA results, and the quantifiable outputs from the SWOT analysis can all be combined to create the Comprehensive Cybersecurity Effectiveness Score (CCES).

$$\text{SWOT\_Index} = w_1 \cdot S_{\text{score}} - w_2 \cdot W_{\text{score}} + w3 \cdot O_{\text{score}} - w4 \cdot T_{\text{score}} \quad (5)$$

Where w1,w2,w3, and w4 are the weights assigned to strengths, weaknesses, opportunities, and threats.

And

Sscore: The total score derived fromthe strengths.

Wscore: The total score that is basedon all of the weaknesses.

Oscore: The total score derived fromall of the opportunities.

Threat score: The scores combinedinto a total score.

4.11.2. Efficiency Score fromDEA (EDEA)

Equation (1) describes the efficiency of a nation's employment in its resources to achieve cybersecurity outcomes.

4.11.3. Root Cause AdjustmentFactor (Radj):

This factor adjusts the score based on the severity and impact of identified root causes. It can be calculated as:

- C_q: Represents the individual root causes identified during the RootCause Analysis (RCA) process.
- w_q: Represents the weight or impactfactor assigned to each root cause C_q.
- $C_q\ w_q$: This is the weighted sum of the root causes. It reflects the overall severity and impact of the root causes identified in a specific country.
- $C_{q(\max)}$: This represents the theoretical maximum value of C_q that could be assigned if the root causes were at their most severe. This value ensures the formula is normalized.

The factor R_{adj} adjusts the CCES downward based on the total severityof the root causes. If the identified rootcauses are severe and impactful, R_{adj} willbe lower, reducing the overall CCES. By dividing by the maximum possible sum of weighted root causes (Max Possible $C_q\ w_q$), the formula ensures that $R_{\text{adj}}$is normalized to a value between 0 and 1.

$$R_{\text{adj}} \approx 1$$

This indicates that the root causes identified are either minimal or have low severity. As a result, there's little to no penalty to the CCES, reflecting a relatively healthy cybersecurity posture from a root cause perspective.

$$R_{\text{adj}} \ll 1$$

This indicates that there are significant and impactful root causes present, which should reduce the CCES. A lower Radj means that the identified root causes are critical and must be addressed urgently.

4.11.4. Comprehensive Cybersecurity Effectiveness Score(CCES)

The CCES can be formulated as a combination of these elements:

$$\text{CCES} = (\text{SWOT Index} \cdot w_s) + (E_{\text{DEA}} \cdot w_e) \cdot R_{\text{adj}} \tag{7}$$

Where:

- w_s: The weight assigned to the SWOTindex.
- w_e: The weight assigned to the DEA efficiency score.

$$\text{CCES} = (\text{SWOT Index} \cdot w_s) + (E\text{DEA} \cdot we) \cdot R\text{adj} \tag{8}$$

To ensure that CCES is on a consistent scale (0 to 1), normalization may berequired as given below:

$$\text{CCES}_{\text{Norm}} = \frac{\text{CCES} - \text{Min CCES}}{\text{Max CCES} - \text{Min CCES}} \tag{9}$$

4.11.5. Providing Recommendations Basedon CCES

Recommendations can be derived byanalyzing the CCES components, particularly where the score is low or where specific weaknesses, inefficiencies, or root causes are identified. Here's how we can approach it:

4.11.6. Analyze CCES Components

- Low SWOT Index: Identify whether weaknesses or threats are driving down the score. Recommendations should focus on addressing these specific areas.
- Low DEA Efficiency Score: Identify resource inefficiencies. Recommendations should focus on optimizing resource allocation and usage.
- High RCA Adjustment Factor: If the RCA reveals critical root causes, these should directly inform the recommendations.

4.11.7. Tailored Recommendations

1 Short-term vs. Long-term: Arrange suggestions according to how long theywill be implemented.
2 Short-term: Use current resources to implement quick gains.
3 Long-term: Strategic projects requirea large amount of money and preparation.

4.11.8. Set priorities

According to how they will affect theimprovement of CCES.

1. Highest priority: actions are those thatdeal with the biggest flaws or inefficiencies.
2. Medium Priority: Less critical actions that nevertheless enhance things overall.
3. Low Priority: Suggestions that canwait until after higher priority measures are taken.

4.11.9. Develop an Action Plan

An action plan for each recommendationis as below:

I. Action: Describe what needs to bedone.
II. Resources: Specify the resourcesneeded.
III. Responsibility: Assign who will beresponsible for implementation.
IV. Timeline: Set a timeline for completion.

4.11.10. Expected Impact

Estimate the improvement in CCES orspecific components.

5. Results

Pakistan's cybersecurity strategies after analysis with benchmarked developedcountries results show huge gaps. Pakistan falls well short in each of the five cybersecurity pillars, according to the DEA analysis. The remaining contributing critical factors in inefficiencies were found by the Root Cause Analysis (RCA), including outdated legal frameworks lack of technical expertise, and lack of international cooperation. These findings highlight how important it isto launch targeted projects to improve Pakistan's cybersecurity infrastructure.

5.1. SWOT Analysis

We carried out SWOT Analysis of Pakistan in which Strengths and Weaknesses as shown in Table 5. While Opportunities and Threats in SWOT analysis in Pakistan perspective are shown in Table 5.1.

Table 5. Strengths and Weaknesses in Cybersecurity Pillars.

Category	Strengths	Weaknesses
Legal	Legislation (PECA 2016)	Fragmented legal framework
Technical	National & Sectoral CERTs	Outdated infrastructure
Organization	Specialized law enforcementunits	Fragmented efforts, Insufficient integration
Capacity Building	Efforts to upgrade forensic science	Lack of facilities for education
Cooperation	Active international engagement	Limited international cooperation

5.2. DEA Bench Marking

We carried out benchmarking to quantify comparison of Pakistan cybersecurity with selected countries as shown in Figure 9

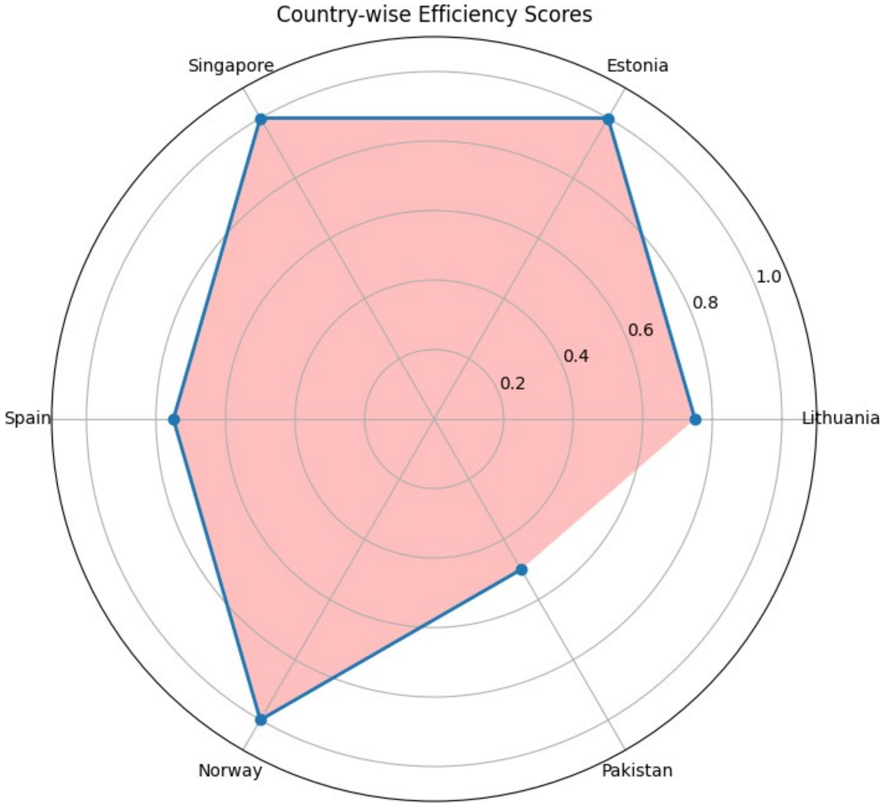

Figure 9. Country-wise Efficiency Scores.

Efficiency Scores by each Country andCategory are shown in Figure 10 below.

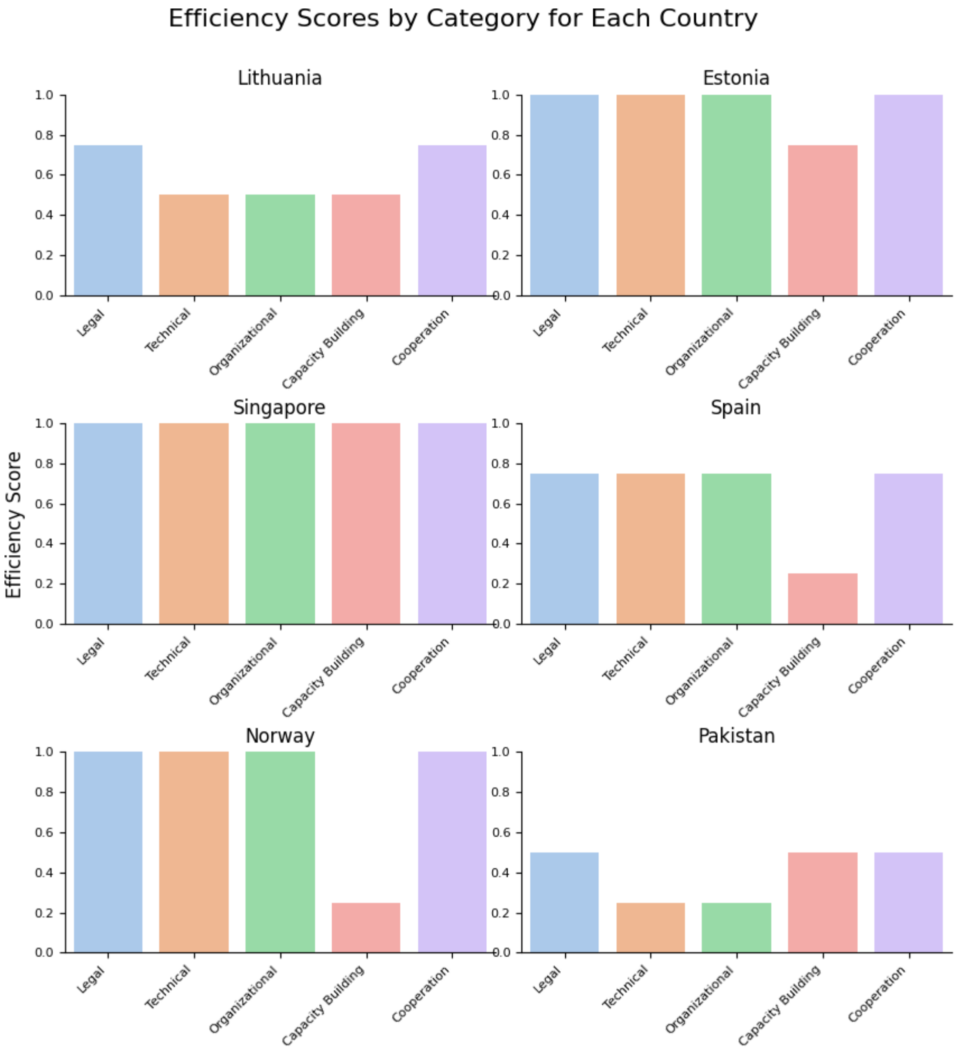

Figure 10. Efficiency Scores by Country and Category.

5.3. Root Cause Analysis(RCA) Results

Outdated policies, delayed court procedures, and a lack of digital tools to streamline legal processes are key weaknesses.Legal system of Pakistan is shown in Figure 11. inadequate staffing levels, insufficient training programs, resistance to organizational change, and unclear roles and responsibilities within cybersecurity teams. Organizational In efficiencies are shown in Figure 13 .

The capacity-building pillar in Pakistan's cybersecurity ecosystem is composed of critical several inefficiencies. Capacity-building inefficiencies are shown in Figure 14.Cooperation efforts of Pakistan's cybersecurity are effected by low stakeholder engagement, weak communication, and a general lack of trust among the key players involved. The basic cause of Pakistan's ineffective cooperation is due to low-scale stakeholder engagementwhich is shown in Figure 15 .

Category	Opportunities	Threats
Legal	Unified legal frameworks	Limited enforcement
Technica	lGlobal collaborations, Regionalized technologies	Risk of increasing cyberattacks
Organiz	ationalStrengthened coordination,International collaboration	Insufficient funding

Capacit Building	yTraining programs, International collaboration	Insufficient funding
Coopera	tiExpanded international cooperation, Global frameworks	Lack of com-prehensivestrategy

5.4. *Comprehensive Cybersecurity Effectiveness Score(CCES)*

We find out CCES by following step by step process as described in the followingsections.

5.4.1. SWOT Analysis Quantification

To evaluate Pakistan's cybersecurity posture a SWOT analysis was performedacross five pillars of GCI each scored outof 10 is shown in Table 6.

5.4.2. Scoring Rationale

Main cause of Inefficiencies in Pakistan's technical infrastructure is dueto a lack of automation and outdated workflows. Inefficiencies in Technical are shown in Figure 12.

Organizational inefficiencies in Pakistan's cybersecurity framework includes Strengths and Opportunities: Higher scores due to positive initiatives and growth potential. Weaknesses and Threats: Lower scores due to significant gaps, challenges, and risks in Pakistan's cybersecurity posture.The Scoring Rationale is elaborated in Table 7.

Table 6. SWOT Analysis Quantification.

Category	Strengths	Weaknesses	Opportunities	Threats
Legal	8	6	8	6
Technical	7	5	7	7
Organizational	7	4	7	5
Capacity Building	6	5	7	6
Cooperative	8	5	8	6
.				

Table 7. Average SWOT Scores.

No.	Category	Score
1	Strengths (S score)	-7.2
2	Weaknesses (W score)	-5.0
3	Opportunities (O score)	-7.4
4	Threats (T score)	-6.0

5.5. *Root Cause AdjustmentFactor R_{adj}*

Table 8 below shows Severity Scores (Cq) range from 1-10. Weights (wq) are assumed equal for simplicity, with a valueof 1. we analyze the adjusted risk valuesacross five pillars as shown in Table 9, therisk value for the legal category is 0.35, while the technical category has a slightlylower value of 0.225.

The Root Cause Adjustment FactorsR_{adj} indicate the degree to which the root causes in each category impact the overall cybersecurity effectiveness. LowerR_{adj} values, such as in the Technical Category, suggest more significant issues thatrequire attention. These factors can beused to adjust the overall cybersecurity effectiveness score, leading to targetedrecommendations for improvement.

Table 8. Severity Scores and Weights.

Category	Sub-Category	Severity Score (Cq)	Weight (wq)
Legal	Policies	8	1
	Procedures	7	1
	People	6	1
	Technology	5	1
Technical	Infrastructure	9	1
	Skills	8	1
	Processes	7	1
	Resources	7	1
Organizational	Structure	6	1
	Culture	7	1
	Processes	6	1
	Resources	7	1
Capacity Building	Training	8	1
	Resources	7	1
	Partnerships	6	1
	Evaluation	6	1
Cooperation	Partnerships	7	1
	Communication	6	1
	Trust	6	1
	Resources	7	1

Table 9. Adjusted Risk Values (R_{adj}).

Category	Adjusted Risk Value (R_{adj})
Legal	0.35
Technical	0.225
Organizational	0.35
Capacity Building	0.325
Cooperation	0.35

5.6. Comprehensive Cybersecurity Effectiveness Score(CCES)

The table below Table 10 presents a detailed breakdown of Five GCI pillars applied to Pakistan's Cyber security ecosystem showing the SWOT Index, EDEA, adjusted risk value (R_{adj}), and the Comprehensive Cybersecurity Effectiveness Score (CCES).

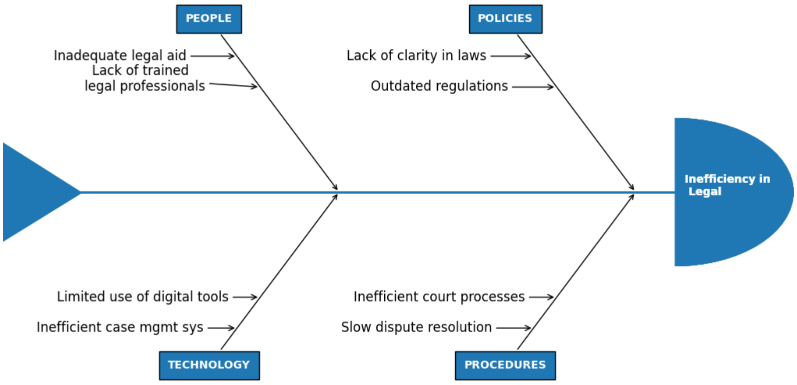

Figure 11. Inefficiency in the Legal frameworks.

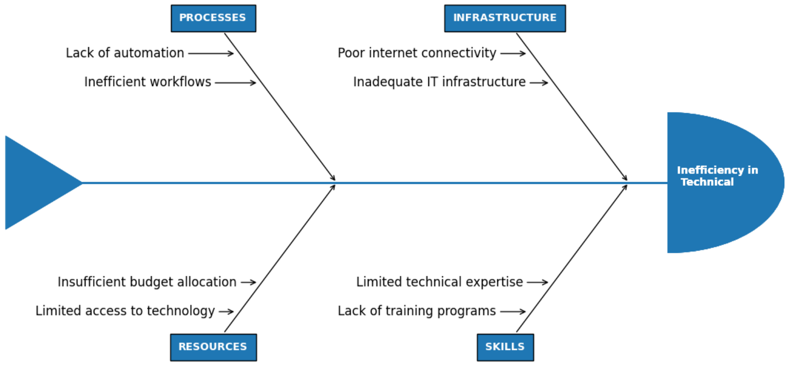
PROCESSES
Lack of automation
Inefficient workflows
INFRASTRUCTURE
Poor internet connectivity
Inadequate IT infrastructure
Inefficiency in Technical
Insufficient budget allocation
Limited access to technology
RESOURCES
Limited technical expertise
Lack of training programs
SKILLS

Figure 12. Inefficiency in the Technical Category.

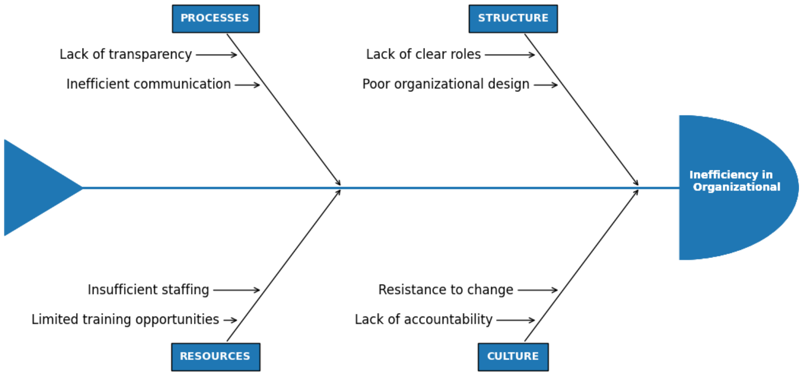

Figure 13. Inefficiency in the Organizational Category.

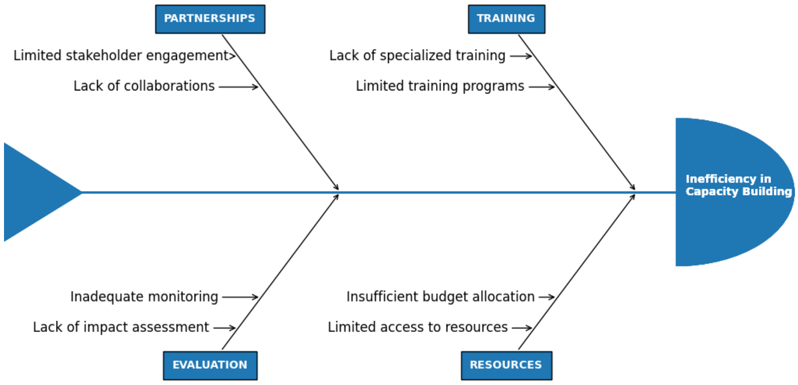
PARTNERSHIPS
Limited stakeholder engagement
Lack of collaborations
TRAINING
Lack of specialized training
Limited training programs
Inefficiency in Capacity Building
Inadequate monitoring
Lack of impact assessment
EVALUATION
Insufficient budget allocation
Limited access to resources
RESOURCES

Figure 14. Inefficiency in the Capacity Building Category.

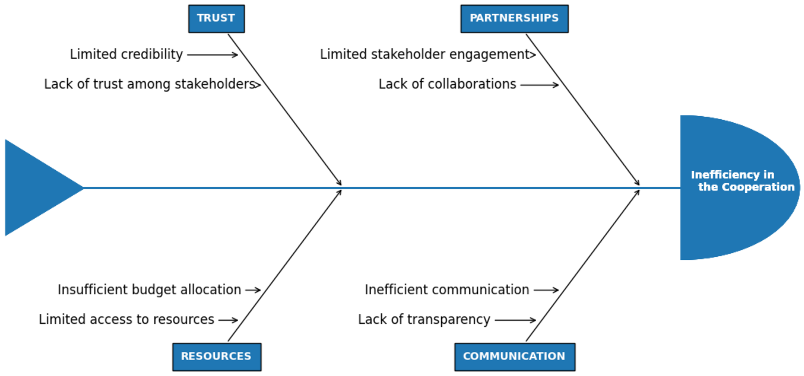
TRUST
Limited credibility
Lack of trust among stakeholders
PARTNERSHIPS
Limited stakeholder engagement
Lack of collaborations
Inefficiency in the Cooperation
Insufficient budget allocation
Limited access to resources
RESOURCES
Inefficient communication
Lack of transparency
COMMUNICATION

Figure 15. Inefficiency in the Cooperation Category.

Table 10. Comprehensive Cybersecurity Effectiveness Score (CCES).

Category	SWOT Index	EDEA	Radj	CCES Value	CCES Value (%)
Legal	3.6	0.50	0.35	1.8875	34.5%
Technical	3.6	0.25	0.225	1.828125	33.3%
Organizational	3.6	0.25	0.35	1.84375	33.6%
Capacity Building	3.6	0.50	0.325	1.88125	34.2%
Cooperation	3.6	0.50	0.35	1.8875	34.5%

6. Discussion

In this section we have discussed and analysed our results on the the perspective of Pakistan cyberSecurity eco sytem in more detail as follows.

We conducted SWOT analysis of Cybersecurity infrastructure in Pakistan which shows Opportunities, Threats, Vulnerabilities, and Strengths. The positive aspect are emerging trends such asa growing cybersecurity workforce and new international collaborations which aims at improving security frameworks. However, main challenges includes Outdated technical standards and legislative frameworks which limits Pakistan's ability to address modern cyber threats. Opportunities, especially in technical measures and international partnerships, were highlighted.These Opportunities are counterbalanced by substantial threats, such as a rise in cyberattacks, geopolitical tensions, and a lack of coordinated national response.The findings of our SWOT analysis provides foundationfor deeper quantitative assessments in future research. The DEA analysis provided us a quantitative comparison of Pakistan's cybersecurity efforts against developed countries. In our analysis each pillar of the GCI Pakistan performed well below the benchmark. Technical andOrganizational pillars shows significant inefficiencies in our analysis of DAE. Pakistan is well behind in effectiveness and resource utilization compared to developed countries which indicates that Pakistan's cybersecurity investments are failing to translate into effective outcomes. The inefficiencies which we find out during our DEA analysis prompted a deeperdive using Root Cause Analysis (RCA)to better understand Pakistan's cybersecurity shortcomings. The RCA shows issues including insufficient infrastructure investments, outdated legal frameworks, and poor coordination among key stakeholders such as government agencies, law enforcement, and private-sector players. Fish bone Diagram visualizedthese issues and highlighted the dependencies between various components of Pakistan's cybersecurity ecosystem.

Outdated policies, delayed court procedures, and a lack of digital tools to streamline legal processes are key weaknesses.Limited access to legal aid and ineffective case management systems constitutes inefficiencies, which result in in delayed. To build a effective legal framework Pakistan must undergo comprehensive legal reforms, including modernizing laws, improving judicial human resources, and expanding technical capabilities within the legal sector.

Main cause of Inefficiencies in Pakistan's technical infrastructure is due toa lack of automation and outdated workflows. Other factors includes poor internet connectivity, inadequate IT infrastructure, and limited access to advanced technologies. Low budget allocations further limit Pakistan's capacity to upgrade its technical infrastructure, leaving the country vulnerable to increasingly sophisticated cyber threats. In order to address these gaps requires strategic investments in technology and capacity-building initiatives.

Organizational inefficiencies in Pakistan's cybersecurity framework includes inadequate staffing levels, insufficienttraining programs, resistance to organizational change, and unclear roles and responsibilities within cybersecurity teams. Poor coordination between departments and a general lack of transparency is main issues. Without proper accountability and a clearly defined structure is one of the solution strengthen cybersecurity in Pakistan. Addressing these inefficiencies is crucial for creating an organizational environment conducive to effective cybersecurity management.

The capacity-building pillar in Pakistan's cybersecurity ecosystem is composed of critical several inefficiencies. Collaboration between stakeholders remains limited which hinders effective capacitybuilding initiatives. Moreover, a lack ofspecialized training programs, inadequatefunding, and poor monitoring mechanisms to assess the impact of existing programs further weaken Pakistan's abilityto build a sustainable cybersecurity workforce. Increasing stakeholder engagement, requisite funding, and improving impact assessment frameworks are critical steps towards filling these gaps.

Cooperation efforts of Pakistan'scybersecurity are effected by low stakeholder engagement, weak communication, and a general lack of trust among the key players involved. Low transparency and insufficient budget allocation further complex efforts to boost cooperation, while limited resource access restricts the capacity of different organizations to work together. In order toAddress these issues require a concrete effort to build trust, improve communication channels, and ensure the availability of sufficient resources for cooperative cybersecurity efforts.

We perform SWOT analysis of Pakistan's cybersecurity posture across thefive GCI pillars, with each pillar being scored on a scale of 1 to 10. Higherscores reflect stronger cybersecurity measures, while lower scores indicate areas requiring improvement. This qualitativescoring method provides a clear visualization of Pakistan's strengths, weaknesses, opportunities, and threats in its cybersecurity framework. The scoring allows for targeted improvements in specific pillars where Pakistan is lagging, especially in technical and organizational aspects,while leveraging strengths such as emerging legal frameworks and cooperative initiatives.

In our Root Cause Adjustment Factors (Radj) which provides a critical insight into the degree to which various root causes affect Pakistan's overall cybersecurity effectiveness. Lower Radj values, particularly in the technical category, indicate more critical issues that require top priority. These factors adjust the overall cybersecurity effectivenessscore, offering a more broader perspective on which areas demand the most immediate and focused interventions. The Radj framework ensures that Pakistan's cybersecurity reforms are driven by databacked insights and targeted recommendations.

The Comprehensive CybersecurityEffectiveness Score (CCES) for Pakistan offers an in-depth analysis of the country's cybersecurity posture across fivecritical categories. The overall CCESof 30.3% reflects moderate effectiveness with notable strengths in legal and cooperative aspects but glaring weaknesses in technical and organizational domains. This score highlights areas where Pakistan needs to focus its efforts to improve, with targeted reforms likely to yield significant improvements in the country's cybersecurity eco system.

7. Recommendations forImprovement

7.1. Short-term Actions:

7.1.1. Update Cybersecurity Regulations

I. Action: Revise and update existing cybersecurity laws, focusing on immediate gaps and aligning them with international standards.
II. Resources: Existing legal frameworks, and the government's legal teams.
III. Responsibility: Ministry of IT andTelecom, legal departments, and relevantlaw enforcement agencies.
IV. Timeline: 6-12 months.
V. Expected Impact: Immediate improvement in the Legal category of the SWOT index by enhancing the clarity and effectiveness of cybersecurityregulations.

7.1.2. Upgrade IT Infrastructure

I. Action: Prioritize quick upgrades incritical IT infrastructure in key sectors such as finance and healthcare.
II. Resources: Existing government and private sector IT budgets.
III. Responsibility: Ministry of IT, relevant industry stakeholders.
IV. Timeline: 12-18 months.

doi:10.20944/preprints202410.1442.v1

V. Expected Impact: Short-term boost in the Technical category, leadingto an increase in the DEA efficiency score.

7.1.3. Improve StakeholderCommunication

I. Action: Develop and implement a transparent communication strategy to ensure effective collaboration among stakeholders.
II. Resources: Communication platforms, and public relations teams.
III. Responsibility: Ministry of IT, National CERT.
IV. Timeline: 3-6 months.
V. Expected Impact: Enhanced Cooperation category, improving trust and collaboration, reflected in a higher SWOT index.

7.2. Long-term Recommendations:

7.2.1. Establish a National Cybersecurity TrainingAcademy

I. Action: Develop a comprehensive training academy to build a skilled cybersecurity workforce over time.
II. Resources: Government funding,and partnerships with international educational institutions.
III. Responsibility: Higher EducationCommission, international partners, Ministry of IT.
IV. Timeline: 3-5 years.
V. Expected Impact: Long-term improvement in the Capacity Building category, contributing significantly to overall CCES.

7.2.2. Enhance Digital CourtProcesses

I. Action: Implement digital tools for automating court processes and casemanagement to improve legal efficiency.
II. Resources: Government IT budgets, international partnerships.
III. Responsibility: Ministry of Lawand Justice, judiciary bodies.
IV. Timeline: 2-4 years.
V. Expected Impact: Sustainable enhancement of the Legal category, improving efficiency and reducing delays in the judicial process.

7.2.3. Forge International Partnerships for CapacityBuilding

I. Action: Develop long-term partnerships with international institutions to facilitate resource sharing, joint training, and knowledge transfer.
II. Resources: International grants, government funding.
III. Responsibility: Ministry of IT, Ministry of Foreign Affairs, internationalorganizations.
IV. Timeline: 3-5 years.
V. Expected Impact: Gradual enhancement of the Capacity Building and Cooperation categories, leading to sustained improvements in CCES.

7.3. High Priority

7.3.1. Improve IT Infrastructure

I. Action: Address inefficiencies in theTechnical category by rapidly improving IT infrastructure, particularly in critical sectors.
II. Resources: Significant governmentinvestment, and private sector collaboration.
III. Responsibility: Ministry of IT, industry partners.
IV. Timeline: 1-2 years.
V. Expected Impact: Significantimprovement in the DEA efficiency score and overall cybersecurity resilience, with a noticeable impact on CCES.

7.4. Medium Priority

7.4.1. Increase Participation inGlobal Cybersecurity Frameworks

I. Action: Enhance Cooperation by joining and actively participating in international cybersecurity organizations and frameworks.
II. Resources: Government funding,diplomatic channels.
III. Responsibility: Ministry of IT,Ministry of Foreign Affairs.
IV. Timeline: 2-3 years.

Expected Impact: Strengthened international cooperation and knowledgesharing, boosting the SWOT index and DEA efficiency scores.

7.5. Low Priority:

7.5.1. Restructure

Cybersecurity Agencies

I. Action: Improve Organizational efficiency by restructuring internal cybersecurity agencies to ensure better coordination and clear role definitions.
II. Resources: Internal audits, organizational change management teams.
III. Responsibility: Ministry of IT,cybersecurity agencies.
IV. Timeline: 3-5 years.
V. Expected Impact: Moderateimprovement in the Organizational category, which will indirectly support overall CCES through better inter-agency coordination and effectiveness.

8. Conclusion

This research demonstrates the effectiveness of a hybrid analytical approachin diagnosing and tackling cybersecurity issues in developing nations. With the integration of DEA benchmarking, RCA, and SWOT analysis, the report offers an extensive evaluation of Pakistan's cybersecurity infrastructure. The results show Pakistan has made progress in some areas. However, a few significantgaps remain particularly in technological expertise and international collaboration.The Comprehensive Cybersecurity Effectiveness Score (CCES) offers a strategic path to enhance cybersecurity resilience, with key recommendations focused on optimizing resource allocation, modernizing legal frameworks, and improving international cooperation.

9. Future Work

The use of Artificial Intelligence (AI) in future studies can further improvethe analysis and recommendations of this study. AI-driven predictive analytics models can forecast emerging cybersecurity risks and simulate the impact of different interventions on the Comprehensive Cybersecurity Effectiveness Score(CCES). AI algorithms can also automate continuous monitoring of cybersecurity metrics providing real-time insights and adaptable strategies for improving and maintaining cybersecurity postures. By Integrating AI into benchmarking and root cause analysis developing countries can manage cybersecurity risks moredynamically and effectively.

References

1. STANDARDIZATION SECTOR and OF ITU. Series x: Data networks, open system communicationsand security telecommunication security. *Interfaces*, 10(20-x):49,2008.
2. Xichen Zhang, Mohammad Mehdi Yadollahi, Sajjad Dadkhah, Haruna Isah, Duc-Phong Le, and Ali A Ghorbani. Data breach: analysis, countermeasures, and challenges. *International Journal of Information and Computer Security*, 19(34):402–442, 2022.
3. Faheem Ahmed Shaikh and Mikko Siponen. Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, 124:102974, 2023.
4. Joanna Światkowska. Tackling cybercrime to unleash developing countries' digital potential. *Pathways for Prosperity CommissionBackground Paper Series*, 33:2020– 01, 2020.
5. Andrew Hume, Jim Leape, Kirsten LL Oleson, Emily Polk, Kevin Chand, and Robert Dunbar. Towards an ocean-based large oceanstates country classification. *Marine Policy*, 134:104766, 2021.

6. Social Af. Handbook on the least developed country category: Inclusion, graduation and special support measures second edition. 2015.
7. Muhammad Riaz Shad. Cyber threat landscape and readiness challenge of pakistan. *Strategic Studies*, 39(1):1–19, 2019.
8. Abdulkarim A Oloyede, Nasir Faruk, Nasir Noma, Ebinimi Tebepah, and Augustine K Nwaulune. Measuring the impact of the digital economy in developing countries: A systematic review and meta-analysis. *Heliyon*,9(7), 2023.
9. Ivan I Ivanov. Digital transformation: Current challenges and future perspectives. In Business Modeling and Software Design: 11th International Symposium, BMSD 2021, Sofia, Bulgaria, July 5–7, 2021, Proceedings 11, pages 275–285. Springer, 2021.
10. Kateřina Petrová, Jan Špatenka, and Miloš Koch. The impact of covid19 on the digital transformation in organizations: a quantitative analysis. 2022.
11. Thanh Nguyen Hai, Quang Nguyen Van, and Mai Nguyen Thi Tuyet. Digital transformation: Opportunities and challenges for leaders in theemerging countries in response to covid-19 pandemic. *Emerging Science Journal*, 5(1):21–36, 2021.
12. Youngjin Yoo, Richard J Boland Jr, Kalle Lyytinen, and Ann Majchrzak.Organizing for innovation in the digitized world. *Organization science*, 23(5):1398–1408, 2012.
13. Sabine Berghaus and Andrea Back.Stages in digital business transformation: Results of an empirical maturity study. 2016.
14. Karl SR Warner and Maximilian Wäger. Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal.*Long range planning*, 52(3):326–349,2019.
15. Daniel Shu Wei Ting, LawrenceCarin, Victor Dzau, and Tien YWong. Digital technology and covid-19. *Nature medicine*, 26(4):459–461,2020.
16. J Frisby. Cybersecurity exposure index (cei) 2020. Retrievedfrom password managers. co:https://passwordmanagers. co/cybersecurity-exposure-index/# global, 2020.
17. Internasional TelecomunicationUnion. Global cybersecurity index 2020. *ITU Publication*, 2020.
18. Yijie Weng, Jianhao Wu, et al. Fortifying the global data fortress: a multidimensional examination of cyber security indexes and data protection measures across 193 nations. *International Journal of Frontiers in Engineering Technology*, 6(2):13–28, 2024.
19. Mykola Khudyntsev, Andrii Davydiuk, Oleksiy Lebid, Oleksandr Trofymchuk, and Artem Zhylin. Cybersecurity indices: Review and classification. *CPITS II (1)*, pages 117–126,2021.
20. Cybersecurity Index.Url: https://www. itu. int/en/itu-d/cybersecurity. *Pages/global-cybersecurity-index. aspx*, 2021/2024.
21. Kjell Brunnstrom, David Hands, Filippo Speranza, and Arthur Webster. Vqeg validation and itu standardization of objective perceptual video quality metrics [standards in a nutshell]. *IEEE Signal processing magazine*, 26(3):96–101, 2009.
22. N Falessi, R Gavrila, MR Klejnstrup, and K Moulinos. National cyber security strategies: practical guide on development and execution. *European Network and Information Security Agency (ENISA) Publication*, 2012.
23. CIOACĂ, Alexan-dru BRATU, and DanielȘTEFĂNESCU. The analysis of benchmarking application in cyber security. Scientific Research and Education in the Air Force–Afases 2017, 2017.
24. Amar Khairi and Martin Petlach.Need for digitalisation to provide security? a comparative study on the member states of the european union. *Univerzita Obrany. Ustav Strategickych Studii. Obrana a Strategie*, 2023(1):24–48, 2023.
25. Liudas Zdanavičius and Nortautas Statkus. Strengthening resilience of lithuania in an era of great power competition: the case for totaldefence. *Journal on Baltic Security.*, 6(2):1–21, 2020.
26. Robin Ruefle, Audrey Dorofee, David Mundie, Allen D Householder, Michael Murray, and Samuel JPerl. Computer security incidentresponse team development and evolution. *IEEE Security & Privacy*, 12(5):16–26, 2014.
27. Marthie Grobler and Harri Bryk. Common challenges faced duringthe establishment of a csirt. In *2010 Information Security for SouthAfrica*, pages 1–6. IEEE, 2010.
28. Nor Shazwina Mohamed Mizan,Muhamad Yusnorizam Ma'arif, Nurhizam Safie Mohd Satar, and Siti Mariam Shahar. Cndscybersecurity: issues and challenges in asean countries. *International Journal of Advanced Trends inComputer Science and Engineering*,8(1.4), 2019.
29. Gunnar Prause, Tarmo Tuisk, and Eunice Omolola Olaniyi. Between sustainability, social cohesion and security. regional development innorth-eastern estonia. *Entrepreneurship and Sustainability Issues*, 6(3):1235, 2019.
30. Christian Czosseck, Rain Ottis, and Anna-Maria Talihärm. Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes incyber security. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 1(1):24–34, 2011.
31. Chew Han Ei and Carol Soon. Towards a unified framework for digital literacy in singapore. *Institute of Policy Studies: Singapore*, 2021.

32. Yvonna S Lincoln and Egon G Guba.Criteria for assessing naturalistic inquiries as reports. 1988.
33. John W Creswell and J David Creswell. Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications, 2017.
34. Joan Solanes Mullor and Aida Torres Pérez. The constitution of spain: The challenges for the constitutional order under european and global governance. *National Constitutions in European and Global Governance: Democracy, Rights, the Rule of Law: National Reports*, pages543–590, 2019.
35. Jan Hovden. Public policy and administration in a vulnerable society: regulatory reforms initiated bya norwegian commission. *Journal of risk research*, 7(6):629–641, 2004.
36. Ehtisham Ul Haque, Waseem Abbasi, Sathishkumar Murugesan, Muhammad Shahid Anwar, Faheem Khan, and Youngmoon Lee. Cyber forensic investigation infrastructure of pakistan: an analysis of the cyber threat landscape and readiness. *IEEE Access*, 11:40049–40063, 2023.
37. Eric Luiijf, Kim Besseling, and Patrick De Graaf. Nineteen nationalcyber security strategies. *International Journal of Critical Infrastructures 6*, 9(1-2):3–31, 2013.
38. HAM Luiif, Kim Besseling, MaartjeSpoelstra, et al. Ten national cyber security strategies: a comparison. In *Proc. 6th International Conference on Critical Information Infrastructures Security (CRITIS 2011)*, 2011.
39. Martti Lehto. The ways, means and ends in cyber security strategies.In *Proceedings of the 12th European conference on information warfareand security*, pages 182–190, 2013.
40. Ünal Tatar, Orhan Çalik, Minhac Çelik, and Bilge Karabacak. A comparative analysis of the national cyber security strategies of leading nations. In *International Conferenceon Cyber Warfare and Security*, page 211. Academic Conferences International Limited, 2014.
41. Kyoung-Sik Min, Seung-Woan Chai, and Mijeong Han. An international comparative study on cyber security strategy. *International journal of security and its applications*, 9(2):13–20, 2015.
42. Riza Azmi, William Tibben, and Khin Than Win. Motives behind cyber security strategy development:a literature review of national cyber security strategy. 2016.
43. Narmeen Shafqat and Ashraf Masood. Comparative analysis of various national cyber security strategies. *International Journal ofComputer Science and Information Security*, 14(1):129–136, 2016.
44. Farzan Kolini and Lech Janczewski. Clustering and topic modelling: A new approach for analysis of national cyber security strategies. 2017.
45. Global Cybersecurity Index. Url:https://www.itu.int/myitu/-/media/publications/2021publications. *Global-CybersecurityIndex-2020.pdf [in English]*,2020.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.