P-ISSN: 2790-6795 | Annals of Human and Social Sciences | Jan-March 2025,Vol. 6, No. 1
O-ISSN:2790-6809 | http://doi.org/10.35484/ahss.2025(6-I)04 | [35-44]

Annals of Human and Social Sciences
www.ahss.org.pk

RESEARCH PAPER

The Role of Cyber Security in Promoting Digital Inclusion: A Case Study of Pakistan

Muhammad Mehmood

M. Phil Scholar, Department of Political Science and International Relations, University of Management and Technology, Lahore, Punjab, Pakistan

Corresponding Author mehmoodpolice786@gmail.com

ABSTRACT

This article explores the essential role of cybersecurity in fostering digital inclusion in Pakistan, a country striving to harness the digital revolution for socio-economic progress. Digital inclusion, ensuring equitable access to technology and services, is a key driver of development. However, Pakistan faces significant barriers such as cyber threats, infrastructure gaps, and the lack of comprehensive legislation, which erode trust in digital platforms and hinder adoption, particularly among underserved communities. Initiatives like Raast and the Digital Pakistan Vision showcase how robust cybersecurity measures can enhance user confidence, encouraging participation in online banking, e-governance, and e-learning. Qualitative methodology used in this study to explore, and describe cyber security and digital inclusion in Pakistan .Addressing cybersecurity issues like data breaches and online fraud is crucial to bridging the digital divide. The result of this study the interdependence of cybersecurity and digital inclusion, emphasizing Pakistan's immediate needs: improving cybersecurity infrastructure, promoting digital literacy, and formulating policies tailored to local challenges. Ultimately, cybersecurity is not just a technical requirement but a foundation for sustainable digital inclusion. By protecting trust and enabling secure access, it accelerates digital transformation, empowers citizens, and reduces socio-economic disparities. The article recommends on policymakers, businesses, and stakeholders to collaborate in creating a secure and inclusive digital future for Pakistan.

Keywords: Cyber Emergency Response Terms (CERTs), National Center of Cyber Security (NCCS), Prevention of Electronic Crimes Act (PECA), Sustainable Development Goals (SDGs), Technological Changes

Introduction

Due to technological changes, cyber security and digital inclusion have become part of the dialogue concerning socioeconomic advancement. Digital inclusion may be simply put as fair provision of equal access to digital tools along with skill to use the tools effectively. Cyber security entails the protection of users and their systems from possible threats(Jang-Jaccard & Nepal, 2014). These two ideas are closely connected and can include persons appropriately only when they can employ the technology safely. Expanding access may compromise an unsuspecting user to the vulnerabilities in the lack of adequate controls placed around it to undermine such trust in those technologies and its benefits. Digital has great growth prospects, but that does not in any way stand at the junction of transformation.

This paper reviews key programs, including the country's secure digital payment system, Raast, and Digital Pakistan Vision, which together emphasize the imperative of security for the adoption of digital solutions. This research therefore analyzes the current scenario and puts forward some actionable recommendations that can help provide a clear roadmap for utilizing cyber security as an enabler of inclusive digital growth in Pakistan (Jamil, 2021). Cyber security and digital inclusion have developed from being only a technical need to being a socio-economic imperative (Alhassan & Adam, 2021). An open, trusted digital environment will play an important role in helping the people of Pakistan make full use of the advantages offered by digital technologies in this increasingly complex digital world. This essay adds its own voice to this critical debate with insights and suggestions on making Pakistan's digital environment safe and inclusive.

Literature Review

Pakistan stands across this route due to the vast broad-band subscriber counts over 87 million with strong internet penetration while making excellent mileage in expanding infrastructures of this aspect. The Digital Pakistan Vision looks at pushing digital literacy and technology outreach to the most marginalized communities. However, in a scenario where threats to cybercrime like data breaches, financial frauds, and misinformation campaigns are multiplying day by day, it is hard to achieve those objectives. Cybercrime cases have witnessed a shocking rise in the past several years and are evidence of the grave vulnerabilities of Pakistan's digital ecosystem (Zahoor & Razi, 2020).

According to (Faisal et al., 2020) Cybersecurity is not merely a technical issue but fundamental to building trust and confidence in digital platforms. People are less likely to adopt or rely on online services if they perceive them as unsafe. This trust is critical for the success of digital inclusion. This relationship between inclusion and security is very important for Pakistan. Due to a lack of digital literacy and socioeconomic inequality, the country is highly vulnerable to exploitation in the digital world. Therefore, it would need a multifaceted strategy that combines efforts in education, regulation, and technology. Around the world, integrating cyber security with digital inclusion has emerged as one of the high priority drivers of sustainable development (Arner et al., 2019).

The Sustainable Development Goals developed by the United Nations underscore technology's role in bridging the socio-economic gaps and its ability to enhance inclusive and secure digital ecosystems (Alamoush et al., 2021). In aligning itself to these global trends, Pakistan has to invest in infrastructure but more importantly build very robust cyber security frameworks that will safeguard its future digital era. This paper analyzes how the nexus between cyber security and digital inclusion defines both a unique set of challenges and opportunities for Pakistan.

Material and Methods

The research would have been carried out the descriptive and analytical approaches to proceed and draw the conclusion. So, this research also included the descriptive and analytical method of research for data collection. For this purpose, qualitative method has been used. All the data given in this study would been collected from books, journals, official reports of the organizations, experts available on internet for instance, secondary methods for the research were consulted and analyzed the recommendations. To gain a more comprehensive understanding to the role of Cyber Security in promoting digital inclusion.

Cybersecurity Challenge: Digital Inclusion in Pakistan

Growing Cyber Threats

As the digital ecosystem of Pakistan grows, vulnerability to cyber threats also grows with it. The list includes:

Data breaches: These are the sophisticated hacking of sensitive information in governments, financial sectors, and health departments. Not only is sensitive information compromised but the public also loses trust in the digital space.

Financial fraud: These hackers make use of gaps in the electronic payment systems that cheat the user, mainly digital illiterates. Dissemination of Wrong Information Campaign

They release information and propaganda comprising of wrong details in the digital systems above the bar, creating political as well as social unrest Hacking (Achim et al., 2021).

Malware: There exist a great number of threats involving significant national security issues associated with critical infrastructure that include energy grids and communication networks (Wangen, 2015).

Cybercrime Trends This is concerning, the rise in cybercrime over the last few years. Crucially, ransomware, phishing scams, and identity theft are among the current occurrences, which have grown frighteningly prevalent. Accusations of cybercrime from Pakistan soared by 83.

Current Cyber Security Measures

These are some of the measures by which Pakistan has responded to these challenges: Legislation: The legal framework to check cybercrime is the Preventing Electronic Crimes Act (PECA) 2016. Despite criminalizing a host of cyber offenses, it is still very weak in its enforcement because of a lack of resources and technical expertise. item Institution Actions: The National Center for Cyber Security (NCCS) has taken major roles and will play along regarding efforts into furthering the cause of advanced cyber defence research and innovation. It is also an institution in developing local solution responses to a possible effective approach toward countering cyber threats. item Awareness Campaigns: Public efforts to educate people in online safety and fraud prevention have been implemented. The effectiveness of such campaigns lies, however in having them on wider, and more continuous coverages given that cyber threats keep changing in their nature and style.

Infrastructural and policy gaps

Pakistan has really developed in terms of digital connectivity, but the cyber security infrastructure is highly disintegrated and underdeveloped. The primary legislative framework with which the country deals with cybercrime is the Prevention of Electronic Crimes Act (PECA) 2016. However, PECA has very weak mechanisms for its implementation, and the ambit is very narrow (Furqan, 2016). For example, although PECA criminalizes most of the manners of cyber acts, it considerably lags behind in providing any procedure to handle fast-emerging threats such as fraud by bitcoin and malware attacks of great sophistication. Lack of comprehensive national cyber security strategy. While developed nations have established comprehensive frameworks, Pakistan has only adopted a reactive approach toward cyber security and not proactive planning. In the absence of coordination among regulatory bodies, there are redundancies and inefficiencies in dealing with cyber threats. (Chohan and Hu, 2020)

Digital Literacy Deficit

Low digital literacy rates compound the problem. (Quayyum & Freberg, 2023)most vulnerable populations in rural areas do not know much about basic cyber security practices and are easily manipulated by fraudsters and cyber attackers. Education in this gap area is still ad hoc and in need of a more robust investment and strategic approach. By addressing such diverse challenges on an integrated model consisting of technology innovations, changes to the law regime, and a campaign towards enhancing education among relevant stakeholders, the country may finally be in the position to realize more secure, non-discriminatory and sustainable digital services, which are inevitable drivers of repressed trust across diverse digital domains in Pakistan.

Socio-Economic Disparities

Socioeconomic inequality in Pakistan makes the issues in digital inclusion more challenging. It remains a privilege rather than an important tool to reach the broader section of masses across the majority in rural and geographically secluded settings, where people struggle to attain inexpensive and secure connectivity. Thus, the problem does not just cause interference with access to those basic service streams like schooling or healthcare delivered digitally but further contributes to more cybersecurity threats for whom little resources can recover (Jamil, 2021).

Another significant challenge is the lack of secure payment systems and digital financial services in many regions. Initiatives like Raast can, in reality, be an important step toward rectifying the problem, but it all very much depends upon the broader socioeconomic barriers inhibiting the adoption of digital technology (Abbas et al., 2022). Pakistan needs a multi-dimensional approach toward the development of a more secure digital environment. Technological innovation must be fostered, legislative reforms introduced, and broad educational initiatives pursued. This will be critical for establishing trust in digital platforms the same trust necessary for ensuring the fair distribution of benefits that arise from the digital revolution across all strata of society.

Interrelation of Cyber Security and Digital Inclusion

Building Trust Through Security

A secure digital environment builds up trust, hence crucial for promotion of participation into digital platforms. For example, a real-time payment system called Raast in Pakistan relies on tough security protocols, thus ensuring efficient and safe monetary transactions. So far, such robust security provisions have been quite a significant incentive for both its individual and institutional users (Bokhari, 2022a).

Reducing the Digital Divide

Cybersecurity thus protects vulnerable population groups from exploitation while ensuring fair play in the electronic economy. All access-expansion programs, therefore, such as Digital Pakistan Vision, have focused on addressing related security concerns as well to forestall further pushing vulnerable groups off the electronic lifeline.

Investment Promotion

A strong cyber security framework can reduce risks associated with business operations in a digital economy. Simultaneously, it acts as an attraction tool for local and foreign investments. Strong financial and e-governance platforms can fuel innovations that support a robust and dynamic digital economy with sustained economic growth (Bokhari, 2022b).

Case Studies

Raast: Digital Safe Payments Raast service has recently been launched by the State Bank of Pakistan that makes it a new step towards countrywide financial inclusion. It is both safe and timely payment service by which economic differences can be at least minimized more towards the deprivated strata of the society. By end-to-end encryption security, it keeps a transaction safe, in confidence, while building trust regarding digital financial services (Bokhari, 2022).

Raast architecture has been able to minimize its transaction costs that have made the product affordable, and therefore, room was made for the uptake of digital payment systems among these target groups; hence, considering all these, it shows how the existence of this entity is crucial because research has actually revealed that a vast majority within

Pakistan's informal economy have reaped benefits from their accessibility of such services. (Ullah et al., 2024).

However, the success of the platform depends on its cyber security measures against threats and retaining the trust of users, which shows that cyber security is a very crucial part of its framework of operations. Comparative analysis with similar systems, such as India's Unified Payments Interface (UPI), reveals some lessons in scaling digital payment platforms. However, Raast is unique in its safe infrastructure, but for sustaining its development and ensuring fair access, constant innovation and strong cyber defenses are required. (Bukhari, 2023).

Digital Pakistan Vision: Digital Pakistan Vision is an all-round and comprehensive vision towards making Pakistan empowered digitally well-rounded society, first launched in the year 2019. Three different segments: development of digital infrastructure, improving digital literacy, and e-governance implemented in terms of facilitating smooth public services and innovation. Though the initiative is very ambitious, its execution has not been smooth because of infrastructural gaps and a lack of coherent policy execution. (Ali et al.).

One of the key success factors of the Digital Pakistan Vision is that it encourages public-private partnerships to enhance the adoption of digital. This collaboration has ensured that the technology aimed at increasing connectivity in remote areas is implemented. Moreover, it stresses secure digital ecosystems because the realization is that cyber security is essential for its realization. Despite all these successes, the program has been criticized for its slow pace in redressing the digital divide.

There is a convincing rationale for targeted intervention in the sense that rural and marginalized communities cannot be left behind. International lessons, such as the Estonian model of e-governance, underscore the point that cyber security must be in every layer of digital transformation so that trust and adoption can be established. (Mujahid, 2002).

Benchmarking Against Global Efforts: Pakistan's digital initiatives, such as Raast and the Digital Pakistan Vision, are using some of the best international approaches for creating these products. Estonia's advanced e-governance system is a fine example of how data infrastructure can maintain public trust. Similarly, the example of India's Unified Payments Interface (UPI) shows that with innovative and scalable products, and a user-centric approach, one can push forward the agenda for financial inclusion.

These examples will be valuable learning points for Pakistan on its road to a safe and inclusive digital ecosystem. Digital literacy and cyber security gaps need to be filled out if Pakistan wants to stay competitive and achieve its goals on digital transformation. Implementing the best international practices from standards developed around the world could make the programs of Pakistan more effective and ensure long term efficiency.

Global Context and Relevance to Pakistan

United Nations' Sustainable Development Goals (SDGs)

The UN Sustainable Development Goals (SDGs) have emphasized the role of technology in reducing inequalities and promoting sustainable development. Specifically, SDG 9 (Industry, Innovation, and Infrastructure) and SDG 10 (Reduced Inequalities) are the objectives of having secure and inclusive digital ecosystems. For Pakistan, these are actionable strategies in achieving such objectives:

- Secure Digital Infrastructure Investment Developing resilient and accessible technologies that are able to stand up to cyberattacks.

- Bridging the digital divide: equitable access to digital technology for all socioeconomic groups, especially in disadvantaged and rural regions.

All these measures are geared towards building an inclusive digital economy where every citizen can meaningfully participate and thrive in the digital space.

Global Best Practices

Estonia and **Singapore** have established a stellar precedent of seamless integration of cyber security with initiatives toward digital inclusion. Begin itemize Estonia: Estonia boasts high advanced digital infrastructure. Estonia's e-residency program are digital services made easier with good cyber security procedures in place. Apart from the good influence on public confidence, it has placed Estonia at the frontline position of international governance of the Internet. Singapore: Singapore has been the gold standard in digital transformation, having comprehensive cyber security frameworks and nationwide digital literacy campaigns. Such initiatives have made it possible for mass digital adoption with the security of user data and privacy (Kotka et al., 2015).

These would mean adaptations in policies toward fitting into unique issues the country faces because of socio-economic and infrastructural obstructions for Pakistan. Success here will depend upon the prioritizing private partnerships, where robust policy implementation becomes an instrument for their implementation.

Conclusion

This article says that cyber security is essential to advance digital inclusion in Pakistan. Cybersecurity becomes a critical enabler and a basis for providing equitable access to technology in the pursuit of the digital revolution. They are crucial in bridging the socioeconomic gap and meeting sustainable development goals because they ensure safe digital ecosystems that enable users to engage in the digital economy, trust it, and safeguard user data.

Two initiatives that reflect how technology can enhance connectivity, governance, and financial inclusion are the Digital Pakistan Vision and Raast. Conversely, these successes also reflect on the problems: cyber threats, infrastructural gaps, and digital illiteracy. Article recommendations-from developing a comprehensive cyber security strategy to fostering public-private partnerships-offer avenues that can be taken for effective confrontation of the challenge at hand.

Policy makers, businesses, and the communities must bring in coordination. Policymakers must strengthen lawmaking frameworks, construct them in alignment with global standards, and protect the businesses by innovating and investing in secure technologies. At the same time, capacities of the communities should be built through awareness campaigns so that it is easy for members of the community to ride through the digital world safely. For Pakistan's digital transformation, a holistic approach is essential—one that prioritizes cybersecurity as a central component of advancing digital inclusion. All stakeholders would collaborate, in the spirit of global best practice, to form a secure and inclusive digital space. Through the development of this framework, Pakistan can empower citizens, unlock new socioeconomic opportunities, and contribute toward the broader goals of global sustainable development.

Recommendations

To strengthen the cyber security framework of Pakistan in accordance with international standards, the following specific recommendations are proposed. Muhammad

Waqar Anwar's review of Pakistan's present cyber security situation and the best practices used in Estonia and Singapore served as the basis for his suggestions.

Develop a Comprehensive National Cyber Security Strategy

A coordinated and future-focused cyber security approach against the new form of digital threats should be created. It should comprise: Identify the Key Threats: Plot the threats to critical infrastructure, financial systems, and public services. Clearly define the goals: protect user data, build digital trust, and make secure transformation in the digital space. Promote cooperation among the government, private sector, academia, and civil society towards work towards harmonization in approaching cyber security (Khan & Anwar, 2020).

Enhance Legislative Frameworks

The Prevention of Electronic Crimes Act 2016 shall be amended along international standards including General Data Protection Regulation of the European Union, as amended herein, includes;

- Strengthen data protection laws. Implement stiffer penalties for breaches and unauthorized use of data.

- Improve Mechanisms of Enforcement Provide regulatory bodies with resources and authority for effective enforcement of cyber laws.

- Emerging Threats: Expand the current scope of the law to cover cryptocurrency fraud, AI-related vulnerabilities, and cross-border cybercrime (Khan, 2020).

Invest in Cyber Security Infrastructure

Pakistan should invest in frontier technologies and infrastructures to become more resilient against cyber threats. Some of these steps are as follows:

- AI-Based Threat Detection Implementation: AI to detect and counter cyber threats in real time; thus, prevent the enemy with proactive defense.

- Critical Infrastructure Upgrades: Implement new state-of-the-art encryption technologies that ensure information-security standards of both public and private sectors' sensitive information.

- Provide National Cyber Emergency Response Teams (CERTs): This can speed up response to cyber incidents at regional and national levels (Bokhari, 2022)

Foster Public-Private Partnerships

The public and private sectors are crucial partners when it comes to exchanging resources and experience.

- Promote private sector involvement; provide incentives like financial rewards in the form of investment in cyber security products.

- You can even raise funds that offer support to entrepreneurs and innovation by supporting local research and development in cyber security technology.

- Leverage Global Expertise: Pakistan should assimilate international best practices and emerging technologies by partnering with foreign agencies. Association with international experts could prove helpful by gaining valuable inputs, innovative answers, and availability of latest tools toward speedy development of a secure robust digital ecosystem. (Mujahid, 2002; Ullah et al., 2024)

Public Awareness

A Pillar of Integrated Cyber Security Architecture The awareness component is also quite important for raising public awareness for a complete framework of cyber security. Major measures include:

- Nationwide Campaign: Public education for the public masses to enlighten them regarding prevalent cyber threats against them and making them use internet responsibly.

- Cyber Security in School: All types of schools and their curriculum-in elementary school, middle school, and high school-need to include topics under cyber security as a teaching approach from early schooling.

- SME Education: Education regarding the knowledge and resources which these small and medium sized business enterprises would need for securing their digital operations in reducing cyber risks as best as possible.

This will establish a vibrant participation base of individuals and business communities having an interest in developing a safer digital world (Ali et al., 2023)

International Partnerships

International frameworks and organizations will also contribute towards much stronger cyber security capabilities for Pakistan. Main activities are the following:

- Join international cyber alliances; through the GFCE, one gets to access trainings and many other resources by joining such organizations.

- It is of highest essence to put these international standards on your nation policies. The accomplishment can be performed by incorporation of the nationals of the respective standards like this incorporation can include its information security by ISO 27001 standard because only for gaining such systematic consistence of strong or strong, secure system.

- Facilitating Knowledge Sharing: Host workshops and conferences to exchange expertise and insights with global leaders in cyber security.

These measures will strengthen Pakistan’s position in the global cybersecurity landscape and enhance its ability to address digital threats effectively.

The implementation of these recommendations will create a secure digital ecosystem in Pakistan that supports the country’s ambitions in terms of digital inclusion and the United Nations’ Sustainable Development Goals. It will encourage trust, improve resilience to cyber threats, and empower citizens to participate in the digital economy.

References

Abbas, H. S. M., Qaisar, Z. H., Ali, G., Alturise, F., & Alkhalifah, T. (2022). Impact of cybersecurity measures on improving institutional governance and digitalization for sustainable healthcare. *Plos one, 17*(11), e0274550. https://doi.org/10.1371/journal.pone.0274550.

Achim, M. V., Borlea, S. N., Văidean, V. L., Florescu, D. R., Mara, E. R., & Cuceu, I. C. (2021). Economic and financial crimes and the development of society. *Improving Quality of Life: Exploring Standard of Living, Wellbeing, and Community Development*, *25*.

Afzal, M., Meraj, M., Kaur, M., & Ansari, S. (2024). How cybersecurity awareness helps in achieving digital financial inclusion in rural India under escalating cyber fraud scenarios. *Journal of Cyber Security Technology*, 1–39. https://doi.org/10.1080/23742917.2024.2347674.

Alamoush, A. S., Ballini, F., & Ölçer, A. I. (2021). Revisiting port sustainability as a foundation for the implementation of the United Nations Sustainable Development Goals (UN SDGs). *Journal of Shipping and Trade*, *6*, 01-40. https://doi.org/10.1186/s41072-021-00101-6

Alhassan, M. D., & Adam, I. O. (2021). The effects of digital inclusion and ICT access on the quality of life: A global perspective. *Technology in Society*, *64*, 101-511.

Ali, B., Salam, A., & Ali, W. (2023). Digital Pakistan Policy: A Document Of Words Or Plans For Implementation, A Critical Analysis, *Pakistan Journal of Social Research*, *5*(1), 627-635.

Arner, D.W., Buckley, R.P. Zetzsche,D., & Veidt, R. (2020). Sustainability, FinTech and Financial Inclusion, European Business Organization Law Review, 21(1), 07-35.

Bokhari, H. (2022). Digital Financial Inclusion of the Informal Sector: The case of Raast Platform in Pakistan. *Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance*, 161–166.

Bukhari, Syeda Sophia. (2023). Digital Payment Adoption in India and Pakistan: A Comparative Analysis. *Focus.*

Chohan, S. R., and Hu, G. (2020). Strengthening digital inclusion through e-government: cohesive ICT training programs to intensify digital competency. *Information Technology for Development, 28*(1), 16–38. https://doi.org/10.1080/02681102.2020.1841713.

Faisal, M., Ali, I., Khan, M. S., Kim, S. M., & Kim, J. (2020). Establishment of Trust in Internet of Things by Integrating Trusted Platform Module: To Counter Cybersecurity Challenges. *Complexity*, *2020*(1), 02-09. https://doi.org/10.1155/2020/6612919

Furqan, M. (2016). PECA 2015: A Critical Analysis of Pakistan's Proposed Cybercrime Bill *UCLA Journal of Islamic and Near Eastern Law., 15*(1), 71-84.

Jamil, S. (2021). From digital divide to digital inclusion: Challenges for wide-ranging digitalization in Pakistan. *Telecommunications Policy*, *45*(8), 102-206.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. https://doi.org/10.1016/J.JCSS.2014.02.005

Khan, U. P., & Anwar, M.W. (2020). Cybersecurity In Pakistan: Regulations, Gaps And A Way Forward. *Cyberpolitik Journal, 5(*10), 205-218.

Kotka, T., Vargas, C., & Korjus, K. (2015). Estonian e-Residency: Redefining the nation-state in the digital era. *University of Oxford Cyber Studies Programme Working Paper*, *3*, 01-15.

Mujahid, Y. H. (2002). Digital Opportunity Initiative for Pakistan. *The Electronic Journal of Information Systems in Developing Countries, 8*(1), 1–14.

Quayyum, F., & Freberg, G. N. (2023). Designing Cybersecurity Awareness Solutions for the Young People in Rural Developing Countries: The Need for Diversity and Inclusion. *ArXiv Preprint ArXiv:2312.12073*.

Ullah, U., Khan, J., Junaid Ali Shah, and Baloch, R. (2024). Customers Experience and Perception Towards the Adaptation of Financial Services; A Special Reference to RAAST. *UCP Journal of Business Perspectives, 1*(2), 1–22.

Wangen, G. (2015). The role of malware in reported cyber espionage: a review of the impact and mechanism. *Information*, *6*(2), 183–211.

Zahoor, R., & Razi, N. (2020). Cyber-Crimes and Cyber Laws of Pakistan: An Overview. *Progressive Research Journal of Arts and Humanities (PRJAH)*, *2*(2), 133-143.