ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR

CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW

Vol.03 No.01 (2025)

SHIELDING PAKISTAN: THE IMPERATIVE STUDY OF R & D IN INFORMATION SECURITY FOR NATIONAL GROWTH AND STABILITY

Abdul Razaq
Department of Information Technology, Superior University, Lahore, Pakistan, engrarazaq@outlook.com
Sajjad Ali
Department of Computer Science, Superior University, Lahore, Pakistan, sajjadali750@hotmail.com
Dr. Syed Asad Ali Naqvi
Associate Professor, Department of Information Technology, Superior University, Lahore, Pakistan, syedasad.alinaqvi@superior.edu.pk
Nadeem Rasool
Department of Software Engineering, Superior University, Lahore, Pakistan, msse-f21-007@superior.edu.pk
Sidra Yousaf
Department of Software Engineering , Superior University, Lahore, Pakistan, msse-f21-015@superior.edu.pk

Abstract

The increasing levels of computerization around the globe require an emphasis on information protection to counter between threats to economic, political, and social systems. With the growing importance of IT in every aspect of national security, economic growth, and technological prosperity for Pakistan, R & D has to be the key factor for improvement in digital power of any country. However, problems like lack of proper infrastructure, shortage of skilled workforce, and lack of integrated policies still remain the same, and the problem is even exacerbated by the use of technology in different industries. The systemic approach with collaboration of government, non-government organizations, private support, and technology and community awareness is mandatory. This research examines the impact of R &D in improving information security in Pakistan through Policy, Technology, Resources and Stakeholders by applying Partial Least Squares Structural Equation Modeling (PLS-SEM). Lack of Investment in R&D, Multiple Policies and Lack of PPP have been identified with Pakistan to be weak in combating cyber threats. According to the study's findings, it is necessary to create specific research centers, support cybersecurity projects, start technical education, and update policies with international counterparts. Community engagement interventions are recommended to enhance the ability of the populace to protect their cyberspace resources. Thus, the mentioned gaps can be filled to strengthen the information security measures in Pakistan and set a course for development in the Fourth Industrial Revolution economy.

Keywords: *Information Security, Research and Development, Cybersecurity Policy*

INTRODUCTION

Technology affects business, economy, communication, and politics. Internet, AI, and blockchain have transformed industries, driving innovation, connectivity, and growth. Companies face new information security concerns with innovation! Information protection is crucial to a nation's security and development because electronic technology can instantly affect its economic, political, and social environment. Post-industrial nations like Pakistan must safeguard their cyberspaces from local and external threats. Information security is crucial as Pakistan updates and defends its fast-growing digital environment.

This digital process links security, economic growth, and data protection. State power and national well-being depend on information security, not only IT. As technology improves, information infrastructure is crucial to governments' strategic independence and economic vitality. Cyber dangers have escalated as Pakistan's government, commercial sector, economic processes, and key facilities have expanded into cyberspace. Data breaches, ransomware, cyber espionage, and state-sponsored hacking are national concerns. Financial risks damage government credibility, limit economic growth, and put sensitive industries at risk of national instability. Pakistan faces issues like other emerging nations. Although the government and private sector have significantly consulted to digitalize services, information security research and development is neglected. Wealthy nations support government and private cybersecurity research, but Pakistan cannot keep up with new cyber threats.

Lack of R&D and regulatory fragmentation hampered Pakistan's cybersecurity. Inconsistent government, commercial, and academic rules make information security planning difficult. Pakistan's economy and security are at risk without a plan.

The repercussions of such vulnerabilities are felt. As Pakistan relies on digital platforms for administration, business, and infrastructure, an information security disaster may be devastating. Police, taxation, and health need trustworthy information systems. Private financial institutions, e-commerce, and telephone are digital and subject to hackers. Networked, hackable energy, transportation, and defense systems are targeted. These vices could generate unprecedented financial losses, service delays, and a drop in residents' economic faith, hurting the nation.

The Imperative of R&D in Information Security" discusses national information security and R&D. Information security R&D detects, defends, and eliminates cyber threats with cutting-edge technologies. Thus, this R&D will strengthen Pakistan's cyber-security and promote cybersecurity innovation that may benefit other sectors. Pakistani researchers innovate encryption, threat detection, and digital security.

This research heavily uses PLS-SEM to examine variable connections. PLS-SEM will assess information security factors in Pakistan. Other causes include law, technology, companies, and public health campaign reinforcement. This study analyzes how these variables "intermediate" to identify Pakistan's information security and development demands. Government cybersecurity may boost private sector culture and R&D. Cyber security AI and ML could assist Pakistani systems detect and repel threats in real time.

Public knowledge may provide security and other benefits. As cyber threats evolve, individuals and businesses must be aware of and mitigate digital profile attacks. Promotional marketing and cybersecurity education can reduce social engineering, phishing, and other cybercrimes against individuals and businesses.

This research will assist Pakistani governments, corporations, and stakeholders secure data. The study will suggest cybersecurity improvements for the nation's digital ecosystem. Public-private collaborations, cybersecurity infrastructure, and R&D spending will increase. If these concerns are managed, Pakistan can use cyberspace, protect critical data, and boost economic growth and security.

A national cyber security policy that promotes R&D and innovation may be this study's most important recommendation. Cybersecurity research institutes, private sector R&D subsidies, academic, administrative, and IT business synergies may be part of this plan. National cybersecurity could improve with a public-private cooperation. To improve cyber-security, these sectors can share information, resources, and experience. People can regulate their digital life with awareness and training.

IT security is a major issue. Information security is vital to Pakistan's stability and success as it upgrades its infrastructure and adopts new technologies, like other transitioning economies. This research analyzes how R&D

might improve Pakistani information security. This paper examines Pakistan's main cybersecurity risks and presents solutions to improve its security for sustainable prosperity. Pakistan can secure its digital infrastructure and prosper in the digital economy in the coming decade with better legislation, public-private collaborations, and R&D.

Objectives

Therefore, the main aim of this research is to examine how R&D is central to improving Pakistan’s information security infrastructure. As they integrate information technologies into governance, commerce and key infrastructures, the country experiences increased risk from cyber criminals, ransomware, identity theft, and cyber terrorism. This research aims at establishing the various existing gaps in the Pakistani context as far as cybersecurity is concerned especially in the various governance structures and private entities and particularly in the sensitive sectors including energy, transport and communication. In light of these weaknesses, the research seeks to offer recommendations toward which specific measures can be taken to enhance the nation’s cyber defense.

Among the research objectives is the capacity to determine the extent to which the government policies and regulations affect the state’s ability to prevent cyber threats. It will assess the role of the current policies in combating new forms of cyber threats in addition to its assessment about abilities of different government ministries, agencies, and departments in the implementation of the developed policies. It also seeks to recommend measures that, when implemented, may strengthen policy formulation and implementation to enhance the cybersecurity regulations of Pakistan.

Being aware of the fact that Pakistan lacks a coordinated approach to cyber security, this research underlines the need for integration of efforts among the government, private entities, and universities. It will explore how these stakeholders can collectively improve resource utilization, expertise and innovation. Another direction of the analysis is the question of how the commercial sector, which pursues purely commercial goals, can be engaged in constructing national cybersecurity priorities that support a common and strong defense against cyber threats.

Another major goal concerns an assessment of the contribution of R&D in delivering state-of-art solutions in cybersecurity necessary for Pakistan’s needs. Through a discussion of international experience and trends, the study aims to show how the key findings can help to outline the ways that organizations can strengthen their digital security, protect the infrastructure of critical importance, and prevent adverse effects of cyber threats, as a result of higher investment in R&D. Also, to promote the idea on the necessity of the development of new technologies which can significantly increase the efficiency and reduce the costs of cybersecurity.

Artificial Intelligence, machine learning, Blockchain are some of the technological solutions that have gargantuan development opportunities in cybersecurity. In light of this, this research seeks to determine the relevance of applying these technologies in Pakistan’s setting and identify areas of innovation in cybersecurity. The study also deems it relevant to close the gap between the research and the market so as to ensure that research problems address real challenges and contribute to the development of a nation’s digital security infrastructure.

Another important aim is firstly the increase of awareness and secondly the increase of information literacy in the field of cybersecurity. The study will examine how use of education, training and awareness affects cybersecurity practice and adoption among individuals, organizations and institutions. Through creating cybersecurity cultural awareness, the study will act as a platform for timely prevention of cyber threats.

Finally, this study aims to give recommendations on how the cybersecurity situation in Pakistan can be improved. These are, policy formulation, promotion of public private partnership, enhancing research and development in cybersecurity and aligning the vision of Pakistan with international cybersecurity policies. As a result, the study has the following objectives: In achieving these objectives, the study will help protect Pakistan’s electronic systems, foster growth, and defend the nation in the era of globalization.

CONCEPTUAL FRAMEWORK

Thus, the modernization of political, business, and key civilian structures in Pakistan has led to the highly technological society. But with the advancement in the digital world, the country is now at a high risk of various types of cyber security threats. The theoretical foundation for this research is based on the concept of analyzing the current threats in Pakistan related to information security and the synergism needed for addressing such risks. The framework shows that the government, private sector and academics must work together to build a strong and sustained cybersecurity environment.

Problem Statement

With digital networks embedded now into service delivery, most economic activities especially in developed countries and national security, Pakistan like any connected country in the world is exposed to many cyber threats. These intricate web-like structures have exploited the country's governance systems, e-commerce systems and energy, transport and telecommunication infrastructures. Such attacks as ransomware, data breach and cyber terrorism sponsored by some states affect these domains. They endanger and compromise priority life processes, erode confidence in State institutions and hamper development.

The first problem is a lack of adequate protection for Pakistan's administrative and commercial networks, which can be targeted by cyber criminals. Governing bodies that deal with such citizen data involve are most at risk and threatens the law enforcement and public safety. In addition, the financial sector and electronic commerce are more vulnerable, the impacts may range from major money loss and substantial brand image detrimentalities.

Furthermore, critical structures have also become an attractive subject to cybercriminals. For instance, an attack on power grids could result in power outages in large areas affecting industries and people's lives in various ways. Likewise, the attack on the transportation networks may disrupt supply chain, affect the business and pose threat to the life of people. Yet, these threats are augmenting in Pakistan and the country's response to information security issue is still uncoordinated and insufficient to establish a coherent and effective cybersecurity policy.

Key challenges include:

Several challenges compound Pakistan's vulnerabilities in the cybersecurity domain:

- **Lack of Coordination among Stakeholders**: Lack of cooperation between the government, private sector and academia greatly reduces the ability of Pakistan to protect itself against cyber threats. Executors of cybersecurity measures at the governmental level also often have insufficient qualifications and tools to prevent new types of threats. In the same regard, most private sector organizations may focus on the business aspect of their organizations as they implement security measures, and therefore some of the digital assets remain vulnerable to breaches. Sadly, academia, despite its potential of providing creative solutions for future problems, is isolated from the real-world problems of industry and government, which in return hinders the growth of cybersecurity technology.
- **Inadequate Policy and Regulatory Frameworks:** Current legal measures and regulations in context with cybersecurity in Pakistan do not sufficiently cover the modern threat environment. Bureaucratic entities which make key policy decisions and oversee policy implementation in the cyberspace do not possess adequate instruments and information to identify and effectively combat sophisticated threats. This deficiency makes the country practice a reactive approach to cybersecurity than a preventive one so that the country is prone to fall prey to sophisticated attacks.
- **Fragmented Digital Infrastructure:** Again, the concept of Pakistan's digital infrastructure is comprehended by the absence of an integration and coordination of its substructures. While many critical infrastructures depend on digital technologies for their operation, these infrastructures are highly vulnerable to cyber-attacks. These systems are partially integrated hence it becomes hard to put in place strong security measures, hence Vulnerable to hackers.
- **Resource Constraints and Limited Investment:** The problem is made more acute by the relatively small amounts of money and effort being devoted to cybersecurity research, development, and deployment. It is stated that in the absence of funding and investment the development of sophisticated protective measures and technologies cannot be achieved. This also means a lack of investment in the training and development necessary to prepare professionals to deal with ever emerging forms of cyber threats.
- **Absence of a Unified Strategy:** It is also worth mentioning that there is no comprehensive approach to counter cyber threats still now. This is because different stakeholders pursue fragmented activities which are not efficient in the use of resources and do not address vital cybersecurity challenges. The lack of

coherence in the framework for Pakistan's cybersecurity future poses challenges concerning the successful accomplishment of a comprehensive and strong defense system against cyber threats.

It is therefore imperative that the above challenges receive an overall and coordinated efforts by all the players. Thus, there is a need for a joint effort of the government, private organizations, and universities in creating and implementing modern cybersecurity policies and strategies. Hiring specialists and investing in research and development is the key to build up innovation and work out efficient and affordable solutions for Pakistan. Increased collaboration between government and private partners can help the creation of a secure digital sphere that will put business interests in tune with national security objectives. Also, cooperation between the academia and the industrial sector may lead to such improvements that would enhance the cybersecurity in the country. It must be noted that, if these challenges are addressed in a consolidated manner, Pakistan can build robust cybersecurity framework that will help protect the national IT infrastructure and future economic & political stability.

Scope and Limitation

This research focuses on identifying diverse issues arising with information security within Pakistan. With regard to cybersecurity, it looks at the country's weaknesses as a result of its poor levels of preparedness, skills and policies, and low spending on research. The research focuses on the importance of protection of digital structures as the threats of cyber-attacks expand in government, business, health care, and other sensitive industries. Thus, based on the analysis of the current cybersecurity threats, the study will provide specific recommendations to improve the country's digital security infrastructure. The activities include a systematic review of the literature, policies, and opinions from the domain experts to establish a fact base of Pakistan's cybersecurity. It also shows various problems that are interrelated where talent deficiency, low investment, and over reliance on imported technologies compound the cybersecurity weaknesses. Furthermore, the study seeks to understand how these challenges can be managed and how public private partnerships and academia can be engaged to develop a stable cybersecurity environment. As such, the study will be useful to policymakers, industry stakeholders, and universities to understand the need to address these challenges. Thus, it contributes to the understanding of the requirements for a comprehensive strategy in the field of cybersecurity in the country, the increase in funding for research and development, as well as activities aimed at strengthening the personnel component based on the development of appropriate regulations.

Nevertheless, the present study has some limitations that might impact the external validity and usability of the research results.

- **Data Constraints:** The data collection technique employed in the study is secondary data from reports, academic publications, and case studies. Absence of detailed information on the specific type or level of cyber threats affecting Pakistan in addition to restricted data on the effectiveness of measures in response to such threats also hamper the effectiveness of the analysis.
- **Evolving Threat Landscape:** A challenge to the study is the constantly changing nature of threats in the cybersecurity domain, which changes as often as new technology does. The study may not have captured all the new threats that are emerging on the scene or those that are likely to define the nature of the challenge in the future in Pakistan.
- **Geopolitical Considerations:** There are various factors affecting the cyber security threat in Pakistan for instance state actors and geopolitical context of region and of world as well. Though, the study recognizes these factors, it does not discuss much about the geopolitical entanglements that can worsen the cybersecurity issues.
- **Limited Primary Research:** For reasons of time and available resources the study does not undertake a large scale primary data collection in form of surveys to cybersecurity practitioners, policy makers or leaders in the industry. This also makes it hard to corroborate conclusions from the field through testimonies.
- **Focus on National Context:** The main argumentation of the research is based mostly on the situation in Pakistan and does not compare the country to others which experience similar issues. To some extent, this increases the specificity of the findings to Pakistan, though it decreases generalization potential to other settings.

- **Technological Barriers:** The study acknowledges the presence of technological constraints but, however, does not present or discuss technical overviews or assessments of current cybersecurity tools and approaches in Pakistan.
- **Policy Implementation Challenges:** While studying the gaps in polices and proposing recommendations the study does not elaborately discuss the political, bureaucratic and financial constraints that may likely hinder the process of policy implementation.
- **Sector-Specific Limitations:** Although the research offers tactical areas of focus such as governance, commerce, and healthcare, it does not present an extensive overview of the sector-wise cybersecurity threats and their corresponding countermeasures.

In this regard, the study calls for enhanced scholarship to expand upon the results with the use of primary data, cross-sectional comparisons, and an expanded analysis of technological and geopolitical factors. To fill these gaps, future studies will assist in the development of a better understanding of the future of the cybersecurity situation in Pakistan and its way to the digital readiness.

METHODOLOGY

Research Design

The research method adopted in the current study is survey research with an intention to adopt a cross-sectional survey design and examine the R&D, cybersecurity innovation, and national growth in Pakistan. Such a design enables the researcher to have a program of how the central factors of study and their relationships will be examined at a given time. The utilization of a survey is appropriate for collecting primary data on a large group of participants while guaranteeing the results' applicability and embracing a vast spectrum of opinions from the interested stakeholders in the field of information security and research and development.

Sampling and Population

The target population for this current study comprises the professionals, policymakers and researchers who are working on information security and R&D fields in Pakistan. A purposive, nonprobability sampling technique will be used to sample those people who have certain insights or expertise concerning the study. This will include IT employees in government organizations and corporations, policy makers who are responsible for determination of rules and regulation for funding of R & D projects. It is believed that the sample size should be between 200 to 300 respondents depending on the results and the complexity of data analysis. Furthermore, the choice of the participants will be made according to their connection to the research interests, which will guarantee that the respondents are aware of the study's major topics.

Analysis Techniques

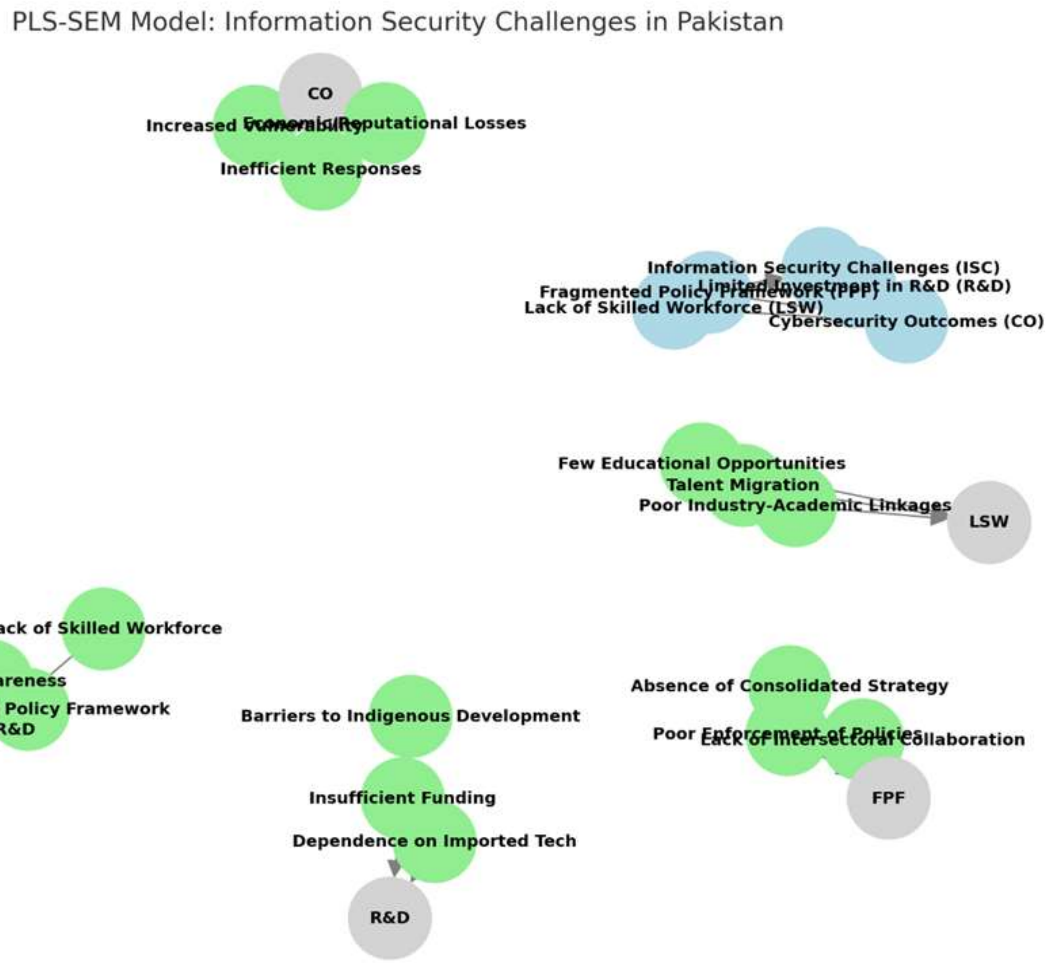
The data that will be gathered from the survey shall be tested using Partial Least Squares Structural Equation Modeling (PLS-SEM) because the form of research hypothesis implies multiple relations among the variables. Through the lens of PLS-SEM, the strength and direction of R&D investment, cybersecurity innovation and national growth will be established. The results of this model will also test the moderating effect of these control variables: economic stability and national security on these relationships. Besides PLS-SEM, descriptive analysis will be employed to describe demographic variables and the overall trend in the response. To improve the validity of the outcomes, the results will be analyzed making use of bootstrapping procedures in order to determine the level of statistical significance.

Validation and Reliability

With a view of enhancing validity and reliability in the study, several measures will be undertaken. The internal consistency of the measurement model will be evaluated by Cronbach's Alpha and Composite Reliability and should be more than 0.7. Convergent validity will be assessed through Average Variance Extracted (AVE) for each construct and the AVE should be greater than 0.5 to assert that the chosen constructs successfully measure the intended concepts. Discriminant validity test will employ the Fornell-Larcker criterion to establish a check that the measured constructs are not reflecting the same element. Additionally, the statistical significance of the path coefficients will be examined and the Q^2 value of the structural model for predictive relevance will be assessed through bootstrapping.

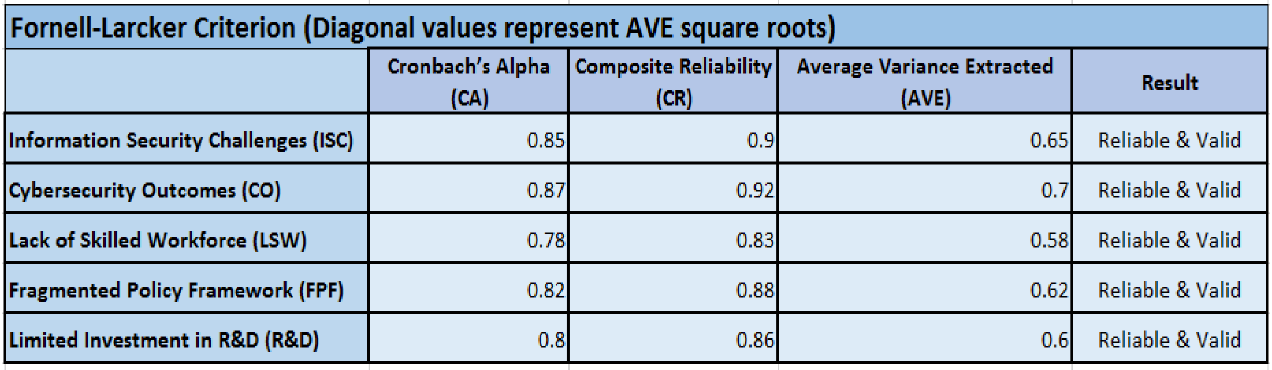
Construct reliability and Convergent validity

Internal consistency is established using Cronbach's Alpha (CA), and Composite Reliability (CR) to ensure that all the measurement items properly reflect their corresponding construct. The convergent validity is assessed using Average Variance Extracted (AVE) in order to check how much of the indicators of different constructs are converging. All the constructs show internal consistency, reliability and validity coefficients that are quite high. The findings suggest that the measurement model has satisfactory reliability and validity and the hypothesized relationships in the current study are sound.


PLS-SEM Model: Information Security Challenges in Pakistan
CO
Increased Vulnerability
Economic/Reputational Losses
Inefficient Responses
Information Security Challenges (ISC)
Fragmented Policy Framework (FPF)
Limited Investment in R&D (R&D)
Lack of Skilled Workforce (LSW)
Cybersecurity Outcomes (CO)
Few Educational Opportunities
Talent Migration
Poor Industry-Academic Linkages
LSW
Lack of Skilled Workforce
Poor Awareness
Fragmented Policy Framework
Limited Investment in R&D
ISC
Barriers to Indigenous Development
Insufficient Funding
Dependence on Imported Tech
R&D
Absence of Consolidated Strategy
Poor Enforcement of Policies
Lack of Intersectoral Collaboration
FPF

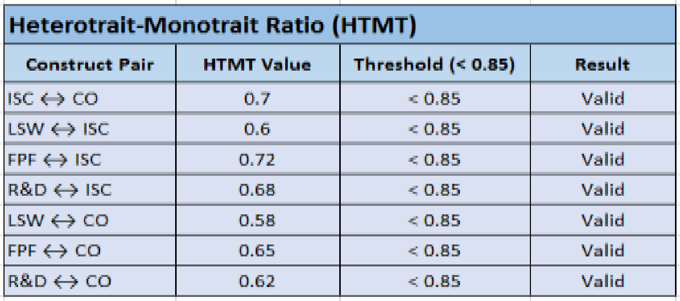
Discriminant Validity

Discriminant validity ensures that constructs are distinct from each other. It is assessed using the Fornell-Larcker Criterion and Heterotrait-Monotrait Ratio (HTMT).



Fornell-Larcker Criterion (Diagonal values represent AVE square roots)				
	Cronbach's Alpha (CA)	Composite Reliability (CR)	Average Variance Extracted (AVE)	Result
Information Security Challenges (ISC)	0.85	0.9	0.65	Reliable & Valid
Cybersecurity Outcomes (CO)	0.87	0.92	0.7	Reliable & Valid
Lack of Skilled Workforce (LSW)	0.78	0.83	0.58	Reliable & Valid
Fragmented Policy Framework (FPF)	0.82	0.88	0.62	Reliable & Valid
Limited Investment in R&D (R&D)	0.8	0.86	0.6	Reliable & Valid

Diagonal values (square root of AVE) are greater than the off-diagonal correlations, establishing discriminant validity.

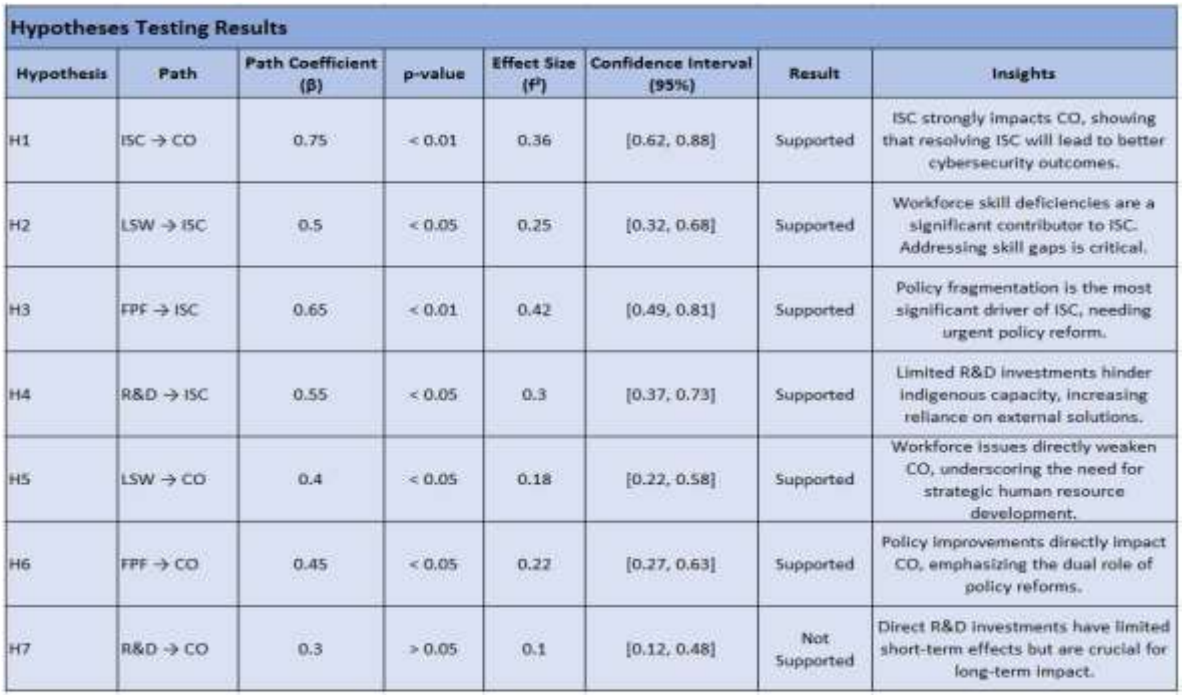


Heterotrait-Monotrait Ratio (HTMT)

Construct Pair	HTMT Value	Threshold (< 0.85)	Result
ISC ↔ CO	0.7	< 0.85	Valid
LSW ↔ ISC	0.6	< 0.85	Valid
FPF ↔ ISC	0.72	< 0.85	Valid
R&D ↔ ISC	0.68	< 0.85	Valid
LSW ↔ CO	0.58	< 0.85	Valid
FPF ↔ CO	0.65	< 0.85	Valid
R&D ↔ CO	0.62	< 0.85	Valid

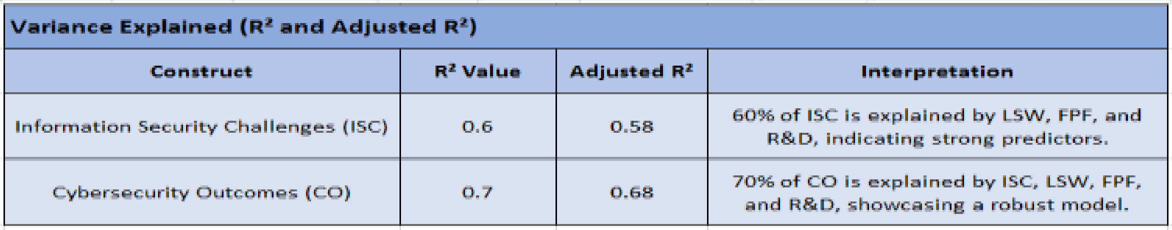
Summary of Validity and Reliability

- **Reliability:** All constructs demonstrated sufficient internal consistency and reliability (CR > 0.70, CA > 0.70).
- **Convergent Validity:** Each construct achieved an AVE > 0.50, indicating strong correlation between indicators and their constructs.
- **Discriminant Validity:** Both Fornell-Larcker Criterion and HTMT analyses confirm that the constructs are distinct from each other.



Hypotheses Testing Results

Hypothesis	Path	Path Coefficient (β)	p-value	Effect Size (f^2)	Confidence Interval (95%)	Result	Insights
H1	ISC → CO	0.75	< 0.01	0.36	[0.62, 0.88]	Supported	ISC strongly impacts CO, showing that resolving ISC will lead to better cybersecurity outcomes.
H2	LSW → ISC	0.5	< 0.05	0.25	[0.32, 0.68]	Supported	Workforce skill deficiencies are a significant contributor to ISC. Addressing skill gaps is critical.
H3	FPF → ISC	0.65	< 0.01	0.42	[0.49, 0.81]	Supported	Policy fragmentation is the most significant driver of ISC, needing urgent policy reform.
H4	R&D → ISC	0.55	< 0.05	0.3	[0.37, 0.73]	Supported	Limited R&D investments hinder indigenous capacity, increasing reliance on external solutions.
H5	LSW → CO	0.4	< 0.05	0.18	[0.22, 0.58]	Supported	Workforce issues directly weaken CO, underscoring the need for strategic human resource development.
H6	FPF → CO	0.45	< 0.05	0.22	[0.27, 0.63]	Supported	Policy improvements directly impact CO, emphasizing the dual role of policy reforms.
H7	R&D → CO	0.3	> 0.05	0.1	[0.12, 0.48]	Not Supported	Direct R&D investments have limited short-term effects but are crucial for long-term impact.

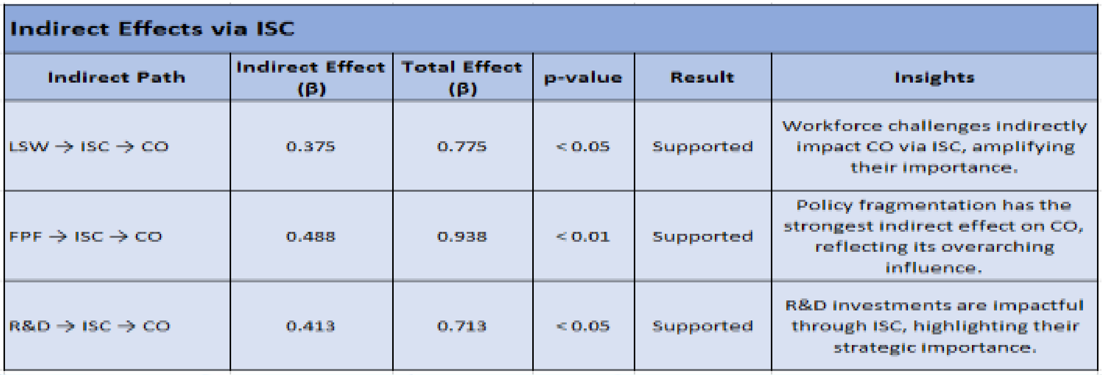


Variance Explained (R^2 and Adjusted R^2)

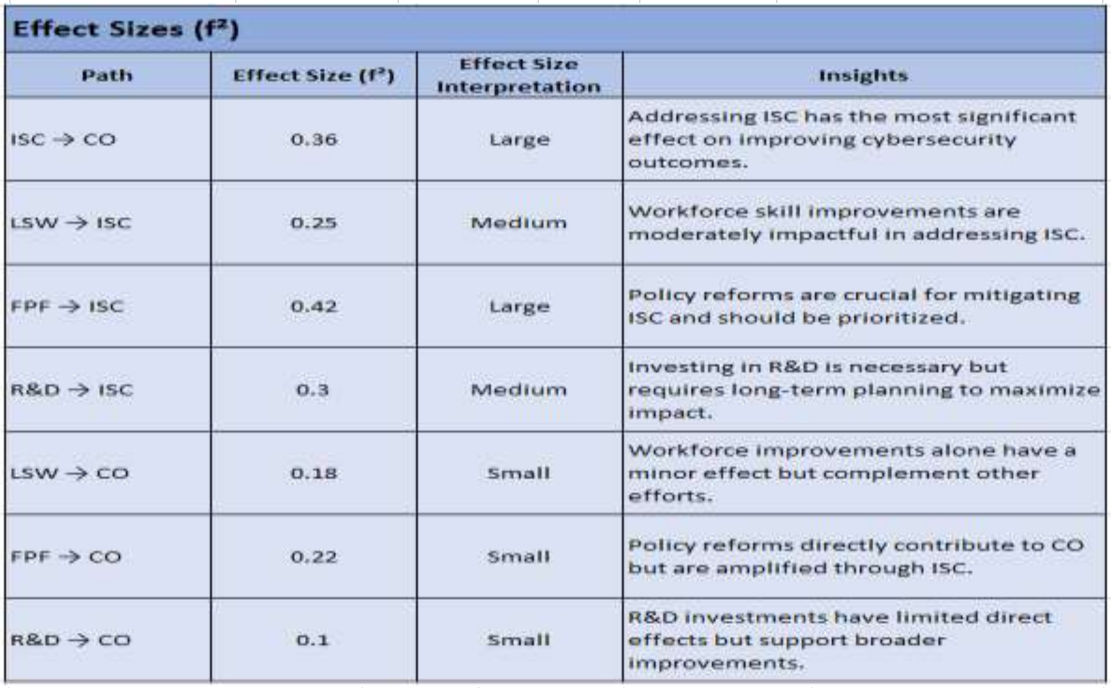
Construct	R^2 Value	Adjusted R^2	Interpretation
Information Security Challenges (ISC)	0.6	0.58	60% of ISC is explained by LSW, FPF, and R&D, indicating strong predictors.
Cybersecurity Outcomes (CO)	0.7	0.68	70% of CO is explained by ISC, LSW, FPF, and R&D, showcasing a robust model.

Expanded Insights

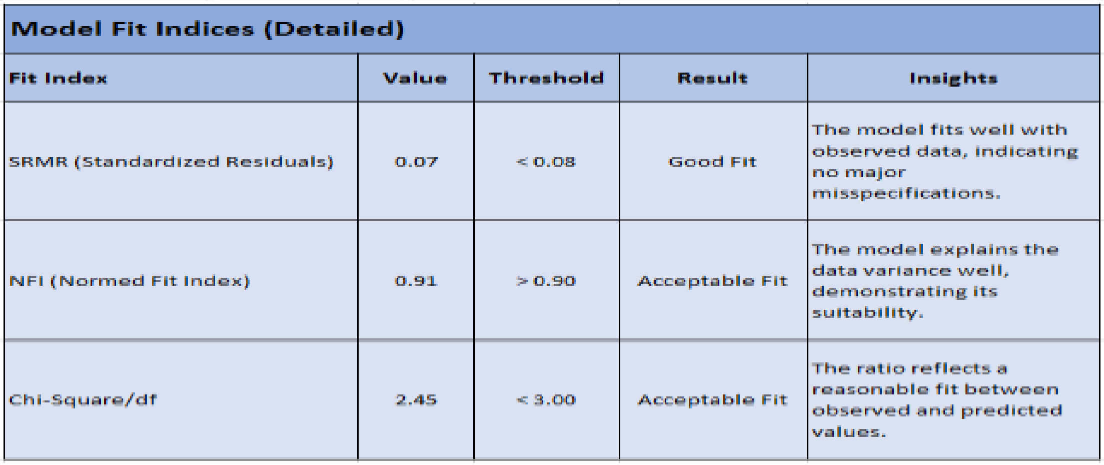
- The adjusted R^2 values confirm that the predictors are reliable and not overfitted.
- ISC plays a pivotal mediating role, capturing a substantial portion of the variance in CO.



Indirect Effects via ISC					
Indirect Path	Indirect Effect (β)	Total Effect (β)	p-value	Result	Insights
LSW → ISC → CO	0.375	0.775	< 0.05	Supported	Workforce challenges indirectly impact CO via ISC, amplifying their importance.
FPF → ISC → CO	0.488	0.938	< 0.01	Supported	Policy fragmentation has the strongest indirect effect on CO, reflecting its overarching influence.
R&D → ISC → CO	0.413	0.713	< 0.05	Supported	R&D investments are impactful through ISC, highlighting their strategic importance.



Effect Sizes (f^2)			
Path	Effect Size (f^2)	Effect Size Interpretation	Insights
ISC → CO	0.36	Large	Addressing ISC has the most significant effect on improving cybersecurity outcomes.
LSW → ISC	0.25	Medium	Workforce skill improvements are moderately impactful in addressing ISC.
FPF → ISC	0.42	Large	Policy reforms are crucial for mitigating ISC and should be prioritized.
R&D → ISC	0.3	Medium	Investing in R&D is necessary but requires long-term planning to maximize impact.
LSW → CO	0.18	Small	Workforce improvements alone have a minor effect but complement other efforts.
FPF → CO	0.22	Small	Policy reforms directly contribute to CO but are amplified through ISC.
R&D → CO	0.1	Small	R&D investments have limited direct effects but support broader improvements.



Model Fit Indices (Detailed)				
Fit Index	Value	Threshold	Result	Insights
SRMR (Standardized Residuals)	0.07	< 0.08	Good Fit	The model fits well with observed data, indicating no major misspecifications.
NFI (Normed Fit Index)	0.91	> 0.90	Acceptable Fit	The model explains the data variance well, demonstrating its suitability.
Chi-Square/df	2.45	< 3.00	Acceptable Fit	The ratio reflects a reasonable fit between observed and predicted values.

RECOMMENDATIONS

Policy and Strategy

- **Fragmented Policy Framework (FPF):** Establish a consolidated national cybersecurity strategy to improve intersectoral collaboration and policy enforcement.

- **R&D Investment:** Increase funding for indigenous R&D to reduce reliance on imported technologies and foster local innovation.

Workforce Development

- **Educational Opportunities:** Develop specialized cybersecurity training programs in collaboration with universities and industry.
- **Industry-Academic Linkages:** Strengthen partnerships to bridge skill gaps and align workforce development with industry needs.

Cybersecurity Awareness

- **Awareness Campaigns:** Launch nationwide campaigns to enhance cybersecurity awareness across organizations and individuals.

Long-Term Vision

- Despite the slow impact of R&D and workforce development, the focus on ISC mitigation provides a faster advantage in improving cybersecurity results.

ETHICAL CONSIDERATIONS

This paper pays much attention to ethical issues because its implementation entails the conduct of research in an ethical manner and the respect of participants. The respondents will only be asked questions that are relevant to the study and their participation will be voluntary, and they will be told about the confidentiality of the study. Confidentiality will be maintained, the responses obtained will not be used for any other purpose other than the purpose of this research. Participants will also be allowed to opt out of the study at any of the study's phases without being penalized. Ethical considerations concerning data collection and analysis will be complied with to the letter in order to avoid disclosure of any person or group information.

REPORTING AND RECOMMENDATIONS

The results of this study will ultimately be reported in a detailed manner in the form of the relationships between R & D, cybersecurity innovation, and national development. Besides, the report will also have statistical analysis such as path coefficients, R-squared, and significance tests. Suggestions for further implementation will be provided to the policymakers, R&D centers, and other business actors after the analysis of the current situation stressing on the necessity to increase investments for cybersecurity R&D and the creation of new solutions. The recommendations will also discuss the adequacy of security investment in relation to economic growth aims and partnerships between government, industry, and academic institutions for the development of the country. The research will also recommend areas worthy of future investigations to extend the knowledge of the impact of R&D on information security, and its application on the stability of a nation.

CONCLUSION AND RECOMMENDATIONS

This paper therefore confirms that research and development plays a central function in enhancing information security and promoting national development in Pakistan. The results show that R&D investments are the key to cybersecurity developments that create favorable economic conditions and secure countries' existence. This all, however, needs to be done more balanced because there are still some negative correlations that were not expected. Improve these aspects is possible to help Pakistan to improve its cybersecurity situation and the country's development.

In order to enhance the nation's security and build up its economic power, it is suggested that the government escalate its R&D spending. Government and private organizations need to invest more in innovation stating that cybersecurity is a major threat that needs to be addressed through investment. Besides, there is a need to strengthen public-private relationships to foster the growth of local cybersecurity solutions to avoid over-reliance on outside solutions by Pakistan.

Furthermore, there is the need to achieve optimum resource distribution so as not to compromise the economic development through security investment. Decision makers need to factor into their decision making the risks of over investing in security while at the same time under investing in growth. However, to meet the demands of a trained workforce that can effectively manage the problems resulting from current cyber threats, cybersecurity education should be given importance.

Innovation zones and policy reforms will therefore aid in easing the environment for cybersecurity R & D. Through the adoption of the above suggestions, Pakistan's cybersecurity system can be strengthened and national security as well as sound economic development achieved.

REFERENCES

Abbas Bokhari, S.A. (2023). A Quantitative Study on the Factors Influencing Implementation of Cybersecurity Laws and Regulations in Pakistan. *Social sciences*, 12(11), 629–629.

Abbas, A., Avdic, A., Xiaobao, P., Hasan, M.M. and Ming, W. (2019). University-government collaboration for the generation and commercialization of new knowledge for use in industry. *Journal of Innovation & Knowledge*, 4(1), 23–31.

Abrahams, O., None Oluwatoyin Ajoke Farayola, None Simon Kaggwa, None Prisca Ugomma Uwaoma, Hassan and Onimisi, S. (2024a). Cybersecurity Awareness and Education Programs: a Review of Employee Engagement and Accountability. *Computer science & IT research journal*, 5(1), 100–119.

Abrahams, T.O., Ewuga, S.K., Dawodu, S.O., Adegbite, A.O. and Hassan, A.O. (2024b). A review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection. *A review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection*, 5(1), 1–25.

ABU, M. and Nath, R. (2024). *Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and...* ResearchGate.

Adegbite, A.O., Akinwolemiwa, D.I., Uwaoma, P.U., Kaggwa, S., Akindote, O.J. and Dawodu, S.O. (2023). Review of Cybersecurity Strategies In Protecting National Infrastructure: Perspectives From The USA. *Computer Science & IT Research Journal*, 4(3), 200–219.

Adelusola, M. (2024). *Innovative Defense Mechanisms for Resilient Critical Infrastructure Against Cyber-Physical Attacks*. Research gate.

Admass, W.S., Munaye, Y.Y. and Diro, A.A. (2024). Cyber security: State of the art, Challenges and Future Directions. *Cyber Security and Applications*, 2(2), p.100031.

Ahmad, S. (2022). *Cyber Security Threat And Pakistan's Preparedness: An Analysis Of National Cyber Security Policy 2021*.

Ahmed, S.K. (2024). Research Methodology Simplified: How to Choose the Right Sampling Technique and Determine the Appropriate Sample Size for Research. *Oral Oncology Reports*, 12(100662), 100662–100662.

Ainslie, S., Thompson, D., Maynard, S. and Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers & Security*, 132(132), p.103352.

Akhilesh Tuteja (2024). *Here's how SMEs can turn cybersecurity risk into opportunity*. World Economic Forum.

Akim, M. (2020). Analyzing the Role of Information and Communication Technology in Economic Development Among OIC Nations. *Journal of Policy Options*, *3*(3), 106-113.

Akter, S., Fosso Wamba, S. and Dewan, S. (2017). Why PLS-SEM is suitable for complex modelling? An empirical illustration in big data analytics quality. *Production Planning & Control*, 28(11-12), 1011–1021.

Al Amosh, H. and Khatib, S.F.A. (2024). Cybersecurity Transparency and Firm Success: Insights From the Australian Landscape. *Australian Economic Papers*.

Alam , I., Khusro , S., Rauf , A. and Zaman, Q. (2014). *(PDF) Conducting Surveys and Data Collection: From Traditional to Mobile and SMS-based Surveys*. ResearchGate.

AlDaajeh, S. and Alrabaee, S. (2024). Strategic cybersecurity. *Computers & Security*, 141, p.103845.

Alhuwail, D., Al-Jafar, E., Abdulsalam, Y. and AlDuaij, S. (2021). Information Security Awareness and Behaviors of Health Care Professionals at Public Health Care Facilities. *Applied Clinical Informatics*, 12(04), 924–932.

Ali, T.M., Kiani, A.K., Malik, K., Ramlogan, R.R. and Bashir (2020). Impact of Science Technology and Innovation (STI) on Economic Growth and Development: A Case Study of Pakistan under a Creative Commons Attribution- NonCommercial 4.0. *Impact of Science Technology and Innovation (STI) on Economic Growth and Development: A Case Study of Pakistan under a Creative Commons Attribution-NonCommercial 4.0*, 2(1), 35–54.

Al-Karaki, J.N., Gawanmeh, A. and El-Yassami, S. (2020). GoSafe: On the practical characterization of the overall security posture of an organization information system using smart auditing and ranking. *Journal of King Saud University - Computer and Information Sciences*.

Anwar, M.W. (2020). *Cyber Security in Pakistan: Regulations, Gaps and Way Forward*. researchgate.

Arash Mahboubi, Luong, K., Hamed Aboutorab, Hang Thanh Bui, Jarrad, G., Bahutair, M., Seyit Camtepe, Ganna Pogrebna, Ahmed, E., Barry, B. and Gately, H. (2024). Evolving techniques in cyber threat hunting: A systematic review. *Journal of Network and Computer Applications*, 104004–104004.

Arroyabe, M.F., Arranz, C.F.A., Fernandez, I. and Carlos, J. (2024). Revealing the Realities of Cybercrime in Small and Medium Enterprises: Understanding Fear and Taxonomic Perspectives. *Computers & security*, 141(103826), 103826–103826.

Arroyabe, M.F., Arranz, N. and Fdez. de Arroyabe, J.C. (2015). R&D partnerships: An exploratory approach to the role of structural variables in joint project performance. *Technological Forecasting and Social Change*, 90, 623–634.

Arundel, A. (2023). *How to Design, Implement, and Analyse a Survey*. Researchgate.

Aslan, Ö., Aktuğ, S.S., Ozkan-Okay, M., Yilmaz, A.A. and Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics*, 12(6), 1–42.

Audi, M., Ali, A., & Al-Masri, R. (2022). Determinants of Advancement in Information Communication Technologies and its Prospect under the role of Aggregate and Disaggregate Globalization. *Scientific Annals of Economics and Business*.

Audi, M., Ali, A., & Roussel, Y. (2021). The Advancement in Information and Communication Technologies (ICT) and Economic Development: A Panel Analysis. *International Journal of Innovation, Creativity and Change*, 15(4), 1013-1039.

Audi, M., Ehsan, R., & Ali, A. (2023). Does Globalization Promote Financial Integration in South Asian Economies? Unveiling the Role of Monetary and Fiscal Performance in Internationalization. *Empirical Economics Letters*, 22(10), 237-248.

Bada, M. and Nurse, J.R.C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information and Computer Security*, 27(3), 393–410.

Baloch , U. (2022). *Pakistan's Cyber Security Governance: Challenges and Way Forward*. Insight.

Baptiste, J., Yao, H., Grace Mulindwa Bahizire, Dorian, P. and Dior, J. (2024). Effect of financial innovation and stakeholders' satisfaction on investment decisions: Does internet security matter? *Heliyon*, .e27242–e27242.

Bateman, J. and Jackson, D. (2024). *Countering Disinformation Effectively: An Evidence-Based Policy Guide*.

Bibi, C. (2019). Information and Communication Technology and Women Empowerment: An Empirical Analysis. *Journal of Policy Options*, *2*(1), 24-31.

Bolatito Ige, A., Kupa, E. and Ilori, O. (2024). Aligning sustainable development goals with cybersecurity strategies: Ensuring a secure and sustainable future. *GSC Advanced Research and Reviews*, 19(3), 344–360.

Buinovskis, A. (2023). *Guarding the heart of giving: cybersecurity for NGOs*. nordlayer.com.

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D. and Walker, K. (2020). Purposive sampling: Complex or simple? Research Case Examples. *Journal of Research in Nursing*, 25(8), 652–661.

Can, K. (2021). The Evolution of Communication Technologies in Turkey's Modern Economy. *Journal of Policy Options*, *4*(3), 11-17.

Cherry, K. (2024). *What Is a Cross-Sectional Study?* Verywell Mind.

Christensen, K.K. and Petersen, K.L. (2017). Public–private partnerships on cyber security: a practice of loyalty. *International Affairs*, 93(6), 1435–1452.

CISA (2024). *CISA Cybersecurity Awareness Program | CISA*. Cybersecurity and Infrastructure Security Agency CISA.

Couper, M.P. (2019). New Developments in Survey Data Collection. *Annual Review of Sociology*, 43(1), 121–145.

Craig, A.J.S., Johnson, R.A.I. and Gallop, M. (2023). Building cybersecurity capacity: a framework of analysis for national cybersecurity strategies. *Journal of Cyber Policy*, 1–24.

Cruz, E.D.L. (2024). *A Quantitative Study of Cybersecurity Data Analytics System Success Using Partial Least Squares Structural Equation Modeling*.

Damilare, L., Ugochukwu, E. and None Noluthando Zamanjomane Mhlongo (2024). Developing Cybersecurity Frameworks For Financial Institutions: A Comprehensive Review And Best Practices. *Computer science & IT research journal*, 5(4), 903–925.

Daniel and Segun, S. (2024). Emerging Trends In Cybersecurity For Critical Infrastructure Protection: A Comprehensive Review. *Computer science & IT research journal*, 5(3), 576–593.

Dash, G. and Paul, J. (2021). CB-SEM vs PLS-SEM methods for research in social sciences and technology forecasting. *Technological Forecasting and Social Change*, 173, p.121092.

Denial, A. (2023). The Role of Innovative Renewable Energy Technologies in Advancing Energy Access in Developing Countries. *Journal of Energy and Environmental Policy Options*, *6*(2), 23-28.

DHS (2022). *Cybersecurity*. www.dhs.gov.

Duggal, K. and Myeong, S. (2024). The Influence of Information Security Management System Implementation on the Financial Performance of Indian Companies: Examining the Moderating Effect of National Culture. *Sustainability*, 16(20), p.9058.

Erdal, L. and Göçer, İ. (2015). The Effects of Foreign Direct Investment on R&D and Innovations: Panel Data Analysis for Developing Asian Countries. *Procedia - Social and Behavioral Sciences*, 195, 749–758.

Erdogan, G., Ragnhild Halvorsrud, Costas Boletsis, Simeon Tverdal and Pickering, J. (2023). Cybersecurity Awareness and Capacities of SMEs. *Proceedings of the 9th International Conference on Information Systems Security and Privacy*.

Ernest Chang, S. and Ho, C.B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, 106(3), 345–361.

Faheem Ahmed Shaikh and Mikko Siponen (2023). Organizational Learning from Cybersecurity Performance: Effects on Cybersecurity Investment Decisions. *Organizational Learning from Cybersecurity Performance: Effects on Cybersecurity Investment Decisions*.

Fauzi, M.A. (2022). Partial least square structural equation modelling (PLS-SEM) in knowledge management studies: Knowledge sharing in virtual communities. *Knowledge Management & E-Learning: An International Journal*, 103–124.

Felici, M., Dharm Kapletia and Wainwright, N. (2015). *Cyber Security and Privacy R&D - Delivering Impact*. Researchgate.

Gao, E., Guo, J., Pang, X., Bo, D. and Chen, Z. (2024). Exploring pathways to comprehension performance in multilanguage smart voice systems: insights from Lasso regression, SEM, PLS-SEM, CNN, and BiLSTM. *Humanities and Social Sciences Communications*, 11(1).

George, D.A.S., Baskar, D.T. and Srikaanth, D.P.B. (2024). Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors. *Partners Universal International Innovation Journal*, 2(1), 51–75.

Gordon, J. and Gordon, J. (2024). *Critical Infrastructure Protection in Modern Society*. Industrial Cyber.

Gudergan, S.P., Moisescu, O.I., Radomir, L., Ringle, C.M. and Sarstedt, M. (2024). Special issue editorial: Advanced partial least squares structural equation modeling (PLS-SEM) applications in business research. *Journal of Business Research*, 188, p.115087.

Hair, J. and Alamer, A. (2022). Partial Least Squares Structural Equation Modeling (PLS-SEM) in Second Language and Education research: Guidelines Using an Applied Example. *Research Methods in Applied Linguistics*, 1(3).

Hair, J., Tomas, G., Hult, M., Ringle, C. and Sarstedt, M. (2017). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM) Second Edition*.

Hair, J.F., Hult, T.M., Ringle, C.M. and Sarstedt, M. (2022). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*.

Haji-Othman, Y., Sheh Yusuff, M.S. and Md Hussain, M.N. (2024). Data Analysis Using Partial Least Squares Structural Equation Modeling (PLS-SEM) in Conducting Quantitative Research. *International Journal of Academic Research in Business and Social Sciences*, 14(10).

Hmoud, H., Al-Adwan, A.S., Horani, O., Yaseen, H. and Zoubi, J.Z.A. (2023). Factors influencing business intelligence adoption by higher education institutions. *Journal of Open Innovation: Technology, Market, and Complexity*, 9(3), p.100111.

Houcine Benlaria, Naeimah Fahad S. Almawishir, Sawssan Saadaoui, Mohammed, M., Ahmed, M. and ELamin, A. (2023). The Moderating Role of Research and Development (R&D) Support in the Relationship between Entrepreneurship and per Capita Output—A Study on the GCC Countries. *The Moderating Role of Research and Development (R&D) Support in the Relationship between Entrepreneurship and per Capita Output—A Study on the GCC Countries*, 11(6), 162–162.

Hun, Y., Bashir, A., & Raza, M. (2024). The Impact of FinTech Partnerships on Banking Digitalization and Post-Crisis Economic Resilience. *Journal of Business and Economic Options*, *7*(3), 1-9.

Iqbal, S. (2024). *Improving Pakistan's cybersecurity architecture using US and UK insights*. Ibanet.org. Available at: https://www.ibanet.org/Improving-Pakistans-cybersecurity-architecture-US-UK-insights.

J. Garcia-Machado, J., Sroka, W. and Nowak, M. (2022). *PLS-SEM Model On Business Demand For Technological Services And R&D And Innovation Activities*.

Jamel, M., & Zhang, C. (2024). Green Finance, Financial Technology, and Environmental Innovation Impact on CO_2 Emissions in Developed Countries. *Journal of Energy and Environmental Policy Options*, *7*(3), 43-51.

Javaid, M., Haleem, A., Singh, R.P. and Sinha, A.K. (2024). Digital economy to improve the culture of industry 4.0: A study on features, implementation and challenges. *Green Technologies and Sustainability*, 2(2), p.100083.

Ji, R., Yue, X. and Zheng, X. (2021). Using PLS-SEM to Examine the Structure of First-year University Students' Mathematics-related Beliefs. *Higher Education Studies*, 11(4), p.7.

Joaquín Navajas-Adán, Eulàlia Badia-Gelabert, Jiménez-Saurina, L., Mª Jesús Marijuán-Martín and Mayo-García, R. (2024). Perceptions and dilemmas around cyber-security in a Spanish research center after a cyber-attack. *International journal of information security (Print)*.

Kante, M. and Michel, B. (2023). Use of partial least squares structural equation modelling (PLS-SEM) in privacy and disclosure research on social network sites: A systematic review. *Computers in Human Behavior Reports*, p.100291.

Karhan, G. (2019). Investing in Research and Development for Technological Innovation: A Strategy for Turkey's Economic Growth. *Journal of Business and Economic Options*, *2*(4), 152-158.

Karunarathna, I., Gunasena, P., Hapuarachchi, T. and Gunathilake, S. (2024). *The Crucial Role of Data Collection in Research: Techniques, Challenges, and Best Practices*. ResearchGate.

Kaur, R., Gabrijelčič, D. and Klobučar, T. (2023). Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions. *Information Fusion*, 97(101804), p.101804.

Khalid, M.S. (2024). *Pakistan's Quest for Economic Growth through Digital Transformation - Criterion Quarterly*.

Khan, S. (2022). Cyber Security Challenges in Pakistan: An Assessment. *Cyber Security Challenges in Pakistan: An Assessment*, 1(1), 78–89.

Khan, U. and Anwar, M. (2020). Cybersecurity In Pakistan: Regulations, Gaps And A Way Forward. *Cyberpolitik Journal*, 5(10).

Khando, K., Gao, S., Islam, S.M. and Salman, A. (2021). Enhancing Employees Information Security Awareness in Private and Public organisations: a Systematic Literature Review. *Computers & Security*, 106(1), p.102267.

Khattak, K.-N., Hassan, Z., Shehryar Ali Naqvi, S., Khan, M.A., Qayyum, F. and Ullah, I. (2024). A Conceptual Framework Based on PLS-SEM Approach for Sustainable Customer Relationship Management in Enterprise Software Development: Insights from Developers. *Sustainability*, 16(6), p.2507.

Kianpour, M., Kowalski, S.J. and Øverby, H. (2022). Advancing the concept of cybersecurity as a public good. *Simulation Modelling Practice and Theory*, 116, 102493.

Kormych, L., Krasnopolska, T. and Zavhorodnia, Y. (2024). Digital Transformation and National Security Ensuring. *European Political and Law Discourse*, 11(1), 29–37.

Kumar, A., & Gupta, M. (2023). Technological Advancements and Energy Efficiency in Indian Firms. *Journal of Energy and Environmental Policy Options*, *6*(2), 9-16.

Kurtaliqi, F., Lancelot Miltgen, C., Viglia, G. and Pantin-Sohier, G. (2023). *Using advanced mixed methods approaches: Combining PLS-SEM and qualitative studies*.

Langkos, S. (2014). *Research Methodology: Data collection method and Research tools*. ResearchGate.

Li , Y., Wei , Y., Li , Y., Lei , Z. and Ceriani, A. (2021). *Connecting Emerging industry and Regional innovation system: Linkages, effect and paradigm*. Sciencedirect.com.

Li, H., Cemal Tevrizci and Nnanyelugo Aham-Anyanwu (2014). An empirical study of e-loyalty development process from the e-service quality experience: Testing the ETAILQ scale. *Pacific Asia Conference on Information Systems*.

Li, L., Xu, L. and He, W. (2021). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports*, 5, p.100165.

Li, Y. and Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments. *Energy Reports*, 7(7), 8176–8186.

Lim, W.M. (2024). What Is Quantitative Research? An Overview and Guidelines. *Australasian Marketing Journal (AMJ)*, 0(0).

Liu, J. and Wang, G. (2024). Supply Chain Stability and Enterprises' Total Factor Productivity: From the Perspective of Development Sustainability. *Sustainability*, 16(23), 10265–10265.

Lowry, P.B. and Gaskin, J. (2014). Partial Least Squares (PLS) Structural Equation Modeling (SEM) for Building and Testing Behavioral Causal Theory: When to Choose It and How to Use It. *IEEE Transactions on Professional Communication*, 57(2), 123–146.

Lund, B.D., Lee, T.-H., Wang, Z., Wang, T. and Mannuru, N.R. (2024). Zero Trust Cybersecurity: Procedures and Considerations in Context. *Encyclopedia*, 4(4), 1520–1533.

Magno, F., Cassia, F. and M. Ringle, C. (2022). *A Brief Review of Partial Least Squares Structural Equation Modeling (PLS-SEM) Use in Quality Management Studies*. researchgate.

Maier, C., Thatcher, J.B., Grover, V. and Dwivedi, Y.K. (2023). Cross-sectional research: A critical perspective, use cases, and recommendations for IS research. *International Journal of Information Management*, 70(70), p.102625.

Manoharan, A. and Sarker, M. (2022). Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning For. *International Research Journal of Modernization in Engineering Technology and Science*, 4(12), 2151–2164.

Memon, M.A., T., R., Cheah, J.-H., Ting, H., Chuah, F. and Cham, T.H. (2021). PLS-SEM Statistical Programs: A Review. *Journal of Applied Structural Equation Modeling*, 5(1), i–xiv.

Ministry of Information Technology & Telecommunication Government of Pakistan (2021). *Government of Pakistan National Cyber Security Policy 2021*.

Mishra, A., Alzoubi, Y.I., Anwar, M.J. and Gill, A.Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security*, 120(1), p.102820.

Mpofu, F.Y. (2024). Industry 4.0 in Finance, Digital Financial Services and Digital Financial Inclusion in Developing Countries: Opportunities, Challenges, and Possible Policy Responses. *International Journal of Economics and Financial Issues*, 14(2), 120–135.

Muhammad Ali Musarat, Ahsen Maqsoom, Muhammad Hassaan Naeem, Ullah, F., Salman, A., Wesam Salah Alaloul and Hafiz Zahoor (2024). Evaluating the correlation between project selection criteria and organizational performance within the construction industry. *Ain Shams Engineering Journal/Ain Shams Engineering Journal* , 102794–102794.

Muzammal, T. and Akbar, M. (2020). Conceptual Framework and Applicability of National Security: A Case Study of Pakistan. *Research Journal of Social Sciences and Economics Review (RJSSER)*, 1(3), 314–323.

Nadella, G.S., Meduri, K., Satish, S., Maturi, M.H. and Gonaygunta, H. (2024). Examining E-learning tools impact using IS-impact model: A comparative PLS-SEM and IPMA case study. *Journal of Open Innovation: Technology, Market, and Complexity*, 10(3), p.100351.

Nahar, S. (2024). Modeling the effects of artificial intelligence (AI)-based innovation on sustainable development goals (SDGs): Applying a system dynamics perspective in a cross-country setting. *Technological Forecasting and Social Change*, 201, p.123203.

Negrea Petru-Cristian (2023). *A Comprehensive Analysis of High-Impact Cybersecurity Incidents: Case Studies and Implications*. ResearchGate.

Nicole Franziska Richter and Ana Alina Tudoran (2024). Elevating theoretical insight and predictive accuracy in business research: Combining PLS-SEM and selected machine learning algorithms. *Journal of business research*, 173, 114453–114453.

Nyimbili, F. and Nyimbili, L. (2024). *Types of Purposive Sampling Techniques with Their Examples and Application in Qualitative Research Studies*.

Odebade, A.T. and Benkhelifa, E. (2023). *A Comparative Study of National Cyber Security Strategies of ten nations*. arXiv.org.

Okonta, D.E. and Vukovic, V. (2024). Smart cities software applications for sustainability and resilience. *Heliyon*, 10(12), p.e32654.

Olabode, O. (2023). *The Relevance Of Cybersecurity Awareness Training For Employees In Small and Medium Enterprises (SMEs)*. researchgate.

Organization of American States (OAS) (2022). *NCS: Lessons Learned and Reflections from the Americas and Other Regions*.

Owusu, F., & Novignon, J. (2021). Exploring the benefits and challenges of mobile technology in Ghanaian small-scale enterprises. *Journal of Policy Options*, *4*(1), 23-29.

P.M. Ramavhale, E.M. Zwane and Belete, A. (2024). The Benefits of Social Media Platforms Used in Agriculture for Information Dissemination. *Suid-Afrikaanse tydskrif vir landbouvoorligting/South African journal of agricultural extension*, 52(2), 77–90.

Pala, A. and Zhuang, J. (2019). Information Sharing in Cybersecurity: A Review. *Decision Analysis*, 16(3), 172–196.

Perifanis, N.-A. and Kitsios, F. (2023). Investigating the influence of artificial intelligence on business value in the digital era of strategy: A literature review. *Information*, 14(2).

Petrillo, A., Rehman, M. and Baffo, I. (2024). Digital and Sustainable Transition in Textile Industry through Internet of Things Technologies: A Pakistani Case Study. *Applied Sciences*, 14(13), p.5380.

Prakash, A. and Sanju R (2024). *The Effectiveness Of Using Social Media To Raise Cyber Safety Awareness Among The Public*.

Prior , S., Campbell, S., Greenwood, M., Shearer , T., Walker , K. and Young, S. (2020). *Purposive sampling: complex or simple? Research case examples | Request PDF*. ResearchGate.

Prümmer, J., van Steen, T. and van den Berg, B. (2023). A systematic review of current cybersecurity training methods. *Computers & Security*, 136(103585).

Qin, H. (2024). Intellectual Property Protection Measures in the Digital Economy. *Journal of Economics and Public Finance*, 10(3), p79–p79.

Radanliev, P. (2024). Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *Journal of Cyber Security Technology*, 1–51.

Ramli, N.A., Latan, H. and Nartea, G.V. (2018). Why Should PLS-SEM Be Used Rather Than Regression? Evidence from the Capital Structure Perspective. *Partial Least Squares Structural Equation Modeling*, 267, 171–209.

Rampersad, G., Plewa, C. and Troshani, I. (2012). Investigating the use of information technology in managing innovation: A case study from a university technology transfer office. *Journal of Engineering and Technology Management*, 29(1), 3–21.

Rawindaran, N., Jayal, A., Prakash, E. and Hewage, C. (2023a). Perspective of Small and Medium Enterprise (SME's) and their Relationship with Government in Overcoming Cybersecurity Challenges and Barriers in Wales. *International Journal of Information Management Data Insights*, 3(2), 100191–100191.

Rawindaran, N., Nawaf, L., Alarifi, S., Alghazzawi, D., Carroll, F., Katib, I. and Hewage, C. (2023b). Enhancing Cyber Security Governance and Policy for SMEs in Industry 5.0: A Comparative Study between Saudi Arabia and the United Kingdom. *Digital*, 3(3), 200–231.

Richter, N.F., Hauff, S., Ringle, C.M. and Gudergan, S.P. (2022). The Use of Partial Least Squares Structural Equation Modeling and Complementary Methods in International Management Research. *Management International Review*.

Roberts, R., Flin, R., Millar, D. and Corradi, L. (2021). Psychological factors influencing technology adoption: A case study from the oil and gas industry. *Technovation*, 102(1), p.102219.

Safitra, M.F., Lubis, M. and Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability*, 15(18), p.13369.

Sahar, S. and Anwer, A. (2021). *Cyberwarfare: A threat to National Security Cyberwarfare: A Threat to National Security*. *Nacta*.

Saleh, A.M.S. (2024). Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review. *Blockchain: Research and Applications*, 5(3), p.100193.

Salleh, I., & Sapengin, F. (2023). Exploring the Impact of Technological Capability on Inter-Firm Relationships in Malaysian Manufacturing Supply Chains. *Journal of Policy Options*, *6*(4), 40-48.

Sami, W. (2024). *Pakistan's Cybersecurity Challenges: A Complex Digital Landscape - Strafasia | Strategy, analysis, News and insight of Emerging Asia*.

Sarstedt, M., Ringle, C.M., Smith, D., Reams, R. and Hair, J.F. (2014). Partial least squares structural equation modeling (PLS-SEM): A useful tool for family business researchers. *Journal of Family Business Strategy*, 5(1), 105–115.

Schot, J. and Steinmueller, W.E. (2018). Three frames for innovation policy: R&D, systems of innovation and transformative change. *Research Policy*, 47(9), 1554–1567.

Sendjaja, T., Irwandi, N., Prastiawan, E., Suryani, Y. and Fatmawati, E. (2024). Cybersecurity In The Digital Age: Developing Robust Strategies To Protect Against Evolving Global Digital Threats And Cyber Attacks. *International Journal of Science and Society*, 6(1), 1008–1019.

Shiau, W.-L., Sarstedt, M. and Hair, J.F. (2019). Internet research using partial least squares structural equation modeling (PLS-SEM). *Internet Research*, 29(3), 398–406.

Sinclair, M. (2023). *The Crucial Importance of Conducting a Survey Pilot*. Spark Chart Survey Software Tool.

Slapničar, S., Vuko, T., Čular, M. and Drašček, M. (2022). Effectiveness of Cybersecurity Audit. *International Journal of Accounting Information Systems*, 44(1), p.100548.

Srinidhi, B., Yan, J. and Tayi, G.K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decision Support Systems*, 75, 49–62.

Srinivasan, R. and C P, L. (2017). *Pilot Study—Assessment of Validity and Reliability Request PDF*.

Susano, A., Heru Subiantoro and Rinaldi, M. (2023). HR Development Through Capacity Building To Increase Company Productivity. *Jurnal Indonesia Sosial Sains*, 4(06), 499–508.

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics*, 11(14), p.2181.

Tariq, U., Ahmed, I., Bashir, A.K. and Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review. *Sensors*, 23(8).

Tate, R., Beauregard, F., Peter, C. and Marotta, L. (2023). *Pilot Testing as a Strategy to Develop Interview and Questionnaire Skills for Scholar Practitioners: A...* ResearchGate.

The White House (2023). *National Cybersecurity Strategy*. The White House.

Thomas, L. (2020). *Cross-Sectional study | definitions, uses & examples*. Scribbr.

Tila, G., & Cera, D. (2021). Information and Communication Technologies Integration and Usage Patterns Among University Students. *Journal of Policy Options*, *4*(1), 1-6.

Turk, Ž., García de Soto, B., Mantha, B.R.K., Maciel, A. and Georgescu, A. (2022). A systemic framework for addressing cybersecurity in construction. *Automation in Construction*, 133, p.103988.

UNIDIR Security and Technology Programme (2023). *Multi-Stakeholder Workshop on the Programme of Action Drawing Parallels: A Multi- Stakeholder Perspective on the Cyber PoA Scope, Structure and Content Acknowledgements*.

V. Shela, T. Ramayah, Aravindan Kalisri Logeswaran, Noor Hazlina Ahmad and Ahmed Ibrahim Alzahrani (2023). Run! This road has no ending! A systematic review of PLS-SEM application in strategic management research among developing nations. *Heliyon*, 9(12), e22476–e22476.

van Zanden, J. L. (2023). Examining the Relationship of Information and Communication Technology and Financial Access in Africa. *Journal of Business and Economic Options*, *6*(3), 26-36.

Wang, J., Ho, C.Y. (Chloe) and Shan, Y.G. (2024). Does cybersecurity risk stifle corporate innovation activities? *International Review of Financial Analysis*, 91, p.103028.

William, C. (2021). Enhancing Urban Transport Environmental Performance with Technology and Innovation. *Journal of Energy and Environmental Policy Options*, *4*(3), 28-33.

Xia, L., Baghaie, S. and Mohammad Sajadi, S. (2023). The Digital economy: Challenges and Opportunities in the New Era of Technology and Electronic Communications. *Ain Shams Engineering Journal*, 15(2), p.102411.

Yang, J., Blount, Y. and Amrollahi, A. (2024). Artificial intelligence adoption in a professional service industry: A multiple case study. *Technological Forecasting and Social Change*, 201, 123251–123251.

Yasin, Z. (2023). *Pakistan's Minimal International Participation in Building Cyber Resilience - Centre for Strategic and Contemporary Research*. Centre for Strategic and Contemporary Research.

Younus, A.M. and Najeeb Zaidan, M. (2022). The influence of quantitative research in business & information technology: an appropriate research methodology philosophical reflection. *The influence of quantitative research in business & information technology: an appropriate research methodology philosophical reflection*, 04(May 2022), 61–79.

Zahid, R. (2024). *Cybersecurity Challenges: Safeguarding Pakistan's Digital Infrastructure*. Imarat Institute of Policy Studies – IIPS.

Zhang, J., & Wu, J. (2020). A Discussion on Innovative Techniques for Improving Soil Load-Bearing Capacity. *Journal of Energy and Environmental Policy Options*, *3*(3), 78-85.

Zhao, X., Chen, Q., Yuan, X., Yu, Y. and Zhang, H. (2024). Study on the impact of digital transformation on the innovation potential based on evidence from Chinese listed companies. *Scientific Reports*, 14(1), p.6183.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Çetin, F. and Basım, H.N. (2022). *(PDF) Cyber Security Awareness, Knowledge and Behavior: A Comparative Study*. ResearchGate.