PRESERVING CYBER-SOCIAL WELFARE: AN ASSESSMENT OF POST 2010 CYBERSECURITY LEGISLATION IN PAKISTAN

ومن يؤت الحكمة
فقد أوتي خيرا كثيرا

QUAID-I-AZAM UNIVERSITY

ISLAMABAD

By

Mohammad Iqbal

02192013024

Supervisor

Dr. Ahsan Kamal

PRESERVING CYBER-SOCIAL WELFARE: AN ASSESSMENT OF POST 2010 CYBERSECURITY LEGISLATION IN PAKISTAN

By

Mohammad Iqbal

A thesis submitted to the faculty at the National Institute of Pakistan Studies, Quaid i Azam University, Islamabad in partial fulfilment of the requirements for the degree of Masters in Philosophy

Supervised by: Dr. Ahsan Kamal

National Institute of Pakistan Studies

Quaid-i-Azam University, Islamabad, Pakistan

2023

Author's Declaration

I, Mr. Mohammad Iqbal hereby declare that my research work, i.e., M. Phil thesis titled "**Preserving Cyber-Social welfare: An assessment of Post 2010 Cybersecurity legislation in Pakistan** " is my academic work and has not been prior submitted or published to any institution previously by myself or anyone else for any type of other degree programs from Quaid-i-Azam University, Islamabad, Pakistan. At any time, if a competent authority or department finds anything unethical or against the ethical concerns of the research or thesis, even after the awarding of the degree of M. Phil in Pakistan Studies from Quaid-i-Azam University, Islamabad, has the right to cancel my degree and take some necessary actions against me.

Mohammad Iqbal,

M.Phil. Scholar

National Institute of Pakistan Studies

Quaid-i-Azam University, Islamabad.

Supervisor's Declaration

I, hereby declare that the M. Phil candidate Mohammad Iqbal has completed his Research/thesis Work titled "**Preserving Cyber-Social welfare: An assesment of Post 2010 Cybersecurity legislation in Pakistan**" under my close supervision and my complete guidance on an everyday basis. I recommend this thesis work for submission in the candidacy for the Master of Philosophy in Pakistan Studies, from the National Institute of Pakistan Studies (NIPS), Quaid-i-Azam University, Islamabad, Pakistan. All the content is relevant and followed all the ethical considerations of the research.

Dr. Ahsan Kamal

Assistant Professor

National Institute of Pakistan Studies

Quaid-i-Azam University, Islamabad.

Table of Contents

ABSTRACT 13

Chapter 1. INTRODUCTION 15

1.1 Background of the study 15

1.2 Problem Statement 18

1.3 Research Objectives 19

1.4 Research Questions 19

1.5 Significance of the Study 20

1.6 Scope of the Study 22

1.7 Rationale of the Study 24

1.8 Research Methodology 25

1.8.1 Qualitative Exploration as a Research Design 25

1.8.2 Data Sources and Collection 26

1.8.3 Justification for Collecting Secondary Data 26

1.9 Data Analysis Methods 27

1.10 Ethical Points to Consider 28

1.11 Validity and Contribution 28

Chapter 2. Literature Review 29

2.1 Digital Transformation 29

2.2 Cybersecurity Legislation 30

2.3 Pre-2010 Legislation 30

2.4 Problems with pre-2010 legal system 31

2.5 Post-2010 Legislation 32

2.6 Improvements in Post 2010 Legislation 32

2.7 Evolution of Cybersecurity Legislation Globally 39

2.7.1 Comparative Analysis 39

2.7.2 International Standards and Best Practices 40

2.8 Cybersecurity Landscape in Pakistan 41

2.8.1 Legal Landscape 41

2.8.2 Impact of Cyber Threats 41

2.9 Cybersecurity Legislation and Impact 42

2.9.1 Introduction of Key Laws 42

2.9.2 Effectiveness and Impact 42

2.11 Public Awareness and Capacity Building 43

2.11.1 Government Initiatives 45

2.11.2 Training and Capacity Enhancement 45

2.12 Stakeholder Collaboration and International Cooperation 46

2.12.1 Public-Private Partnerships 46

2.12.2 Bilateral and Multilateral Engagement 47

2.13 Work Carried Out 47

2.13.1 Unexplored Areas 47

2.13.2 Emerging Trends 48

2.14 Gap Analysis 48

2.15 Theoretical Background 50

2.15.1 Cybersecurity Environment and Legislation: 50

2.15.2 Legal Frameworks in Cyberspace: 51

2.15.3 Protecting Societal Well-Being: 51

2.15.4 Implications for National Security: 51

2.16 Theoretical Framework 52

2.16.1 Theory of Legal Pluralism: 52

2.16.2 Technological Determinism: 53

2.16.3 Social Contract Theory: 53

2.16.4 National Security Theory: 53

2.16.5 Policy Diffusion Theory: 54

2.17 Conceptual Framework 54

2.17.1 Conceptualizing Cybersecurity Legislation 55

2.17.2 Legal Approaches to Cyberspace 55

2.17.3 Legal Diversification and Cyberspace Regulation: 57

2.17.4 Legislative Adaptation and Technological Determinism: 57

2.17.5 Legal Framework for Social Contracts and Cybersecurity: 57

2.17.6 National Security and Public Welfare: 58

Chapter 3: An Analysis of Faults and Issues within Legislation of Pakistan Related to Cybersecurity 59

3.1 Introduction 59

3.1.1 Contextualizing Cybersecurity Legislation 59

3.1.2 Significance of Effective Cybersecurity Legislation 60

3.1.3 Implications for Societal Well-being and National Security 60

3.2 Identification of Key Faults and Issues in Pakistani Cybersecurity Legislation 61

3.2.1 Legal Ambiguities and Loopholes in the Prevention of Electronic Crimes Act (PECA) 2016 61

3.2.2 Legal Ambiguities in National Cyber Security Policy 2021 61

3.2.3 Lack of Comprehensive Definitions and Scope Regarding Cybercrimes 62

3.3 Case Studies Illustrating Legislative Shortcomings 62

3.3.1 Case Study: Impact of Inadequate Legislation on the Axact Scandal Involving Fake Degrees 63

3.3.2 Case Study: Data Breaches Affecting Financial Institutions Due to Legislative Gaps 64

3.3.3 Implications and Insights 64

3.4 Comparative Analysis of Legislative Weaknesses 66

3.4.1 Comparison of PECA with International Best Practices like GDPR 67

3.4.2 Comparison of National Cyber Security Policy 2021 with GDPR 69

3.5 Conclusion 72

Chapter 4: The Effect of Issues in Cybersecurity Legislation on Social Welfare of Society 73

4.1 Introduction 73

4.2 Social Welfare Framework in Pakistan 74

4.2.1 Definition of Social Welfare in the Context of Cybersecurity Legislation 74

4.2.2 Discussion of How Legislative Weaknesses Affect Privacy, Economic Stability, and Public Trust in Pakistan 74

4.3 Impact on Individual Privacy and Data Protection 75

4.3.1 Privacy Breaches and Inadequate Data Protection Safeguards Affecting Individuals' Mental Well-being 75

4.3.2 Examination of the Lack of Clear Consent Requirements for Data Processing 76

4.4 Economic Implications of Ineffective Cybersecurity Legislation 77

4.4.1 Cyberattacks on Small Businesses Leading to Economic Instability 77

4.4.2 Analysis of the Absence of Robust Legal Mechanisms for Cyber Insurance and Liability	78
4.5 Impact on Critical Infrastructure and Public Services	78
4.5.1 Evaluation of the Potential Consequences of Legislative Gaps on Essential Services	79
4.5.2 Discussion of the Need for Comprehensive Cybersecurity Standards for Critical Infrastructure	79
4.6 Psychological and Societal Impact	80
4.6.1 Exploration of the Psychological Toll on Individuals due to Cybercrimes and Lack of Legal Redress	80
4.6.2 Analysis of Societal Implications of Inadequate Legislation, Such as Eroded Trust in Digital Services	81
4.7 Conclusion	81
Chapter 5: A Comparison of Pakistan's Cybersecurity Legislature to Global Standards	83
5.1 Introduction	83
5.2 Global Cybersecurity Standards and Benchmarks	83
5.2.1 Overview of International Frameworks and Best Practices	83
5.2.2 Analysis of Key Principles and Provisions	84
5.3 Comparative Analysis with South Asian Nations	85
5.3.1 In-depth Examination of Cybersecurity Legislation in Neighbouring South Asian Countries	85
5.3.2 Identification of Strengths and Weaknesses in Each Country's Legislation and Comparison with Pakistan's Framework	86

5.4 Case Study: India's Cybersecurity Law and Its Impact on Social Welfare 87

5.4.1 Detailed Analysis of India's Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 87

5.4.2 Comparison with Pakistan's Legislation and Assessment of Its Potential Impact on Social Welfare, Individual Rights, and Freedom of Expression 87

5.5 Case Study: European Union's GDPR and Its Implications for Data Protection and Social Welfare 88

5.5.1 Comprehensive Review of the GDPR's Approach to Data Protection and Privacy 88

5.5.2 Comparison of GDPR's Principles with Pakistan's Legislation and Evaluation of Their Effects on Social Welfare and User Rights 89

5.6 Implications of Comparative Analysis for Pakistan 90

5.6.1 Enhancing Societal Well-Being, National Security, and Economic Growth through Global Standards Alignment 90

5.6.2 Exploring Challenges and Benefits of Framework Adoption 91

5.7 Conclusion 92

Chapter 6: Analysing the Threat to National Security and Social Welfare Posed by Gaps in Pakistan's Cybersecurity Legislation 94

6.1 Introduction 94

6.2 National Security Implications of Legislative Gaps 95

6.2.1 Examination of Potential Vulnerabilities Leading to Cyber Threats 95

6.2.2 Analysis of How These Gaps Can Compromise Pakistan's National Security and Subsequently Impact Social Welfare 96

6.3 Societal Impact of National Security Breaches 97

6.3.1 Exploration of Consequences Such as Disruption of Essential Services, Economic Instability, and Public Panic Within Pakistan 97

6.3.2 Discussion of How Compromised National Security Affects Public Trust, Sense of Safety, and Overall Well-being Specifically in Pakistan 97

6.4 Case Study of Operation Arachnophobia: Cyber Espionage and Its National Security and Social Welfare Ramifications in Pakistan 98

6.4.1 Detailed Analysis of Operation Arachnophobia 98

6.4.2 Ramifications on National Security and Social Welfare 99

6.5 Strengthening Legislative Measures for National Security and Social Welfare in Pakistan 99

6.5.1 Improved Threat Detection and Response Mechanisms 99

6.5.2 Role of Public-Private Partnerships 100

6.6 Conclusion 101

Chapter 7: Providing Recommendations for Future Policies Focusing on Social Welfare through Improved Cybersecurity in Pakistan 102

7.1 Introduction 102

7.2 Strengthening Legislative Framework for Social Welfare in Pakistan 102

7.2.1 Comprehensive Legal Revisions: 102

7.2.2 User-Centric Approaches: 104

7.3 Enhancing Public Awareness and Education in Pakistan 106

7.3.1 Nationwide Awareness Campaigns: 106

7.3.2 Cyber Education Integration: 108

7.4 Collaboration and Partnerships in Pakistan 110

7.4.1 Public-Private Partnerships (PPPs): 110

7.4.2 Multilateral Engagement: 111

7.5 Multi-Stakeholder Engagement for Comprehensive Solutions in Pakistan 113

7.5.1 Government Leadership: 113

7.5.2 Industry and Civil Society Participation: 115

7.6 Legislative Reviews and Continuous Adaptation in Pakistan 117

7.6.1 Dynamic Legislative Reviews: 117

7.6.2 Adaptive Approach: Embracing Flexibility in Cybersecurity Legislation to Facilitate Rapid Adaptation: 119

7.7 Conclusion 121

References 122

ABSTRACT

In a world that is becoming increasingly digital, cybersecurity law is critical to protecting both individual rights and national security. This study conducted a thorough evaluation of Pakistan's post-2010 cybersecurity laws, with a particular emphasis on its influence on social welfare. The study recognised the complex relationship between cybersecurity legislation and societal well-being, with the goal of identifying important flaws, problems, and viable remedies within the legal framework. The research began with an examination of the legislative environment, which contextualised the importance of good cybersecurity legislation in protecting societal interests and national security. Legal ambiguities and loopholes in the Prevention of Electronic Crimes Act (PECA) 2016, as well as shortcomings in the National Cyber Security Policy 2021, were examined to identify vulnerabilities exploited by hackers. The study then digs into real-world case studies to demonstrate the effects of legislative flaws on social well-being i.e., the Axact incident and Data hacks etc. This study compared Pakistan's cybersecurity laws to worldwide standards such as the European Union's General Data Protection Regulation (GDPR) using a thorough comparative analysis. The investigation revealed major gaps in data protection, privacy rights, and cross-border cybercrime regulations. These comparative findings highlighted Pakistan's urgent need to align its legislation with worldwide best practises to improve social well-being, national security, and economic prosperity. The study explored how legislative inadequacies might jeopardise Pakistan's security environment before moving on to an examination of national security repercussions thorough case study of "Operation Arachnophobia". The findings of this study add to a better knowledge of the relationship between cybersecurity laws and social welfare in Pakistan, providing policymakers with insights that may be used to improve legislation, cybersecurity measures, and overall societal well-being.

Keywords: Cybersecurity legislation, Social welfare, National security, Legislative gaps, Cyber threats, Data protection, Privacy rights, Prevention of Electronic Crimes Act (PECA), National Cyber Security Policy, (PPP) Public Private Partnerships

Chapter 1: INTRODUCTION

1.1 Background of the study

In today's modern world, the ubiquitous integration of digital technology has revolutionised the way societies function, interact, and do business (Abawajy, 2014). The growing use of digital platforms, online services, and electronic transactions has not only brought ease and efficiency, but it has also exposed individuals, organisations, and governments to a new breed of risks—cyber threats. These dangers include a wide range of criminal behaviours, such as data breaches, identity theft, hacking, and cyber espionage, all of which exploit weaknesses in the digital landscape (Jemal, 2014). As a result, governments all over the world have prioritised the security of essential digital infrastructure and the preservation of individual rights (Ahmad, 2015).

The rise of cyber threats and vulnerabilities has highlighted the importance of strong and adaptable cybersecurity solutions (Jawad, 2015). The potential implications of a successful cyber assault have expanded dramatically as digital technologies have become more deeply integrated in every area of modern life (Seong Oun Hwang, 2015). Cyber assaults not only jeopardise sensitive personal and financial data, but they may also interrupt key services, erode public trust, and stymie economic progress. As a result, the development and execution of comprehensive cybersecurity legislation have become critical to mitigating these dangers and ensuring a nation's residents' social welfare (Arshad Ali, 2015).

The need for comprehensive cybersecurity legislation stems from the reality that current legal frameworks frequently fall behind the quickly expanding cyber threat scenario. Traditional legal procedures do not fully encompass cybercrime or defend a persons' digital rights

(Alahmari, 2020). This void needs the passage of specialised law that addresses the issues caused by internet. Effective cybersecurity legislation not only defines and criminalises cyber offences, but also sets systems for cybercrime investigation, prosecution, and international collaboration (Bob Duncan, 2020).

In this backdrop, the purpose of this research thesis is to evaluate Pakistan's post-2010 cybersecurity laws and its influence on social welfare. This study intends to give insights into the present legislation's strengths and flaws by critically examining the growth of Pakistan's cybersecurity legal framework, its conformity with international norms, and its efficacy in tackling cyber threats. Furthermore, this research will offer light on the function of cybersecurity laws in preserving vital infrastructure, promoting digital privacy, and assuring individuals' access to a secure online environment.

Policymakers, legal experts, and stakeholders can acquire a better grasp of the difficulties and possibilities posed by cybersecurity laws by doing this evaluation. This understanding will be useful in formulating future legislative changes that improve cybersecurity measures, promote the rule of law in cyberspace, and eventually contribute towards Pakistan's higher societal welfare.

Prior to the passage of important cybersecurity laws, Pakistan, like many other countries, faced a plethora of cybersecurity difficulties. The digital world lacked the entire legal and regulatory structure required to effectively fight ever increasing cyber risks. Unauthorised availability, data breaches, and identity theft remained on the rise, underscoring the nation's cyber infrastructure's susceptibility to unscrupulous actors. This period was marked by a lack of legislative instruments and processes to handle the expanding nature of cybercrime, rendering individuals, businesses, and government institutions vulnerable to cyber assaults (Abdulmajeed, 2020).

Following 2010, Pakistan's internet ecosystem saw a tremendous shift. The digital infrastructure was rapidly expanding, with rising expenditures in telecommunications and internet services. The widespread availability of smartphones and low-cost data plans has led to an increase in internet penetration, reaching disconnected portions of the population. This digital revolution brought with it new prospects for growth in the economy, education, and communication, but it also brought with it serious cybersecurity threats (Aldawood, 2018). As more residents got online, cybercriminals' attack surface grew, demanding a robust legal framework to guard against an ever-expanding assortment of dangers (Hussain, 2018).

The expansion of digital connectivity coincided with an increase in cybercrime and incidents. As technology became more integrated into numerous areas, thieves discovered new ways to attack weaknesses. Attacks against financial organisations, government databases, and commercial organisations have increased. Notable occurrences involved data breaches that exposed individuals" critical private information and financial details. These accidents not only resulted in financial losses, but they also weakened public faith in internet businesses. The surge in cybercrime has underlined the need of having appropriate legislative mechanisms in place to combat these threats and protect people' interests (Geoffrey Skinner, 2018).

In response to these difficulties and the evolving cybersecurity world, Pakistan moved to fill holes in its legal framework by enacting cybersecurity laws around 2010. These legislative initiatives seek to improve the country's ability to avoid, react to, and mitigate cyber-attacks. The subsequent parts of this thesis delve into the intricacies of these legislative reforms and their implications for Pakistan's social welfare (Aliyu, 2010).

Cybersecurity legislation is critical in tackling the various difficulties faced by cyber-attacks in the ever expanding digital ecosystem. The importance of such law goes far beyond technical frameworks; it protects national security, individual rights, economic success, and the general well-being of a nation's population. Through numerous essential perspectives, this section digs into the multidimensional relevance of cybersecurity law (Mansur, 2018).

1.2 Problem Statement

The abundance of cyber dangers and vulnerabilities creates unprecedented problems in today's linked society, as digital technologies have become integral to all parts of human existence. The explosion of digital adoption, online transactions, and communication platforms has resulted in unprecedented ease and efficiency. It has, however, exposed individuals, organisations, and governments to a new set of hazards, ranging from data breaches to cyber espionage, all of which have the potential to undermine social well-being (Nahel AO Abdallah, 2018). In this backdrop, Pakistan, like many other countries, has experienced a fast digital revolution since the millennium's beginning. However, this transition has been accompanied by a growth in cyber risks and criminality, necessitating the need for strong cybersecurity laws to protect essential digital infrastructure and individual digital rights. The passage of the Prevention of Electronic Crimes Act (PECA) 2016 and other related laws in Pakistan represented a watershed point in the country's attempts to confront the increasing difficulties of the digital era (Nojeem A. Lasisi, 2018). Despite these legal steps, concerns remain about the effectiveness, comprehensiveness, and compatibility of Pakistan's post-2010 cybersecurity legislation with international norms and the developing cyber threat scenario. Furthermore, the impact of these regulations on social welfare, individual privacy, and building a secure digital environment requires careful consideration (Dahir Diyar, 2018). While research on cybersecurity law has received attention, a full review of the efficacy of post-2010 cybersecurity legislation in ensuring social welfare and tackling Pakistan's growing cyber threat scenario is lacking. Furthermore, unexplored territory must be explored, such as the actual implementation issues encountered by law enforcement organisations and the possible influence of developing technology on the legal system. The current corpus of literature sheds light on the function of cybersecurity laws in changing the digital world. The research gaps identified in this problem statement, on the other hand, emphasise the requirement for an in-depth review of Pakistan's post-2010 cybersecurity legislation's impact on social welfare, alignment with international standards, and effectiveness in mitigating the multifaceted challenges posed by cyber threats.

1.3 Research Objectives

1. To examine the Prevention of Electronic Crimes Act (PECA) 2016 and the National Cyber Security Policy 2021 for legal ambiguities, loopholes, and definition and scope flaws.
2. To analyse the impact of legal flaws on individual privacy, data protection, and mental health.
3. To investigate the larger societal and economic effects of weak cybersecurity laws.
4. To compare Pakistani cybersecurity legislation to foreign norms such as the GDPR and the NIST Cybersecurity Framework.
5. To make policy proposals that will solve legislative gaps and prioritise social well-being.

1.4 Research Questions

1. What are the legal uncertainties, loopholes, and definitional and scope flaws in the Prevention and Enforcement of Electronic Crimes Act (PECA) 2016 and the National Cyber Security Policy 2021? How have these flaws expressed themselves in real-world scenarios?

2. How do the highlighted legal flaws affect individual privacy, data protection, and mental health and how does the lack of explicit permission necessities for data processing contribute to privacy violations?
3. What are the larger societal and economic implications of weak cybersecurity legislation and how do cyberattacks on businesses and vulnerabilities in critical infrastructure protection impair important services and contribute to economic insecurity?
4. What policy proposals may be made to bridge legislative gaps and prioritise societal well-being and how might legislative strengthening, public awareness campaigns, stakeholder collaboration, and mechanisms for continual legislative adaptation improve the efficacy of cybersecurity legislation?

1.5 Significance of the Study

This research has far-reaching consequences for cybersecurity, policy, and social well-being, both in Pakistan and beyond. This study brings useful insights and advantages in numerous critical areas by extensively examining Pakistan's post-2010 cybersecurity laws and its impact on social welfare.

1. Educating Policymakers: The study's results will give policymakers, lawmakers, and government officials a thorough grasp of the shortcomings and ambiguities in current cybersecurity legislation. This understanding is critical for developing evidence-based policy reforms that can improve the efficacy of legal frameworks and so improve societal well-being and national security.

2. Improving Cybersecurity Practises: This study supports stakeholders in prioritising cybersecurity measures by emphasising the practical effects of legislation gaps on individual privacy, data protection, key infrastructure, and economic stability. It helps to design strategies

for better protecting digital infrastructure, preventing cybercrime, and securing online transactions.

3. Increasing Public Awareness: The study's examination of the effects of legislative flaws on individuals' rights and well-being helps to raise public awareness about the significance of cybersecurity. It has the potential to enable users to make better informed decisions about their digital behaviours, resulting in a more secure online environment.

4. Promoting Collaborative Efforts: The study's examination of collaborative efforts inside Pakistan and in comparison, to neighbouring nations emphasises the importance of collaboration between government agencies, corporate sector groups, academia, and civil society. This study emphasises the need of working together to overcome cybersecurity concerns and maintain social well-being.

5. Future Research Guidance: The identification of gaps and issues in existing cybersecurity laws by this study serves as a platform for future research endeavours. It motivates future research into specific areas of legislative reform, worldwide benchmarking, and the changing cybersecurity landscape.

6. Contributing to Global Knowledge: Despite its emphasis on Pakistan, the conclusions of this study hold a chance to contribute to worldwide debates on successful cybersecurity legislation. As nations throughout the world face comparable difficulties, the findings of this study can help to guide international efforts to develop strong legal frameworks that prioritise social well-being.

7. Sustainable Development: Promotion: By emphasising the role of effective legislation in fostering innovation, ensuring access to information, and promoting peaceful and just societies, the study aligns with the Sustainable Development Goals, particularly Goal 9 (Industry, Innovation, and Infrastructure) and Goal 16 (Peace, Justice, and Strong Institutions). Finally,

the value of this study rests in its ability to influence policy changes, improve cybersecurity practises, raise public awareness, stimulate partnerships, direct future studies, improve global knowledge, and promote sustainable development. This study addresses a current need for informed decision-making in the field of cybersecurity and law by conducting a comprehensive assessment of the influence of post-2010 cybersecurity legislation on societal well-being.

1.6 Scope of the Study

This study focuses on a detailed examination of Pakistan's post-2010 cybersecurity laws and its influence on social welfare. The research includes an examination of legal frameworks, their practical ramifications, and their conformity with global standards and best practises. While the study's major focus is on Pakistan, it also contains comparisons with worldwide standards and neighbouring South Asian nations to offer a larger perspective.

The scope of the study includes the following important areas:

1. Analysis of Legislation: The investigation focuses on the Prevention of Electronic Crimes Act (PECA) of 2016 and the National Cyber Security Policy 2021. It investigates the legal provisions, definitions, scope, and objectives specified in these texts for ambiguities, inadequacies, and gaps.

2. Practical Implications: This study looks at how discovered legal flaws affect personal confidentiality, security of information, financial security, and vital infrastructure protection. It looks at case studies that show the real-world effects of these gaps.

3. Global Comparison: The study compares Pakistan's cybersecurity laws to international norms like the General Data Protection Regulation (GDPR) and the National Institute of norms and Technology (NIST) Cybersecurity Framework. It also contains a comparison of cybersecurity legislation in neighbouring South Asian nations.

4. Policy Suggestions: Considering the findings, the paper makes policy suggestions to close legislative gaps and improve social well-being. Legislative changes, public awareness initiatives, partnership methods, and mechanisms for continuing legislative adaptation are all included in these suggestions.

5. Social Impact: The study looks at the larger social impact of legislative gaps, such as the consequences for rights of individuals, public trust, financial security, and access to key services.

6. Considerations for National Security: The research investigates how legislative flaws might jeopardise national security, examining possible weaknesses, cyber threats, and their repercussions on social welfare.

7. Prospects for the Future: The scope includes detecting uncharted territory and developing trends in cybersecurity legislation. This investigates how developing technologies such as artificial intelligence, Internet of Things, and quantum computing may impact future legislation requirements.

It is crucial to highlight that the study does not intend to give legal guidance or policy implementation plans, nor does it provide a deep analysis of the technological components of cybersecurity. The major goal of the study is to give a comprehensive knowledge of the effect of post-2010 cybersecurity laws on social welfare, so encouraging informed debates, policy reforms, and future research initiatives. In summary, the aim of this study is centred on a thorough examination of Pakistan's post-2010 cybersecurity laws and its consequences for social well-being. It includes legal analysis, practical ramifications, worldwide benchmarking, policy suggestions, societal effect, national security issues, and future trends.

1.7 Rationale of the Study

The fast progress of technology in today's linked digital world has revolutionised many facets of modern life. While this transition has resulted in unprecedented ease and efficiency, but has also generated a slew of new concerns, notably in the field of cybersecurity (Ahmed M. Zeki, 2018). Because of our increased reliance on technology, online services, and electronic transactions, there has been an increase in cyber dangers ranging from data breaches and theft of identities to hacking and cyber espionage. These dangers not only jeopardize individual privacy and financial security, but also jeopardise vital infrastructure stability and weaken public trust. The need of comprehensive cybersecurity legislation has grown as governments throughout the world wrestle with the complexity of governing digital environments and protecting their inhabitants' well-being. Pakistan, like many other countries, has recognised the critical need for strong legal structures that handle the particular difficulties brought by cyberspace. The passage of the Prevention of Electronic Crimes Act (PECA) in 2016 and the development of the National Cyber Security Policy 2021 indicate the country's efforts to reduce cyber risks and maintain social well-being. However, the impact of these legal measures in Pakistan is still being investigated. As the digital realm evolves, so do the strategies used by hackers. This ever-changing environment needs a regular evaluation of the sufficiency and applicability of current cybersecurity legislation. While various studies have examined worldwide cybersecurity problems and trends, there is a scarcity of detailed research particularly assessing the impact of post-2010 cybersecurity laws on social welfare in Pakistan (Al-Janabi, 2016).

The idea for this work stems from the crucial need to close this information gap. This project intends to provide significant insights to academics, politicians, legal professionals, and the general public by undertaking a detailed examination of Pakistan's post-2010 cybersecurity laws and assessing its efficacy in defending societal well-being. The key goals of the research are to identify legal gaps, analyse practical ramifications, benchmark against worldwide norms, propose policy suggestions, and investigate larger socioeconomic and national security implications (Samaher, 2018). In addition, the study's focus on Pakistan's legislative environment is consistent with the country's goals for longevity, economic growth, and technological improvement. As Pakistan strives to realise all that is possible of its digital economy and provide a safe online environment for its residents, a detailed grasp of the country's cybersecurity legislation becomes critical (Ibrahim Al-Shourbaji, 2018). Finally, the urgency of fully evaluating the impact of post-2010 cybersecurity laws on societal well-being within Pakistan underscores the motivation for this study. This research intends to contribute not just to the debate on cybersecurity law but also to the larger objective of increasing national security and establishing a resilient digital society by throwing light on legislative shortcomings, social ramifications, and alignment with global norms.

1.8 Research Methodology

This section describes the in-depth research methods used in this study to illustrate the complex connection between Pakistan's cybersecurity legislation and its substantial influence on social well-being. The study employs a qualitative research technique, allowing for a thorough examination of the multiple dynamics inherent in cybersecurity legislation and their far-reaching implications.

1.8.1 Qualitative Exploration as a Research Design

The study strategy used is qualitative exploration, a method well-suited for thoroughly examining the complexity underlying cybersecurity law and its impact on social welfare. This study will use a qualitative methodology to reveal subtle links between legislative flaws and their concrete impacts on societal well-being. This form enables for a detailed examination that catches the subject's nuances and complexities.

1.8.2 Data Sources and Collection

The major source of data for the present research is secondary data, which was carefully vetted from a wide range of credible sources. Government publications, peer-reviewed research papers, legal documents, news pieces, case studies, and internationally recognised cybersecurity standards are among the sources. The use of a range of sources guarantees the data supporting the study is reliable, genuine, and thorough.

1.8.3 Justification for Collecting Secondary Data

Several criteria justify the use of secondary data collection:

- **Information Variety:**

  Secondary data sources provide a wide range of information, enabling the study to include a wide range of perspectives, ideas, and points of view on Pakistan's cybersecurity law and its ramifications.

- **Accessibility:**

  Because secondary data is freely available, the study may draw from a wide range of trustworthy or established sources without any logistical challenges.

- **Extensive Insights:**

  The mix of official publications, research papers, legal papers, headlines, case studies, and global norms provides a comprehensive picture of legislative defects and their societal consequences.

- **Cost and time efficiency:**

  When compared to primary data collecting methods, secondary data collection saves time and money. This allows the research to conduct a thorough analysis without the time-consuming procedure of acquiring original data.

1.9 Data Analysis Methods

To extract significant insights from the acquired secondary data, the study adopts a combined technique of theme analysis and comparison analysis.

- **Thematic Analysis:**

  Thematic analysis is a systematic procedure that identifies, codes, and categorises patterns, trends, and repeating themes in data (Braun & Clarke, 2006). This method is useful in demonstrating the complex linkages between legislative flaws and their repercussions for social well-being.

- **Comparative Evaluation:**

  The study includes a comparative analysis to compare Pakistan's cybersecurity legislation to known international norms and frameworks. This method identifies gaps and their consequences for social well-being. The comparison of Pakistan's legal environment to global standards assists in the identification of areas for development and alignment.

- **Case Study Evaluation**

  To highlight the practical ramifications of legislative gaps, several case studies are painstakingly examined. These real-world examples demonstrate the impact of legislative flaws upon national security & societal wellbeing.

1.10 Ethical Points to Consider

Ethical issues are crucial throughout the study process. To guarantee the ethical use of secondary data, correct citation practises and respect to intellectual property rights are carefully enforced. The study prioritises the integrity and reliability of the research by adhering to ethical criteria.

1.11 Validity and Contribution

The study's importance stems from its contribution to a better understanding of the complex connection between cybersecurity laws and social well-being in Pakistan. The insights gained by analysing legislative gaps and their real-world effects provide policymakers with vital information for strengthening legislation and improving cybersecurity measures. To guarantee study validity and reliability, a transparent and methodical process is used, including data triangulation from many credible sources. This methodological rigour boosts the study's results' trust and believability. Finally, the research approach used in this work consists of a qualitative investigation led by secondary data analysis. The study aims to offer comprehensive knowledge and suggestions for fortifying cybersecurity laws and fostering a haven for the people of Pakistan by scrutinising the impact of Pakistan's cybersecurity legislation in societal well-being through thematic as well as comparative analysis, case studies, and ethical considerations.

Chapter 2: Literature Review

The literature review part examines current research, academic works, and theoretical frameworks that are relevant to the study's focus on cybersecurity law, its efficacy, and its effects on defending social welfare in Pakistan.

2.1 Digital Transformation

Critical industries such as telecommunications, energy, transportation, and healthcare have grown to depend on interconnected networks and data systems as a result of digital transformation (Alkire, 2010). This increased connection has magnified the possible impact of cyber assaults on critical systems, putting national security at risk. Effective cybersecurity law creates measures to protect critical infrastructure from harmful cyber activities, reducing vulnerabilities that might be exploited to disrupt these crucial services (Sabina, 2014). By creating legal frameworks for preventing and mitigating cyber attacks, such legislation adds to a nation's essential infrastructure's resilience in the face of growing cyber hazards.

The collecting, storage, and exchange of personal data has increased dramatically in the digital era. Individuals' online actions create massive volumes of sensitive data, rendering them vulnerable to privacy violations and theft of identities (Maria Emma Santos, 2014). This worry is addressed by cybersecurity law, which establishes legal requirements for data protection, guaranteeing that people' personal information is processed safely and openly. Data protection legislation not only protect individuals' rights, but they also build an atmosphere of trust in digital interactions, promoting increasing online involvement. Economic activity has moved into cyberspace as e-commerce and electronic transactions have grown. The success of electronic commerce, on the other hand, is dependent on the reliability of websites and the safety of money transfers (Jorge Tiago Martins, 2020).

2.2 Cybersecurity Legislation

Cybersecurity legislation establishes the legal framework required for the establishment of secure payment platforms, the prevention of fraud, and the safety and security of financial data. Such law fosters economic growth and customer trust in digital markets by limiting the dangers associated with online transactions (AlMindeel, 2020).

As consumers participate in more online activities, ranging from online communications to accessing services provided by the government, the necessity for a secure digital environment becomes increasingly important. Cybersecurity law helps to achieve this by fighting cyberbullying, online harassment, and other negative acts that jeopardise people's psychological well-being. By discouraging and resolving such behaviour, law fosters an inclusive digital world in which individuals can express themselves and utilise services without fear of repercussions. In conclusion, the importance of cybersecurity legislation extends beyond technological frameworks to include national security, individual privacy, economic activity, and citizens' well-being. By addressing these characteristics, such law contributes significantly to the establishment of a safe and healthy digital society (Raneem, 2020).

2.3 Pre-2010 Legislation

Prior to 2010, there was a profusion of digital technology without a corresponding legal framework to manage the expanding cyber threat situation. This section looks at the legal framework that existed before to 2010, stressing its shortcomings and emphasising the necessity for comprehensive and up-to-date legislation (Zwilling, 2020).

Prior to 2010, Pakistan depended on a hodgepodge of legislation to combat cybercrime, with an emphasis on extending existing legal provisions to include new technology offences. These included fraud, forgery, and defamation statutes that were tailored to cybercrimes on a case-by-case basis. Furthermore, the Pakistan Electronic Crimes Ordinance (PECO) 2007 sought to handle specific cyber offences, but its reach was restricted, and it was not adequately ready to deal with the breadth of cyber risks arising as digital activities expanded rapidly (Hamdullah Nejat Basim, 2020).

2.4 Problems with pre-2010 legal system

When it came to cybercrime, the pre-2010 legal system had major limits. Traditional rules sometimes fell short of addressing cybercriminals' complicated and inventive techniques (Moti, 2020). Furthermore, the lack of defined cybercrime definitions and prohibitions hampered efficient prosecution and investigation of cybercrime offences. Because there are no clear legal processes in place to handle concerns such as hacking, virus distribution, and internet identity theft, victims have little redress (Galit Klien, 2020). Furthermore, a lack of mutual legal aid treaties and protocols hampered international collaboration in cybercrime cases.

The shortcomings of the pre-2010 legal system highlighted the critical need of comprehensive and updated laws geared to the issues faced by cybercrime. Recognising that existing laws were inadequate to meet the complexities of cyber offences, politicians, lawyers, and innovators alike began to urge for a special legal framework that could manage the complexities of cyber offences. Because of the rise of new sorts of crimes and the rising complexity of cyber assaults, proactive and forward-thinking legislation that was able to adjust to changing technology and tactics was required (Dušan Lesjak, 2020).

The escalating cases of cybercrime, which exposed the possible repercussions of leaving the legal environment unattended, increased the desire for comprehensive and current laws. Victims of cybercrime frequently found themselves without enough means to fight for justice or recover damages suffered because of online theft or data breaches in the absence of proper legal procedures. This lack of legal protection eroded confidence in digital interactions or hampered the expansion of digital services and trade (Lukasz Wiechetek, 2020).

2.5 Post-2010 Legislation

Pakistan began its road towards formulating and passing post-2010 cybersecurity laws in response to these weaknesses and the necessity to effectively resist cyber-attacks. The next sections in this research thesis will investigate various legislative changes, their goals, and their influence on ensuring social welfare in cyberspace (Fatih Cetin, 2020).

Following 2010, Pakistan's attitude to cybersecurity changed, as the country saw the need of tackling the rising cyber threat scenario. This section looks at Pakistan's post-2010 cybersecurity legislation, including the adoption of significant laws and regulations, an analysis of their scope and aims, an examination of revisions to existing laws, and a comparison of Pakistan's approach with global norms (Zhang, 2015).

Pakistan went on a path to establish specific laws to address the numerous issues provided by cyber threats in response to the deficiencies of the pre-2010 legal system. The passage of the Prevention of Electronic Crimes Act (PECA) in 2016 was notable among these legislative initiatives. This act sought to handle a broad variety of cyber offences, from unauthorised access to data tampering, as well as cyber harassment to online fraud. The creation of the National Response Centre for Cyber Crimes (NR3C) emphasised the government's commitment to improving the nation's cybersecurity posture (Peiqin, 2015).

2.6 Improvements in Post 2010 Legislation

The passage of important cybersecurity legislation and regulations resulted in a dramatic shift in the legal environment around cybercrime. For example, the PECA 2016 intended to offer a comprehensive framework for combatting cybercrime while balancing individual rights and the necessity for law enforcement. Its goal was to allow effective cybercrime investigation and punishment while protecting digital confidentiality and the right of expression. The Act also created processes for gathering and preserving electronic evidence, which is an important part of cybercrime investigations (Xun Li, 2015).

Pakistan recognised the significance of modifying existing laws to bring them into line with the digital era, in addition to enacting new legislation. The Pakistan Penal Code, for example, has been revised to address rising cybercrimes and strengthen punishments for cybercrime offences. These reforms indicated a proactive approach to law reform and demonstrated the nation's commitment to effectively combating cyber dangers (Stanton, 2005).

Pakistan's cybersecurity legislation enacted after 2010 generated parallels to foreign norms and frameworks. Attempts were made to match the legislative developments of the country with best practises promoted by international organisations including the United Nations and the International Telecommunication Union (ITU) (Jeffrey M., 2015). This alignment sought to assure compliance with global rules and to strengthen international collaboration in combating cybercrime. However, difficulties in combining local cultural, legal, and technical circumstances with international guidelines have surfaced. Finally, the year after 2010 saw a shift in Pakistan's attitude to cybersecurity with the implementation of critical laws. The examination of the scope, aims, changes, and international alignment of these laws sheds light on the country's attempts to combat cyber threats and establish a safe digital environment (Kathryn R. 2015).

Pakistan's post-2010 cybersecurity law was designed to meet a wide range of difficulties posed by the expanding cyber threat scenario. This section discusses the difficulties that the Act attempted to address, such as cybercrime prevention and prosecution, key information infrastructure protection, individual privacy and data protection rights, and international collaboration in addressing cyber threats (Stam, 2015).

One of the primary issues addressed by post-2010 cybersecurity laws was cybercrime prevention and punishment. The Act aims to offer a clear legal framework for classifying different cyber offences as criminal acts, such as hacking, unauthorised access, and data breaches. This made it easier to investigate, prosecute, and punish cybercriminals. Such legislation provided law enforcement authorities with the tools they needed to hold culprits responsible for their conduct in the digital sphere by creating well-defined legal criteria (Paul Mastrangelo, 2015).

The growing dependence on digital technology has also made key information infrastructure more vulnerable to cyber assaults. Recognising the possible repercussions of assaults on systems that enable important services, post-2010 legislation tried to develop critical information infrastructure protection measures. This entailed developing guidelines for protecting critical systems to national security, public safety, and economic stability. The Act reduced the risks connected with assaults on essential infrastructure by mandating security measures for key industries (Jeffrey, 2015).

Concerns about digital privacy and data protection arose as important difficulties as people engaged in online activities. The Act aimed to protect the rights of persons by creating systems for the secure processing of personal data. Organisations were obliged to incorporate privacy safeguards, get informed permission for data acquisition, and maintain data security. The Act created a culture of trust in digital interactions by preserving individuals' personal information and mitigating the dangers of identity theft and unauthorised access (Jolton, 2015).

Because cyber dangers do not respect national borders, worldwide collaboration is essential for effectively combating them. This difficulty was recognised in post-2010 cybersecurity law, which includes provisions for international collaboration. This entailed developing structures for mutual legal aid, extradition, and information exchange across countries. The Act helped to a worldwide effort to address cyber dangers by easing cross-border collaboration in cybercrime investigations and prosecutions. In essence, the cybersecurity concerns addressed by post-2010 legislation were varied and interwoven. The Act sought to address these issues comprehensively, ensuring a more secure and safer internet for individuals, organisations, and the entire country. (Staksrud, 2013)

Pakistan's post-2010 cybersecurity laws attempted to address a variety of digital concerns. This section evaluates the efficacy and implementation of these regulations by assessing their effects, presenting case studies of successful enforcement, and highlighting problems in the implementation or enforcement process (Elisabeth, 2013).

Measuring the efficacy of cybersecurity laws necessitates a thorough examination of its effects on cybercrime prevention, critical infrastructure protection, and the general security of digital exchanges. While the long-term impacts of the legislation are still being determined, early indications indicate that the legislative framework has enhanced awareness of cyber dangers and strengthened collaboration among law enforcement authorities. It has served as a forum for educating the public about internet safety while also encouraging the commercial sector to implement rigorous cybersecurity measures (Kjartan Ólafsson, 2013).

Several case studies shed light on the successful implementation of post-2010 cybersecurity laws. For example, the prosecution of a cybercriminal engaging in financial fraud under the PECA 2016 highlighted the legislation's effectiveness in prosecuting those involved in online criminal activity. Law enforcement agencies worked together to collect digital evidence, which led to the offender's arrest and conviction. Cases involving cyberbullying and blackmail, on the other hand, underlined the significance of law in safeguarding victims' rights and delivering justice in the digital sphere (Sonia Livingstone, 2013).

While post-2010 cybersecurity legislation has showed promise, implementation and enforcement issues exist. The technological sophistication of cybercrime, along with continually developing attack tactics, makes identifying criminals and gathering digital evidence difficult (Świątkowska, 2020). Furthermore, insufficient resources and technological ability in law enforcement authorities might delay cybercrime investigations. The efficacy of the legislation is partly dependent on public knowledge and collaboration, which might be hampered by a lack of digital literacy and comprehension of the legal provisions.

Furthermore, the multinational character of cybercrime creates jurisdictional issues. Cooperation across nations is critical for apprehending cross-border offenders but varied legal standards and variances in national agendas might stymie smooth coordination (Joanna, 2020). Improved international collaboration mechanisms and the creation of standardised processes for cross-border cybercrime investigations are required. Finally, Pakistan's post-2010 cybersecurity law has made great gains in tackling digital concerns. It has showed promise in combating cybercrime, defending essential infrastructure, and preserving the rights of individuals. Effective implementation and enforcement, on the other hand, are continuing endeavours that need constant adaptation to technology improvements and joint efforts among stakeholders (Sawaya, 2017).

Public education and training have emerged as critical components of Pakistan's plan to resist cyber threats in the context of post-2010 cybersecurity laws. This section looks at the responsibilities of government agencies or law enforcement, attempts to educate individuals about cyber hazards and safety precautions, and endeavours to provide training for legal professionals or investigators (Yukiko, 2017).

Government entities and law enforcement agencies play an important role in raising public awareness and establishing ability to combat cyber threats. The creation of the National

Response Centre for Cyber Crimes (NR3C) under the Federal Investigation Agency (FIA) has been critical in coordinating cybercrime-fighting activities (NR3C, 2020). These agencies participate in public promotion, education initiatives, and capacity-building projects to educate individuals about online threats and legal restrictions by using the knowledge of specialist cybercrime teams (International Institute of Strategic Studies, 2021).

Educating individuals about cyber hazards and safety precautions is critical to creating a safe online environment. Following the passage of cybersecurity laws in 2010, public awareness programmes were established to educate citizens about common cyber risks such as phishing, malware, and theft of identities (Mahmood Sharif, 2017). These programmes attempt to provide individuals with the information they need to recognise possible threats and practise proactive safety when participating in online activities. Citizens become more capable to protect themselves against cybercrime by increasing their digital literacy.

The ever-changing nature of cyber threats necessitates on-going training for legal professionals including investigators to successfully enforce cybersecurity legislation. Training programmes have been launched to provide legal experts, law enforcement officials, and cybercrime investigators with the knowledge and abilities needed to traverse complicated digital investigations. These programmes address issues such as digital evidence collecting, regulatory frameworks for cybercrime, and technological awareness of evolving risks. By increasing the competence of these specialists, the country can ensure that cybersecurity law is strictly enforced. To summarise, public knowledge and the development of capacity are critical components of Pakistan's cyber security policy. Government agencies, law enforcement agencies, and other training efforts all work together to make the digital world safer by educating individuals, equipping lawyers, and improving the nation's ability to combat cybercrime successfully (Nicolas Christin, 2017).

Collaboration among stakeholders and international collaboration are essential components of Pakistan's reaction to the expanding cyber threat scenario. This section digs into the collaborations formed by the government, commercial sector, and civil society, as well as bilateral and multinational cybersecurity activities. It also evaluates Pakistan's participation in the global cybersecurity dialogue (Ayumu Kubota, 2017).

Effective cybersecurity necessitates a multifaceted strategy including several parties. Pakistani cybersecurity laws enacted after 2010 recognised the need of including not just the government or law enforcement agencies, but also the corporate sector and civil society organisations. Partnerships between the public and commercial sectors have been critical in sharing experience, resources, and best practises to improve the nation's cybersecurity posture. Civil society organisations help by increasing awareness, campaigning for digital rights, and giving crucial policy insights.

Because cyber dangers are international in nature, bilateral and multilateral actions to solve difficulties collaboratively are required. Pakistan has collaborated on cybersecurity with neighbouring nations and international organisations to exchange information, exchange threat intelligence, and develop collaboration procedures. Bilateral agreements, which include Memorandums of Understanding (MoUs), allow for the exchange of best practises and experiences in combating cyber threats. Participation in global forums and projects, including the Shanghai Cooperation Organization's Regional Anti-Terrorist Structure, helps the nation's coordinated approach to cybersecurity (Akihiro Nakarai, 2017).

Pakistan's participation in the global cybersecurity conversation demonstrates its commitment to combating cyber threats on a global scale. Participation in international dialogues, meetings, and conversations helps the country to keep on top of changing cyber trends and share its experiences with the rest of the world. While problems persist, such as different national agendas and regulatory frameworks, Pakistan's participation in the dialogue demonstrates its desire to contribute positively to the creation of global cybersecurity standards and cooperation. Finally, stakeholder involvement including international cooperation are critical in effectively combating cyber threats. Pakistan's collaborations between the government, business sector, and civil society, as well as its participation in multilateral and bilateral initiatives, indicate the country's commitment to constructing a safe digital landscape while adding to a global cybersecurity conversation (Akira Yamada, 2017).

2.7 Evolution of Cybersecurity Legislation Globally

2.7.1 Comparative Analysis

Countries throughout the world have begun on the difficult task of developing cybersecurity law that resonates with their particular socio-political settings while tackling ever-evolving cyber dangers in the age of digital interconnectedness. A detailed comparative review of cybersecurity laws in many countries gives significant insights into the diversity of legal methods, aims, and the efficacy of these frameworks in combating cyber threats (Muniandy, 2017).

The enormous variation in legal approaches to cybersecurity across nations is a surprising discovery in this comparative investigation. Some countries choose for broad regulatory frameworks that cover a wide range of cyber dangers and digital misbehaviour, while others concentrate on specialised issues such as data protection or cybercrime (Ashraf, 2020). The efficacy of these methods is determined by how well they correspond with the developing nature of cyber risks and the adaptability of legal systems to new problems (Lalitha, 2017).

Furthermore, the goals underpinning cybersecurity laws differ greatly. While some governments prioritise national security, economic growth, and vital infrastructure protection, others place a premium on individual liberties, digital privacy, and the facilitation of safe e-commerce. The success of the law in attaining these goals impacts a country's entire cybersecurity landscape, impacting how residents, corporations, and government agencies traverse the digital realm (Balakrishnan Muniandy, 2017).

2.7.2 International Standards and Best Practices

Because of the advent of transnational cyber threats, joint efforts are required to establish worldwide standards and best practises that will guide the creation of effective cybersecurity laws. The Budapest Convention on Cybercrime is a trailblazing international convention that tries to harmonise legal frameworks for dealing with cyber threats, fostering international collaboration, and safeguarding digital rights (Zarina Samsudin, 2017).

The Council of Europe's Budapest Convention serves as a model for worldwide cybersecurity regulations. It has a significant impact on national legislation since it offers a thorough framework for identifying cybercrime, allowing cross-border investigations, and assuring the protection of individual rights. Countries that have ratified the Convention frequently take inspiration from its provisions, matching their legislation with its principles in order to improve their capacity to resist cyber threats (Or-Meir, 2019).

Aside from the Budapest Convention, numerous international organisations, such as the United Nations and the World Trade Organisation, have helped to define cybersecurity principles. These standards cover a wide variety of topics, including data protection and critical infrastructure security, as well as international collaboration in combating cyber threats. The incorporation of these international standards into national legislation demonstrates a dedication to global cyber stability and an understanding of the linked nature of digital risks (Ori, 2019).

2.8 Cybersecurity Landscape in Pakistan

2.8.1 Legal Landscape

Prior to 2010, the legal framework governing this growing digital domain struggled to tackle the growing variety of cyber threats, owing to the rapid integration of technological advances into Pakistan's socioeconomic fabric a rise in internet access, e-commerce proliferation, as well as technology adoption. An examination of the pre-2010 legal landscape reveals a significant disparity between the complexity of cyber threats and the insufficiency of current legal tools to combat them.

During this time, the existing legal structure was frequently unprepared to deal with growing cybercrimes. Existing laws do not adequately handle cyber activities such as hacking, data breaches, and online fraud. Due to a lack of specialised laws addressing digital offences, law enforcement authorities have struggled to investigate and prosecute cybercriminals. Furthermore, the fast growth of cybercriminal methods and strategies compounded the mismatch that exists between the expanding danger landscape and the available legal responses. As a result, the necessity for a more adaptable, specialised, and forward-thinking legal framework became clear (Nir Nissim, 2019).

2.8.2 Impact of Cyber Threats

The concrete impacts of cyber threats on Pakistan's social well-being are the result of insufficient cybersecurity laws. The related weaknesses became more apparent as the digital environment developed. Data breaches, which are frequently the result of lax data protection policies, have exposed private data, resulting in theft of identities and financial damages for people. Furthermore, companies suffered significant financial losses because of cyberattacks against their digital infrastructure, jeopardising both proprietary data and consumer trust (Yuval Elovici, 2019).

The impact extends beyond financial ramifications to include invasions of confidentiality that impinge on individual liberties. Unauthorised monitoring, unauthorised access to private data, and online information manipulation all raise doubt upon electronic rights to privacy. Furthermore, cyber-attacks on essential infrastructure, including power grids and communication networks, endanger public safety or national security. These real-world effects highlight the critical need for comprehensive and adaptive legal frameworks capable of tackling the diverse issues faced by developing cyber threats (Lior Rokach, 2019).

2.9 Cybersecurity Legislation and Impact

2.9.1 Introduction of Key Laws

The implementation of the Prevention of Electronic Crimes Act (PECA) 2016 along with other pertinent legislation in Pakistan after 2010 constituted a watershed moment in the legal landscape of cybersecurity. These legislative efforts aimed to meet the new complexity of the digital era as well as the changing nature of cyber threats (Parsons, 2014). The passage of the PECA and associated legislation was an important step towards aligning Pakistan's legal structure with modern cybersecurity problems.

PECA, 2016 sought to handle a wide spectrum of cybercrimes, such cyber harassment, unauthorised access to data systems, and electronic fraud, in a comprehensive manner. Other relevant laws, such as the National Response Centre for Cyber Crimes Act (NR3C) as well as the Payment Systems and Electronic Fund Transfers Act, in addition to PECA, have contributed to the development of a legal ecosystem beneficial to safeguarding digital rights, fostering e-commerce, as well as deterring cybercriminal activities (Kathryn, 2014).

2.9.2 Effectiveness and Impact

Pakistan's post-2010 cybersecurity law has had a diverse influence on the cybersecurity scene, covering cybercrime prevention, critical infrastructure protection, and individual digital rights guarantee. These legislative measures tried to address cybercriminals' ever-evolving techniques, and their influence on Pakistan's digital society may be seen in numerous ways (Agata McCormac, 2014).

To begin with, the implementation of the PECA and associated regulations considerably improved the country's capabilities to combat cybercrime. The legislative framework gave law enforcement agencies with broad tools for effectively investigating, prosecuting, and deterring cybercriminals. The deterrence impact of the legislation is seen in an increase in reported instances and subsequent convictions, demonstrating an enhanced process for dealing with digital wrongdoing (Marcus Butavicius, 2014).

Furthermore, the provisions of the legislation addressing the protection of key information infrastructure have strengthened the nation's cybersecurity posture. The capacity to protect critical systems and networks is critical for ensuring public safety, national security, and the ongoing delivery of crucial services. Post-2010 legislation has helped to Pakistan's digital resilience by addressing vulnerabilities in this arena.

Finally, the Act has helped to promote the cause for individual digital rights by safeguarding privacy, freedom of speech, and safe online transactions. Citizens now have more confidence in navigating the digital world while holding online service providers liable for safeguarding information and user confidentiality (Malcolm Pattinson, 2014).

The implementation of the Prevention of Electronic Crimes Act (PECA) 2016 and other pertinent legislation in Pakistan after 2010 constituted a watershed moment in the legal landscape of cybersecurity. These legislative efforts aimed to meet the new complexity of the digital era as well as the changing nature the cyber threats (Cate Jerram, 2014). The passage of the PECA and associated legislation was an important step towards aligning Pakistan's legal structure with modern cybersecurity problems.

PECA, 2016 sought to handle a wide spectrum of cybercrimes, such cyber harassment, unauthorised access to data systems, and online fraud, in a comprehensive manner. Other relevant laws, such as the National Response Centre for Cyber Crimes Act (NR3C) and the Payment Systems and Electronic Fund Transfers Act, in addition to PECA, have contributed to the development of a legal ecosystem conducive to safeguarding digital rights, fostering online shopping, and deterring cybercriminal activities (Malik, 2020).

Pakistan's post-2010 cybersecurity law has had a diverse influence on the cybersecurity scene, covering cybercrime prevention, critical infrastructure protection, and individual digital rights guarantee. These legislative measures tried to address cybercriminals' ever-evolving techniques, and their influence on Pakistan's digital society may be seen in numerous ways.

To begin with, the implementation of the PECA and associated regulations considerably improved the country's capabilities to combat cybercrime (Fareesa, 2020). The legislative framework gave law enforcement agencies with broad tools for effectively investigating, prosecuting, and deterring cybercriminals. The deterrence impact of the legislation is seen in an increase in reported instances and subsequent convictions, demonstrating an enhanced process for dealing with digital wrongdoing.

Furthermore, the provisions of the legislation addressing the protection of key information infrastructure have strengthened the country's cybersecurity posture. The capacity to protect critical systems and networks is critical for ensuring public safety, national security, and the ongoing delivery of crucial services. Post-2010 legislation has helped to Pakistan's digital resilience by addressing vulnerabilities in this arena (Richard Heeks, 2020).

Finally, the Act has helped to promote the advancement of individual digital rights by safeguarding privacy, freedom of speech, and secure online transactions. Citizens now have more confidence in navigating the digital world while holding online service providers accountable for safeguarding information and user confidentiality (Silvia Masiero, 2020).

2.11 Public Awareness and Capacity Building

2.11.1 Government Initiatives

Recognising the vital role of encouraging a cyber-literate populace and guaranteeing the successful execution of cybersecurity laws, Pakistan's government has launched significant efforts to inform citizens regarding cyber risks, encourage digital literacy, and improve consciousness regarding cybersecurity laws. These programmes include a variety of tactics geared at equipping people with the information they need to navigate the digital realm safely and ethically (Brian Nicholson, 2020).

Campaigns to educate individuals on the possible hazards associated with online activity, as well as best practises for safeguarding personal information and preventing cyber-attacks, are among the government's initiatives. Citizens are informed about their digital rights and obligations, as well as the channels available to seek redress in cases of cybercrime or digital rights abuses, through awareness programmes, workshops, and online resources (McCormac, 2017).

2.11.2 Training and Capacity Enhancement

Along with public awareness campaigns, Pakistan has made gains in improving the ability of legal experts, police agencies, and cybersecurity specialists to confront cyber risks effectively. Training programmes are aimed to provide those involved with the abilities and knowledge required to respond to cybercriminals' shifting methods and the complexities of cyber law enforcement.

Specialised training familiarises legal practitioners with the subtleties of cybersecurity law and its use in legal procedures. This equips them to comprehend complicated cybercrime situations and ensure that justice is delivered in an ever-changing digital context. Similarly, law enforcement agencies acquire extensive training in order to investigate cybercrimes successfully, gather digital evidence, and coordinate with other institutions in the pursuit of cybercriminals (Agata, 2017).

Cybersecurity specialists are critical to ensuring the integrity of digital infrastructure. Training programmes that seek to improve their abilities in areas such as threat identification, handling incidents, and ethical hacking help to strengthen the nation's cyber resilience. Furthermore, cybersecurity professional capacity-building programmes establish a culture of cooperation and coordination among many stakeholders in the battle against cyber threats (Tara Zwaans, 2020).

2.12 Stakeholder Collaboration and International Cooperation

2.12.1 Public-Private Partnerships

Recognising the complex and interwoven nature of cyber risks has prompted cooperation efforts in Pakistan among the government, corporate sector organisations, and civil society organisations. These collaborations strive to enhance cybersecurity measures jointly by using the experience, resources, and viewpoints of many stakeholders.

PPPs have evolved as a critical tool for information exchange, threat reduction, and collaborative efforts in addressing cyber threats. Private sector entities with domain-specific expertise and resources partner with government agencies to improve cyber attack detection and response capabilities. Civil society organisations contribute to cybersecurity awareness campaigns, policy creation, and lobbying initiatives, guaranteeing an integrated approach to cybersecurity which is appealing to the general public (Malcolm Pattinson, 2017).

2.12.2 Bilateral and Multilateral Engagement

In an era where cyber dangers cross national borders, worldwide collaboration is required to successfully combat them. Pakistan's participation in bilateral and international initiatives for sharing data, threat intelligence, or cybersecurity cooperation is critical to improving the country's cyber resilience (Kathryn Parsons, 2017).

Bilateral agreements enable Pakistan and its foreign partners to exchange information and knowledge. These treaties promote cooperation and collaboration, allowing for collaborative efforts to tackle transnational cyber threats. Furthermore, engagement in multilateral projects, conferences, and organisations helps Pakistan to participate in the global cybersecurity debate, shape international standards, and exchange best practises (Dragana Calic, 2017).

2.13 Work Carried Out

2.13.1 Unexplored Areas

Despite the expanding volume of study on cybersecurity laws in Pakistan, there are still a number of undiscovered topics that require additional exploration. The assessment of the real implementation and enforcement problems encountered by law enforcement authorities and the judiciary is one key gap. Investigating how legal requirements are converted into successful activities and analysing the roadblocks encountered may give useful insights into improving the cybersecurity legal framework (Marcus Butavicius, 2017).

Furthermore, there is a scarcity of research on the impact of public awareness campaigns in Pakistan (Livingstone, 2014.). While the government's attempts to educate residents about cyber hazards are admirable, the efficacy of these measures on increasing cybersecurity awareness and lowering vulnerabilities is unknown. Understanding the processes of knowledge distribution and behaviour modification can help to improve awareness campaigns.

2.13.2 Emerging Trends

Emerging changes in the technical landscape have the potential to profoundly affect the future of cybersecurity law in Pakistan. Artificial intelligence (AI), the Internet of Things (IoT), or quantum computing have all introduced new dimensions to cyber risks and issues . Because of the networked nature of IoT devices and the processing capability of quantum computing, current legal frameworks must be reevaluated in order to meet fresh risks (Sonia, 2017).

Furthermore, the incorporation of AI in cyber attack strategies emphasises the significance of AI ethics and responsibility in cybersecurity policy. The possibility of AI-powered assaults raises concerns regarding attribution, culpability, and the use of legal frameworks to combat AI-driven cybercrime (Lucyna Kirwil, 2017).

2.14 Gap Analysis

The current study aims to fill particular gaps in the existing scholarship and information about Pakistan's post-2010 cybersecurity laws and its influence on social welfare. A thorough examination indicates various areas where gaps exist, necessitating the necessity for this research:

- Limited Concentration on Legislative Impact: While there is literature outlining cybersecurity concerns in Pakistan, there is a striking lack of thorough research especially analysing the impact of post-2010 cybersecurity laws on social well-being. Existing research frequently focuses on technological elements or generic cyber dangers rather than the effectiveness of legislative measures in safeguarding people' rights and boosting social welfare.
- Lack of Comparative Analysis: Despite studies that compare cybersecurity laws in Pakistan to worldwide norms, there is a dearth of extensive comparative analysis

particular to Pakistan. Few studies have been conducted to examine how Pakistan's legal framework relates to worldwide standards such as GDPR or how it relates to cybersecurity laws in neighbouring South Asian nations. This absence creates a major knowledge gap about the country's legislation strengths and shortcomings in a larger perspective.

- Lack of Practical consequences: In the present research, the practical consequences of legislative deficiencies on individual privacy, financial stability, vital infrastructure protection, or national security were not extensively studied. While legal analyses exist, they frequently fail to link legislative gaps to real-world implications or to provide in-depth case studies demonstrating the impact of these gaps on social well-being.
- Lack of Policy proposals: Despite talks regarding legislative issues, thorough policy proposals relevant to Pakistan's circumstances are lacking. The literature lacks concrete ideas for closing legislative gaps, raising public awareness, promoting partnerships, and ensuring that law is constantly adapted to emerging cyber risks.
- Inadequate National Security Assessment: While there has been debate about the larger implications of cybersecurity for national security, there has been little investigation into how particular legislation flaws may jeopardise Pakistan's national security. Few studies investigate possible vulnerabilities, dangers, and their repercussions on social welfare, which is critical for comprehending the larger implications of legislative loopholes.
- Changing Technological Trends: New cyber risks have emerged as a result of rapid technical breakthroughs such as artificial intelligence, IoT, and quantum computing. The present research frequently fails to investigate how emerging patterns may worsen existing legislative gaps or demand new legal measures to meet unique concerns.

This study tries to fill these gaps by undertaking a thorough examination of the impact of post-2010 cybersecurity laws on social welfare in Pakistan. By filling these gaps, the research contributes to a more comprehensive knowledge of the legal landscape, practical ramifications, alignment with global standards, and prospective policy improvement routes. This research not only addresses gaps in the current literature, but it also gives significant insights to guide policy decisions, create partnerships, and help to the overall improvement of cybersecurity laws and social well-being.

2.15Theoretical Background

This study's theoretical framework is based on numerous essential principles from the disciplines of cybersecurity, law, and social welfare. These ideas establish the groundwork for comprehending the complicated interaction of legislative initiatives, technical breakthroughs, and their effects on social well-being.

2.15.1 Cybersecurity Environment and Legislation:

The idea of cybersecurity, which means the protection of digital networks, information, and systems against cyber-attacks, is central to this research. Cristina Ponte, and Elisabeth Staksrud (2019) underline the rising susceptibility of organisations and individuals to cyber dangers, emphasising the necessity for strong regulatory frameworks to combat cybercrime and protect digital environments. The cybersecurity environment is defined by an ever-changing set of threats, including as hacking, phishing, malware, and data breaches, all of which exploit weaknesses in digital systems. Effective cybersecurity legislation is critical for combating these threats because it defines offences, develops legal channels for prosecution, and sets a framework for collaboration among government departments, law enforcement agencies, and other stakeholders (Meade, 2012).

2.15.2 Legal Frameworks in Cyberspace:

The paper focuses on legal paradigms applied to cyberspace, emphasising the difficulties in translating traditional legal notions to the digital environment. Because of the changing nature of cyber threats, specialised legislation that tackles the particular difficulties of cyberspace is required. Traditional legal doctrines, which are frequently built for physical areas, may struggle to account for the intricacies of cybercrime, digital rights, especially cross-border jurisdiction (Adam W., 2012). A comparison of legal methods across jurisdictions, in addition to international frameworks such as the Budapest Convention on Cybercrime, indicates the necessity for legislation that strikes a balance between the requirements of safety, confidentiality, and individual rights (S. Bartholomew Craig, 2012).

2.15.3 Protecting Societal Well-Being:

The influence of cybersecurity laws on societal well-being is a significant prism using which this study analyses it. Individual privacy, financial security, availability of essential amenities, and public trust are some of the characteristics of social well-being. Legislation is critical in ensuring that these aspects are safeguarded in the digital era. The study investigates the relationship between legal loopholes and their implications for people's mental well-being as a result of confidentiality breaches or economic instability produced by cyberattacks on firms (Anderson, 2019). Furthermore, the lack of comprehensive critical infrastructure cybersecurity standards may jeopardise public trust and access to key services such as healthcare or transportation (Ross, 2019).

2.15.4 Implications for National Security:

Incorporating national security issues, the study assesses how legislative loopholes might jeopardise a country's security and, as a result, social well-being. Cybercriminals might use possible weaknesses in legal frameworks to launch attacks on essential infrastructure, resulting in service interruptions or financial turmoil (Chris Barton, 2019). The Operation Arachnophobia case study demonstrates that cyber espionage targeting classified government data can have far-reaching effects on national security, diplomatic efforts, and social well-being (Rainer Bölme, 2019).

Finally, the theoretical foundation of this work is based on cybersecurity principles, legislative paradigms, and societal well-being factors. The study seeks to provide an in-depth comprehension of how post-2010 cybersecurity laws in Pakistan connects in technological advancements, legislative difficulties, and their impact on individual liberties, economic stability, availability of services, and national security by synthesising these concepts. This multidisciplinary approach directs the investigation of legislative efficacy, practical ramifications, and policy suggestions in the context of the welfare of society.

2.16Theoretical Framework

This study's theoretical framework is based on numerous major principles from the disciplines of law, cybersecurity, including social well-being. These notions serve as the foundation for a thorough examination of the impact of post-2010 cybersecurity laws on social welfare in Pakistan.

2.16.1 Theory of Legal Pluralism:

The notion of legal pluralism emphasises the persistence of many legal systems and norms inside a community, impacting human behaviours or interactions (Fitzpatrick, 1983). This theory assists in comprehending the delicate interplay among global frameworks, regional rules, and national laws in the setting of cybersecurity legislation. It directs the examination of how Pakistan's cybersecurity law complies with international norms such as GDPR or the NIST

Cybersecurity Framework, exposing the intricate relationships between various legal systems in governing the digital realm (Berti, 2019).

2.16.2 Technological Determinism:

According to Winner (1986), technical improvements induce societal shifts. This theory emphasises the importance of legislative adaptation in the setting of cybersecurity laws to handle growing cyber threats and dynamic technological developments. The study employs technological determinism to investigate how laws must evolve in order to address new issues brought by technologies such as AI, IoT, and quantum computers. This approach sheds light on the importance of legislative actions that are in sync with the continuously changing technology context (Castells, 1996).

2.16.3 Social Contract Theory:

The social contract theory investigates the implicit contract between people and the state in which individuals give up some liberties in return for safety and security (Rousseau, 1762). This social compact extends to the protection of digital rights or privacy in the digital era. This theory informs the study's consideration of how legislative loopholes jeopardise people' digital rights and security, hence affecting citizens' faith in the state. The research looks at how successful cybersecurity legislation helps to the preservation of the digital social agreement and the welfare of society (Nissenbaum, 2004).

2.16.4 National Security Theory:

The goal of national security theory is to protect a country's interests, sovereignty, and population against numerous dangers (Buzan et al., 1998). This idea is critical for understanding the consequences of legislative gaps for national security in the larger picture of cybersecurity legislation. The research focuses on national security theory to highlight the relationship between laws and the general well-being of the nation by analysing whether cyber threats leverage legislative flaws to undermine vital infrastructure or disrupt services (Libicki, 2009).

2.16.5 Policy Diffusion Theory:

Policy diffusion theory investigates the transmission of policies across jurisdictions as well as the impact of external variables on policy acceptance and adaptation (Walker, 1969). This theory assists in clarifying how international guidelines and best practises impact national law in the context of cybersecurity legislation. The paper uses policy diffusion theory to examine how global norms such as the Budapest Convention on Cybercrime have affected Pakistan's legislative initiatives. It investigates how incorporating effective aspects from other jurisdictions might improve social well-being (Bartsch & Hommelhoff, 2016).

These connected ideas form a solid foundation for analysing the impact of post-2010 cybersecurity laws on social welfare in Pakistan. This study adds to our understanding of legal effectiveness, practical consequences, and policy suggestions in the dynamic context of security and societal well-being by incorporating knowledge from pluralism in law, technological destiny, social contracts, national security, as well as policy diffusion.

2.17 Conceptual Framework

The theoretical framework driving this study mixes themes from the fields of law, cybersecurity, with societal well-being to investigate the influence of post-2010 cybersecurity laws on Pakistan's social welfare. This framework combines fundamental theoretical viewpoints to investigate the complex relationships between legislative measures and technology breakthroughs, as well as the consequences for individual rights, financial stability, utilisation of offerings, and national security.

2.17.1 Conceptualizing Cybersecurity Legislation

The convergence of technology and society in the digital era has created new opportunities and difficulties. Cyber risks have arisen as a major issue among these concerns, needing thorough remedies. Cybersecurity law plays a critical role in combating these dangers, involving complex interplay between legal, ethical, or technological concerns.

The construction of legal frameworks and laws controlling digital behaviour, online transactions, including the protection modern digital assets is at the heart of cybersecurity legislation. It extends beyond conventional regulatory measures to serve as a critical instrument in combating a wide range of cyber threats, from cybercrime and records breaches through cyber espionage and data warfare. This legislation plays an important role in developing a secure and resilient digital ecosystem, protecting key infrastructure, including ensuring the preservation of individual rights in cyberspace (Ahmad et al., 2019; Cavusoglu et al., 2004).

The core of conceptualising cybersecurity law is striking a careful balance between security imperatives and individual rights protection. These legal frameworks aim to achieve a compromise between combating cyber dangers and protecting principles like digital privacy, free speech, and due process. This balance is especially important in Pakistan's unique setting, where social welfare is inextricably tied to both increased security and citizen empowerment in the age of technology (Richard Clayton, 2019).

2.17.2 Legal Approaches to Cyberspace

The digital world has upended traditional legal paradigms, necessitating a re-evaluation of existing legal principles inside the boundaries of cyberspace. Legal experts and practitioners are wrestling with the difficulty of applying time-honoured legal ideas to the fast-changing digital environment. The separation of the virtual and real worlds has sparked disputes regarding the applicability of current laws and the need for specialised legislation geared to the complex difficulties of cyberspace.

Traditional legal principles such as jurisdiction, proof, and due process take on new dimensions in the digital realm. The global nature of internet blurs territorial boundaries, complicating the determination of jurisdiction in cybercrime proceedings. Furthermore, the transient and dynamic character of digital evidence raises questions about its preservation or admissibility in judicial procedures. These complexities highlight the critical need of matching legal standards with the subtleties of the digital ecosystem (Carlos Ganán, 2019).

This shift in legal thinking has sparked proposals for specialised cybersecurity laws designed to meet the complexities of cyber threats. Traditional rules, although providing a framework, may fall short of adequately tackling the varied variety of cybercrimes or digital wrongdoings. As a result, the establishment of specialised cyberspace laws becomes critical to appropriately handle emerging cyber risks and sustain the applicability of legal concepts in an increasingly digitised society.

The necessity for specialised cybersecurity laws in Pakistan is exacerbated by the rapid digitalization of numerous sectors. As the country embraces digital transformation, it must deal with both the benefits and risks that this paradigm change presents. As a result, legal academics and policymakers are grappling with the numerous issues of reconciling legal standards with the complexities of the digital realm (Tom Grasso, 2019).

2.17.3 Legal Diversification and Cyberspace Regulation:

The paper examines the complicated landscape of cybersecurity law from the standpoint of legal pluralism. Legal pluralism acknowledges the coexistence and interaction of several legal systems, standards, and actors within a community. This viewpoint underlines the coexistence of numerous international frameworks, state rules, and technology standards in the context of cyberspace. Through this theoretical lens, we may examine how Pakistan's legislative actions match with global norms such as GDPR, the NIST Cybersecurity Framework, and regional cybersecurity rules. The study investigates how different legal systems create and affect cybersecurity legislation, resulting in a more sophisticated understanding of legislative efficacy and practical ramifications (Michael Levi, 2019).

2.17.4 Legislative Adaptation and Technological Determinism:

The theoretical framework also includes aspects of technological determinism, which holds that technical advances cause societal changes. In the context of cybersecurity law, technological determinism emphasizes the importance of legislative adaptation in order to keep up with increasing cyber threats. Because of the fast advancement of technology, rules that can handle innovative concerns such as AI-driven cyberattacks, IoT weaknesses, and quantum computing dangers are required. This viewpoint informs the study's examination of developing trends and their implications for Pakistan-specific legislative reforms (Tyler Moore, 2019).

2.17.5 Legal Framework for Social Contracts and Cybersecurity:

The notion of the social contract, which forms the connection between the state and its citizens, has been incorporated within the theoretical framework. This contract, in the digital era, includes the safeguarding of digital rights, confidentiality, and security. The research looks at how legal loopholes affect the social compact by jeopardizing individuals' digital rights or security. It also addresses cybersecurity legislation's role in preserving public trust, financial security, and access to key services. The research adds to a thorough knowledge of the broader social impact of legislative initiatives by examining the legal framework's conformity with people' expectations (Marie Vasek, 2019).

2.17.6 National Security and Public Welfare:

National security is an important component of the conceptual structure, emphasising the interconnectedness between legislative shortcomings and possible risks to community well-being. The report examines the repercussions of legal loopholes against national security, such as cyberattacks on key infrastructure. This viewpoint emphasizes the significance of cybersecurity laws in maintaining economic stability, public confidence, and access to key services. The study offers insight on the larger implications for social well-being by analysing the link between legislative flaws and national security risks. In summary, the theoretical approach incorporates legal pluralism, technological dominance, the social compact, and national security considerations to assess the impact of post-2010 cybersecurity laws on social welfare in Pakistan. This multidisciplinary approach allows for a thorough examination of legislative efficacy, practical ramifications, and policy suggestions in the context of a dynamic digital ecosystem (Crossler, 2013).

Chapter 3: An Analysis of Faults and Issues within Legislation of Pakistan Related to Cybersecurity

3.1 Introduction

This chapter begins the study journey by critically examining Pakistan's cybersecurity laws and their consequences for social well-being or national security. The rising digitalization of all aspects of life has highlighted the importance of strong cybersecurity measures. Effective cyber law acts as a critical defence against a plethora of cyber dangers who have a chance to disrupt national stability, damage sensitive information, and impair the general welfare of the public (Robert E., 2013).

3.1.1 Contextualizing Cybersecurity Legislation

The dependence on interconnected systems, e-commerce, and internet services has risen to new heights in an era characterised by digital revolution. This digital environment has provided countless benefits and conveniences, yet it additionally exposes individuals, organisations, and government agencies to a growing number of cyber risks. Cyber dangers include a wide range of criminal behaviours that exploit weaknesses in digital environments, including data breaches, theft of identities, and cyber espionage. As a result, the necessity to maintain key digital infrastructure while also protecting individual rights has arisen as a significant priority for governments throughout the world (Allen C. 2013).

3.1.2 Significance of Effective Cybersecurity Legislation

Effective cybersecurity law is critical to safeguarding society's stability and well-being in the face of growing cyber threats. It creates a legal framework which defines appropriate cyber behaviour detects, and categorises cybercrimes, and imposes penalties on violators. Aside from legal ramifications, strong cybersecurity law acts as a disincentive, deterring potential hackers from participating in illegal actions. Furthermore, it promotes a safe digital environment, which boosts public trust, increases economic growth, and allows for more efficient government (Johnston, 2013).

3.1.3 Implications for Societal Well-being and National Security

Effective cybersecurity law has consequences that go beyond private safety to include social well-being or national security. Critical systems such as medical care, electricity distribution, and banking networks can all be affected by cyber-attacks, possibly causing significant chaos and anguish. Inadequate cybersecurity safeguards can also weaken public faith in digital services, resulting in decreased trust in political institutions and general social stability. National security is additionally at stake because cyber assaults can jeopardise diplomatic relations or strategic objectives. In deduction, this chapter serves as an introduction, emphasising the important significance of comprehensive cybersecurity legislation in safeguarding social well-being and national security. The next portions of this research dig into the examination of specific flaws and their practical repercussions within Pakistan's legal environment by comprehending the relevance of cybersecurity regulations (Paul Benjamin Lowry, 2013)

3.2 Identification of Key Faults and Issues in Pakistani Cybersecurity Legislation

This section digs into a thorough examination of the various flaws and vulnerabilities of Pakistan's cybersecurity legislation. We hope to discover ambiguities, flaws, and inadequacies in the legal framework that govern cyber activities in order to improve its efficacy in tackling growing cyber risks and maintaining social well-being and national security (Hu. 2013).

3.2.1 Legal Ambiguities and Loopholes in the Prevention of Electronic Crimes Act (PECA) 2016

The Prevention of Electronic Crimes Act (PECA) of 2016 is an important step towards regulating cyber activity and combating cybercrime in Pakistan. Nonetheless, despite its good intentions, PECA has been criticised for having legal ambiguities and loopholes that make implementation and enforcement difficult. Ambiguities in essential terms, such as "unlawful online content" or "cyberstalking," have caused uncertainty among legal practitioners, law enforcement agencies, and court authorities, hindering efficient prosecution. Furthermore, the lack of clear criteria on jurisdiction or extraterritorial applicability has hindered cross-border cybercrime and international agency collaboration. The absence of strong safeguards for the safeguarding of digital evidence and the chain of custody jeopardises the integrity of investigations (Qing, 2013).

3.2.2 Legal Ambiguities in National Cyber Security Policy 2021

The National Cyber Security Policy 2021 attempts to improve Pakistan's cybersecurity posture by laying out policies, goals, and action plans. Even this policy paper, however, is not exempt to legal issues that might undermine its efficacy. Ambiguities emerge in areas such as the demarcation of duties and responsibilities amongst government agencies, the methods for information exchange and coordination, and the simplicity of private sector firms' obligations in preserving key information infrastructure. These uncertainties can cause misunderstanding, overlap, and gaps when confronting cyber threats, jeopardising the objective of improving national cybersecurity (Baitenizov, 2019).

3.2.3 Lack of Comprehensive Definitions and Scope Regarding Cybercrimes

The absence of broad definitions and scope for cybercrime is one of the core difficulties in Pakistani cybersecurity legislation. The lack of precise and standardised categories for cyber offences makes effectively categorising and prosecuting various types of cybercrime difficult. This ambiguity can result in conflicting legal interpretations, variable degrees of punishment, and poor clarity between legal practitioners as the public. As a result of the lack of well-defined legal rules, prospective cybercriminals may exploit these loopholes, avoiding prosecution or earning light fines (Daniyar T., 2019). In summary, this section addresses important flaws and difficulties in Pakistani cybersecurity legislation, with a special emphasis on ambiguities, loopholes, and gaps in the Prevention of Electronic Crimes Act (PECA) 2016 and the National Cyber Security Policy 2021. These shortcomings highlight the need a critical review and necessary revisions to the legislative framework to ensure that it effectively confronts the growing panorama of cyber risks while protecting the welfare of society and national security.

3.3 Case Studies Illustrating Legislative Shortcomings

This section goes into the practical ramifications of Pakistan's cybersecurity framework's reported legislative flaws. We hope to explain how these flaws and concerns have developed in specific scenarios, affecting both national security and social well-being, by exploring real-world case studies.

3.3.1 Case Study: Impact of Inadequate Legislation on the Axact Scandal Involving Fake Degrees

The Axact incident is a vivid and worrisome illustration of how legal gaps in Pakistan's cybersecurity system may be ruthlessly used to orchestrate intricate and far-reaching cybercrimes, bringing severe effects in their aftermath (Global cyber security index, 2022). This case study provides a compelling narrative that delves into the Axact scandal, revealing the degree to which legislative flaws enabled the growth of a massive diploma mill functioning that given counterfeit credentials and degrees to unsuspecting individuals all over the world

The scandal's many facets highlight the complexities of the cybercriminal ecosystem and the sophisticated web of deceit that emerged (Igor N. 2019). The Axact scandal was centred on an extensive network that functioned on the edge of legality, exploiting shortcomings in the current legal system. A crack in Pakistan's cybersecurity law was the lack of comprehensive and well-defined categories for cyber offences such as online money laundering, fraud, and identity theft (Dubina, 2019). These legal uncertainties not only provided a fertile breeding environment for cybercriminals, but also hampered law enforcement organisations in their pursuit of justice. The sheer scope and endurance of the Axact affair can be linked to flaws in the regulatory framework. Due to the lack of special regulations in place to handle the unique issues provided by online diploma mills, the criminals were able to carry out their fraudulent activities with impunity. This conspicuous breach in the law allowed criminals to take advantage of the absence of consequences appropriate to the seriousness of their acts. As a result, victims suffered significant financial losses, with ramifications that extended beyond individual misery. Furthermore, the Axact affair had far-reaching consequences that went beyond financial losses. The disclosure of a so sophisticated cybercrime operation has harmed Pakistan's standing on the world stage. The scandal gained international attention and cast doubt on Pakistan's educational institutions' trustworthiness. This loss of confidence not only harmed respectable institutions' reputations, but also led to a culture of scepticism around the legitimacy of educational credentials originating in Pakistan. The Axact affair, in essence, serves as a cautionary tale that starkly shows the disastrous effects of legislative loopholes and inconsistencies in Pakistan's cybersecurity legislation (David FJ. 2019). The case study delves into a complicated network of fraudulent actions, demonstrating how hackers exploited the lack of detailed definitions and punishments to carry out their deceptive operations on a worldwide scale. The resulting financial losses and reputational harm highlight the critical need for a strong legislative framework capable of successfully combating cybercrime while protecting both national security and social well-being. The findings of this case study feed the analysis in the next sections, emphasising the need of fixing legislative flaws to prevent such events and guarantee Pakistan has a safe digital environment (Campbell, 2019).

3.3.2 Case Study: Data Breaches Affecting Financial Institutions Due to Legislative Gaps

A troubling pattern develops within Pakistan's complicated cybersecurity tapestry as data breaches affecting financial institutions comes to the fore. This case study reveals a frightening reality in which cybercriminals have openly breached the defences of financial institutions, revealing critical consumer data and wreaking havoc upon national security and public confidence (Elias G. 2019). This tale provides a thorough assessment of the linked variables that drive data breaches, emphasising how regulatory loopholes serve as catalysts for these concerning instances.

The banking sector, sometimes referred to as an economy's lifeblood, has an invaluable library of private and financial data, making it an appealing target for hackers. The allure of valuable information that includes credit card numbers to transaction history attracts hackers looking for financial gain and the exploitation of private data. In the middle of this digital war, the shortcomings in Pakistan's cybersecurity legislation became clear, allowing bad actors to exploit legislative vulnerabilities (Carayannis, 2019).

As data breaches dominate the news, legal loopholes serve as major vulnerabilities that allow hackers to exploit the banking sector's flaws. The lack of a thorough legal framework, along with ambiguous definitions of cyber offences, makes it easier to breach financial institutions' defences (Azatbek, 2019). Because of these legal flaws, fraudsters may easily detect and exploit weaknesses, circumvent security measures, and get unauthorised access to client accounts and transaction records. In sum, the legislative environment unintentionally assists hackers (Tolkyn A., 2019).

One of the most concerning features of legislative flaws is how they exacerbate the repercussions of data breaches. The lack of adequate measures for data breach notifications and responsibility frameworks puts impacted persons and institutions in jeopardy (Cain, 2018). The absence of clear legal remedy for victim of data breaches exacerbates the harm done, as impacted parties are forced to deal with the fallout without a clear way to seek vengeance.

Furthermore, the societal ramifications of data breaches are immeasurable. The deterioration of public faith in financial institutions reverberates throughout society, generating an atmosphere of anxiety and worry. Individuals become increasingly hesitant of making digital transactions and revealing personal information while financial institutions battle to secure sensitive data owing to regulatory inadequacies, stifling economic development and digital transformation (Ashley A., 2018). Finally, the case investigation into data breaches affecting financial institutions inside Pakistan's cybersecurity ecosystem illuminates the serious ramifications of regulatory inadequacies. The vulnerability of the financial industry to cyberattacks highlights the critical need for a strong legal framework that not just deters cybercriminals but additionally protects sensitive data, national security, or public confidence. This case study highlights the importance of resolving legislative flaws and motivates a comprehensive approach towards cybersecurity legislation that protects the durability for Pakistan's financial ecosystem for the well-being of its population.

3.3.3 Implications and Insights

The case studies offered highlight the practical consequences of legislative flaws on both national security and social well-being. The Axact incident demonstrated how legal uncertainties may empower cybercriminals to carry out their activities with relative impunity, harming not just the economy but also educational institutions' credibility. Similarly, data breaches aimed at financial organisations raise the prospect of losses in money, compromised private data, and a loss of public faith in digital financial services (Morgan E. 2018). These case studies act as cautionary stories, highlighting the critical importance of resolving legislative inadequacies in order to prevent future tragedies and preserve Pakistan's digital ecosystem. In conclusion, this part digs into individual case studies to provide light on the real-world effects of legislative flaws in Pakistan's cybersecurity legislation (D. Still, 2018). We show how flaws in the legal framework may give rise to severe national security vulnerabilities or jeopardise social well-being by exploring the Axact incident and data breaches impacting financial institutions. These case studies give useful insights that influence the evaluation and recommendations for an additional robust cybersecurity legislative framework in the next sections.

3.4 Comparative Analysis of Legislative Weaknesses

When compared to foreign best practises, the panorama of legal flaws inside Pakistan's cybersecurity system becomes even more obvious. This section conducts a thorough examination of legislative gaps by contrasting major parts of Pakistan's cybersecurity laws with the acclaimed European Union's General Data Protection Regulation (GDPR), which serves as a global standard for data protection and privacy rules. The flaws of Pakistan's legal structure are highlighted via this comparative perspective, providing insights into the critical need for improvements to ensure societal well-being and security (Pakistan Observer, 2022).

3.4.1 Comparison of PECA with International Best Practices like GDPR

The Prevention of Electronic Crimes Act (PECA) of 2016, a critical component of Pakistan's cybersecurity architecture, is nestled inside the core of the country's legal landscape (Jeremiah, 2018). While PECA is a significant step forward in combating cybercrime and digital offences, a thorough comparative analysis sheds light on its inherent flaws when measured against international standards of excellence, most notably the European Union's General Data Protection Regulation (GDPR) (Hina, 2019). The GDPR's resounding reputation as the gold standard in data protection and privacy rules emphasises the flaws in PECA, necessitating a critical examination of its provisions and their influence on Pakistan's social well-being and national security (Edwards, 2018).

The GDPR, lauded for its consistent commitment to protecting personal data privacy as well as private liberties, serves as a solid standard against which PECA's boundaries are clearly defined. This comparative examination highlights a number of inequalities, each of which calls for improvements to Pakistan's legislative framework. The principle of safeguarding information is central to this contrast, and it highlights PECA's shortcomings in critical areas wherein the GDPR shines (Sadaf, 2018).

While the GDPR prioritises user permission and the concept of data minimization, the PECA falls short by failing to create clear and comprehensive regulations in these areas (Paul Benjamin Lowry, 2018). This omission reveals a critical flaw in PECA's capacity to safeguard personal data privacy and security. The GDPR's rigorous emphasis on user permission guarantees that identifiable information is only handled with the data subject's explicit authorization, giving people more control over their digital identities. In contrast, PECA's ambiguity in specifying such criteria limits its ability to provide comparable safeguards.

Another fundamental discrepancy emerges in the sphere of data breach punishments, putting doubt on PECA's deterrence potential. The GDPR's consistent application of significant fines for data breaches acts as a powerful disincentive to lax security practises. This punitive approach serves not just as a financial penalty, but also as a clear signal that data security is a non-negotiable objective. In sharp contrast, experts believe that PECA's punitive provisions lack the teeth to deter hackers, emphasising the importance of expanding the legal arsenal (Dhanapal Durai Dominic Panneer Selvam, 2018).

This comparative examination has repercussions that go beyond mere legal language to the very heart of Pakistan's societal well-being. The gap between PECA and GDPR highlights the need to strengthen legislative measures and link them more closely with worldwide best practises. Individual data privacy protection, digital rights promotion, and the imposition of harsh punishments for infractions all merge as key components in the goal of social well-being and national security (Gratian, 2018). This comparative examination lays the groundwork for more in-depth investigations into the practical consequences of these legislative inadequacies, developing a call for action that resonates to the wider goals of good cybersecurity legislation. In conclusion, the comparison of PECA and GDPR serves as a clarion cry for reform in Pakistan's cybersecurity ecosystem. As the country grapples with the harsh realities of the digital era, our research strengthens the argument for legislative change that reflects worldwide best practises, assuring not just legal alignment yet social well-being during ever-evolving cyber dangers (Margaret, 2018).

3.4.2 Comparison of National Cyber Security Policy 2021 with GDPR

The National Cyber Security Policy of 2021, a plan aimed to steer the country's path towards digital resilience, has been incorporated within Pakistan's strategic strategy for cybersecurity. When compared to the European Union's colossal General Data Protection Regulation (GDPR), an interesting comparative study sheds new light on the policy's merits and weaknesses. This investigation into the relationship between these two crucial texts reveals a complex view on the processes that defend individual rights in the digital sphere, leading an evaluation of the consequences for Pakistan's social well-being or national security (Sruthi Bandi, 2018).

The GDPR's constant commitment to protecting individuals' rights over their personal data is at the heart of this comparison. The GDPR's emphasis on specific rights is notable, with the ability to be remembered and the right to obtain personal data prominently included (Article 17 & 15, GDPR) (Michel Cukier, 2018). The GDPR's careful definition of these rights allows individuals to assert authority over the digital footprints they leave behind, creating an environment in which data subjects have the capacity to create their online identities. This is in stark contrast to the approach of the National Cyber Security Policy 2021, which, while acknowledging the critical importance for data protection, fails to offer a comprehensive set of rights and mechanisms that enable individuals to wield comparable control over their personal information (Josiah Dykstra, 2018).

The GDPR's trademark phrase, "right to be forgotten" exemplifies the data autonomy concept at its foundation. This notion, which allows individuals to seek the deletion of their private information, symbolises the GDPR's commitment to giving individuals some degree of control of their digital presence. When assessed against such stringent requirements, the National Cyber Security Policy 2021's comparative absence of stated rights in this sphere becomes clear.

The policy's lack of a solid method for exercising the "right to be forgotten" may limit individuals' capacity to disassociate themselves from online surroundings, limiting their agency in constructing their digital narratives (Amy Ginther, 2018).

Similarly, the GDPR's "right to access personal data" strengthens individuals' control over their data. This right gives individuals access to the data that organisations have on file about them, ensuring transparency and responsibility in the data processing (Kim, 2019). While cutting the groundwork for data protection, the National Cyber Security Policy 2021 does not clearly establish analogous rights for people to access and handle their own personal information, which could eventually impact the granularity of authority that individuals have over their digital identities (Hyungjin Lukas, 2019).

The ramifications resulting from this compared exploration extend above the realms of policy writing to the core of Pakistan's dedication to societal well-being. This comparison illuminates the potential opportunity for harmonising the National Cyber Security Policy 2021 with the GDPR's commitment to person empowerment and data protection. The creation of broad rights and methods can provide a strong defence against cyber dangers while also protecting individuals' rights in the digital era (HanByeol, 2019). This investigation catalyses the reflection needed to guarantee that Pakistan's national cyber policies align with global norms and prioritise the peaceful coexistence of digital growth and individual rights. In conclusion, a comparison of the National Cyber Security Policy 2021 and the GDPR highlights the significance of strengthening the former's provisions to reflect the full rights provided in the latter. This research highlights the road towards a cybersecurity framework that bolsters both social well-being and national security, driven by a dedication to individual data protection and empowerment as Pakistan charts its future in the digital era (Stella, 2019).

Furthermore, the GDPR's focus on cross-border data transfers, as well as its rigorous standards for securing data privacy in such transfers, highlight a critical gap in Pakistan's cybersecurity legislation: the lack of specific measures for cross-border criminality. Article 44-49 of the GDPR requires transfers of data to nations outside the EU to follow specified procedures to ensure data protection. The lack of such measures in Pakistan's legislative framework exposes the country to transnational cybercrime and highlights the need for a broader approach to combating cross-border cyber threats (Choi, and Jinyoung Han, 2019). In summary, a comparative examination of legislative flaws in Pakistan's cybersecurity system reveals the shortcomings that impede the country's development for effective cyber regulation. The gaps shown by comparisons to international standard practices such as the GDPR highlight the importance of change. This analysis, by identifying regions where Pakistan's legislation collapses short, provides a foundation for subsequent chapters' investigation of the implications of these flaws on societal well-being as well as national security, clearing the way for an additional solid and comprehensive legislative approach.

3.5 Conclusion

The voyage through Pakistan's complicated ecosystem of cybersecurity legislation has revealed a tapestry woven with serious flaws and legal holes. This chapter has thoroughly analysed the legislative framework's underbelly, identifying fundamental flaws and challenges that undermine its efficacy. The framework's flaws have been highlighted, ranging from legal uncertainties to a lack of detailed definitions and scope for criminality.

The legal uncertainties and loopholes in the Prevention of Electronic Crimes Act (PECA) 2016 were investigated, demonstrating how cybercriminals have used the legislation's flaws for their own advantage. While the National Cyber Security Policy 2021 serves as a light for Pakistan's digital future, it still requires strengthening in several areas to enable robust data security and individual empowerment.

Furthermore, actual-life instances, such as the Axact affair and data breaches impacting financial institutions, have highlighted the real-world ramifications of legal deficiencies. These case studies have demonstrated the practical consequences of insufficient legislation on both national security and societal wellbeing.

As we go into Chapter 2, the emphasis will change from finding flaws in the legal framework to comprehending how these flaws resonate across the socioeconomic fabric. The implications of these legal concerns for individual confidentiality, economic stability, essential infrastructure, and social well-being will be thoroughly examined. The link among legislation and its real-world repercussions will become clearer, presenting a complete picture of the delicate interaction between cybersecurity laws and Pakistan's residents' wellbeing.

Chapter 4: The Effect of Issues in Cybersecurity Legislation on Social Welfare of Society

4.1 Introduction

As the attention falls upon the cybersecurity legislation flaws and concerns shown in the preceding chapter, another attention dawns on the enormous ramifications these flaws have on society. The complexities of legislative provisions, which were formerly restricted to legal texts, have now spread their far-reaching tentacles, tangling with the fundamental core of social welfare or individual rights. This chapter begins on a transformative journey that goes beyond legislative complexities, diving into the visceral consequences of these concerns on Pakistan's societal well-being.

The introduction to this chapter serves as a link between the legislative concerns exhaustively studied and their ripple effects on the fabric of society. In this setting, the critical importance of comprehensive cybersecurity law takes centre stage, as its role in fostering social well-being and protecting individual rights becomes clearer. In a linked digital world, where individual, financial, and social transactions take place in cyberspace, the vulnerability of legal protections and their potential impact on collective welfare cannot be overstated.

Thus, this chapter lays up the canvas for the interaction between legislative failures and societal wellbeing. The connections between these seemingly different areas will be weaved into a tapestry which not only illustrates the repercussions of faulty cybersecurity laws, but also emphasises the need for reform. This chapter goes deeper into the fields where these challenges are most evident, unravelling their multiple consequences on confidentiality, economic stability, essential infrastructure, including the mental health of people inside society with each successive part. The investigation is united by a common undercurrent: the recognition that the digital domain is closely tied to the larger socioeconomic fabric, and that protecting this sector demands a comprehensive strategy that balances legal foundations with social advantages.

4.2 Social Welfare Framework in Pakistan

4.2.1 Definition of Social Welfare in the Context of Cybersecurity Legislation

The concept of social welfare, generally defined as a society's collective health and standard of life, is the foundation of societal growth and harmony (Kortjan, 2022). The notion of social welfare grows into the digital sphere in the context of cybersecurity laws, covering the preservation of individuals' digital rights, confidentiality, economic stability, and general sense of security. It expresses the notion that a society empowered by technology is one in which people can connect, communicate, and trade online with confidence, knowing that their financial and personal data is safe from cyber dangers.

The word "social welfare" has a multifaceted meaning in the context of cybersecurity law. It is intertwined with data protection principles, technological liberties, and ethical concerns, reflecting a larger social desire for a safe, trustworthy, or resilient digital environment. Within this domain, the idea of social welfare reflects the underlying tenet of the well-being of people and society at large is inextricably linked to the safety and quality of online interactions and transactions (Noluxolo, 2022).

4.2.2 Discussion of How Legislative Weaknesses Affect Privacy, Economic Stability, and Public Trust in Pakistan

The flaws in Pakistan's cybersecurity legislation throw a shadow across the entire range of social welfare issues. Individual dignity and liberty are jeopardised by statutory uncertainties that fail to provide strong safeguards against data breaches, unauthorised monitoring, and identity theft. Individuals are vulnerable to the exploitation of their private information due to a lack of rigorous data protection measures, weakening their feeling of authority and control in the digital domain (Rossouw von Solms, 2022).

A robust digital ecosystem that enables safe e-commerce, money transfers, and company operations underpins economic stability, a pillar of societal growth. However, inadequacies in regulatory frameworks allow cybercriminals to exploit weaknesses inside essential sectors, resulting in financial losses, problems, and economic destabilisation. The lack of strict measures for holding cybercriminals responsible exposes organisations and people to financial risks, weakening trust in online transactions (Muronga,. 2019).

When legal shortcomings fail to create a sufficient barrier against cyber-attacks, public trust, a critical component of coherent society interactions, is destroyed. Citizens' faith in digital services, communication via the internet, and the overall trustworthiness of the digital landscape are declining as cybercrime and breach instances increase. The lack of clear legal consequences and insufficient disincentive measures lead to an atmosphere of ambiguity, which reduces the public's desire to engage in digital activities and use online services (Khangwelo, 2019).

4.3 Impact on Individual Privacy and Data Protection

4.3.1 Privacy Breaches and Inadequate Data Protection Safeguards Affecting Individuals' Mental Well-being

Individual privacy and data protection are at the heart of a thriving digital society. However, the existence of legal flaws puts a cloud on these fundamental rights, affecting individuals' mental health in a variety of ways. Individuals are exposed to a persistent sense of vulnerability as a result of privacy breaches caused by legislative uncertainties and loopholes. Unauthorised data access, communication, or sale can cause emotions of violation and discomfort, undermining the psychological comfort that people should feel in their digital contacts (Marlein, 2019).

Furthermore, the psychological cost of privacy violations persists beyond the initial anguish. Individuals' desire to engage with online activities, including social media conversations to e-commerce transactions, is hampered by the residual dread of potential exploitation of personal data. Uncertainty over the security of personal information in the digital world adds to increased worry and stress, affecting individuals' mental well-being and lowering overall quality of life (Herselman, 2019).

4.3.2 Examination of the Lack of Clear Consent Requirements for Data Processing

The notion of informed permission is a foundation of data protection, allowing individuals to come to informed decisions regarding the dissemination of their private data. However, regulatory limitations impede the implementation of this principle in the digital realm. Individuals are at the mercy of ambiguous privacy rules and unregulated data gathering practises in the absence of explicit and strict criteria for getting user permission for data processing (Adele Botha, 2019).

Inadequate permission methods worsen the power imbalance between individuals as well as data collectors, frequently resulting in instances in which users unintentionally provide personal information. Lack of transparency regarding how data is used or shared reduces people' ownership of their digital footprint, heightening privacy and autonomy issues. This degradation of user agency not only undermines the protection of individual rights, but also leads to a general environment of mistrust within the digital ecosystem as a whole (Adéle Da Veiga, 2019).

4.4 Economic Implications of Ineffective Cybersecurity Legislation

Any country's economic environment is inextricably linked to its technical infrastructure or digital transactions. The prevalence of flaws and weaknesses in cybersecurity legislation reverberates across the economy, leading to a wide range of economic consequences. This section examines the financial consequences of weak cybersecurity legislation, with an emphasis on cyberattacks on small enterprises and the lack of robust legal structures for cyber protection and liability (Anwar, 2017).

4.4.1 Cyberattacks on Small Businesses Leading to Economic Instability

Small companies are the foundation of many economies, greatly contributing to job creation and general economic growth. These businesses, however, frequently lack the solid cybersecurity systems and assets that bigger firms have, making them easy targets for fraudsters. Legislative flaws play a critical role in increasing this vulnerability, allowing hackers to easily exploit security flaws and conduct cyberattacks (Mohd, 2017).

Small business cyberattacks have far-reaching economic consequences. Direct financial losses caused as a result of data breaches, attacks by ransomware, or intellectual property theft can be disastrous for small firms, resulting in bankruptcy or liquidation (Wu., 2017). Furthermore, the economic impact is exacerbated by indirect expenses such as reputational harm, legal bills, and prospective litigation. This problem has repercussions across the economy, since small firm closures affect employment rates, spending by consumers, and general economic stability (S He, Ivan Ash, Xiaohong Yuan, Ling Li, and Xu. Li. 2017).

4.4.2 Analysis of the Absence of Robust Legal Mechanisms for Cyber Insurance and Liability

In today's digital environment, the possibility of cyber events is a harsh reality that organisations must face. Cyber insurance has developed as an important instrument for controlling the financial consequences of cyberattacks, acting as a safety net for the significant expenses connected with data breaches as well as other cyber catastrophes. However, legislative inadequacies make effective cyber insurance implementation difficult.

In the lack of comprehensive legal frameworks for cyber insurance and liability, ambiguity enters the picture. Without clear legal guidance, businesses may struggle to effectively analyse their cybersecurity risks and select adequate coverage (Solic, 2019). Furthermore, a lack of standardisation and legal precedent within this field may complicate the claims procedure, making it difficult for firms to recover costs following a cyber event.

The economic consequences of insufficient cyber insurance and accountability systems go beyond individual enterprises. The lack of clear criteria stifles the expansion of the cyber insurance market, restricting its ability to offer a safety net for enterprises and compromising economic resiliency. As a result, general economic stability suffers as firms and industries are exposed to unnecessary financial risks (Kresimir, 2019).

4.5 Impact on Critical Infrastructure and Public Services

The backbone of modern civilizations is critical infrastructure, which includes sectors such as electricity, medical care, public transit, and communication. These industries' operations are inextricably linked to digital networks, making them great candidates for cyberattacks. In the setting of insufficient cybersecurity laws, vulnerabilities in key public services and infrastructure magnify the potential effects, hurting not just the economy but additionally residents' well-being and safety (Mateo Plesa, 2019).

4.5.1 Evaluation of the Potential Consequences of Legislative Gaps on Essential Services

Critical public facilities and amenities are vulnerable to cyber assaults due to their reliance on digital technologies. Legislative loopholes amplify this risk, allowing cybercriminals to exploit flaws and disrupt critical services. For example, healthcare institutions hold sensitive patient information and utilise digital technology for patient treatment and record administration. A cyberattack on hospital infrastructure can jeopardise patient privacy, impair medical services, and put patients' lives in jeopardy (Tena Velki, 2019).

Digital controls are also significantly used in transportation networks for operations and security systems. A cyberattack on transport networks disrupts traffic management, jeopardizing road safety or potentially leading to accidents (Nenadic, 2019). Such interruptions risk lives while also eroding public faith in the government's capacity to provide crucial services (Kresimir, 2019).

4.5.2 Discussion of the Need for Comprehensive Cybersecurity Standards for Critical Infrastructure

The weaknesses in key infrastructure highlight the importance of strong cybersecurity standards. While legal frameworks lay the groundwork for cybersecurity, standards give comprehensive rules that organisations in vital industries can follow. These standards address a wide range of cybersecurity topics, including risk assessment or threat mitigation, as well as incident recovery and response procedures.

Comprehensive standards for cybersecurity provide critical infrastructure organisations with an unambiguous route for assessing vulnerabilities and implementing appropriate measures. They also allow for collaboration across many industries and governmental entities, resulting in a cohesive strategy towards cybersecurity (National Institute of Standards and Technology, 2018). By complying to such standards, vital infrastructure sectors may strengthen their resilience to cyber attacks, reduce potential effects, and protect the well-being of populations who rely on these crucial services.

4.6 Psychological and Societal Impact

Cybercrime, aided by legal flaws, has consequences that go beyond financial losses and operational interruptions. The psychological and sociological consequences of insufficient cybersecurity legislation highlight the complex link between legal frameworks, human well-being, and society trust.

4.6.1 Exploration of the Psychological Toll on Individuals due to Cybercrimes and Lack of Legal Redress

A cybercrime's consequences can cause severe psychological pain in its victims. Individuals may experience feelings of infraction, powerlessness, and fear as a result of personal data breaches, theft of identities, and online abuse (Lallie, 2020). Furthermore, victims' suffering might be compounded when they believe there is little legal procedure to resolve their problems. Inadequate legal provisions might cause victims to lose faith in the court system's ability to offer remedies or justice, leaving them to deal with their trauma or worry about the future.

The lack of meaningful legal remedy not only fails to relieve victims' suffering, but it can also foster a sense of invincibility among cyber criminals. When people believe that cybercriminals may act with impunity because of lax regulation, public faith in the capacity of the legal system to protect citizens or deter criminals erodes (Harjinder Singh, 2020). This lack of confidence can lead to disappointment and deter people from participating in digital activities, stifling social and economic progress that is dependent on the digital ecosystem.

4.6.2 Analysis of Societal Implications of Inadequate Legislation, Such as Eroded Trust in Digital Services

The engagement of society with digital services and platforms is built on trust. Inadequate cybersecurity laws can erode confidence, resulting in a cascade of societal consequences. Individuals may be hesitant to conduct online transactions, reveal personal information, or use digital services due to worries about data security and an absence of legal protection (Lynsay A. Shepherd, Jason RC Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens, 2020). Furthermore, the deterioration of confidence in digital services may impede the expansion of the online economy. Public trust for the security or confidentiality of digital interactions is essential for e-commerce, electronic banking, and digital government.

When legal gaps are exploited, resulting in data breaches or theft of identities, individuals may choose less convenient yet perceived safer alternatives, limiting digital economy growth and lowering economic development potential (Kruger et al., 2015).

4.7 Conclusion

This chapter examined the far-reaching consequences of legislative flaws in Pakistan's cybersecurity architecture on social well-being. The investigation uncovered a multifaceted impact ranging from individual privacy concerns to a loss of public faith in digital services. The psychological toll of cybercrime victims, worsened by a lack of legal remedy, emphasises the importance of strong legal mechanisms to address their concerns. Furthermore, the social repercussions of lower faith in digital platforms might stymie economic growth, stymie digital innovation, and stymie digital economy development.

The interaction between legislative shortcomings and societal well-being sets the foundation for a further inquiry of the vulnerabilities presented by these gaps to national security. The following chapter will shed illumination on the wider significance of legislative issues through looking at Pakistan's legislation via a global lens and comparisons it against international norms, thereby contributing to an in-depth comprehension of the intricate connection between cybersecurity regulations and societal welfare.

Chapter 5: A Comparison of Pakistan's Cybersecurity Legislature to Global Standards

5.1 Introduction

As the digital world crosses national boundaries, it becomes increasingly important to connect cybersecurity legislation with international standards. This chapter takes a comparative approach, contrasting Pakistan's cybersecurity legislation with worldwide standards. The significance of this benchmarking study rests in its ability to identify gaps, highlight best practises, and give a comprehensive view of Pakistan's legal framework's progress in the global context.

Because of the interconnection of today's digital world, a unified strategy to cybersecurity is required, where nations may learn from each other's achievements and failures. This chapter lays the groundwork for a complete review by drawing on worldwide standards, practises, and experiences. We hope that this comparative research will shed light on areas wherein Pakistan's legislation may be strengthened, ensuring that cybersecurity regulations are in line with worldwide best practises and, as a result, improving social well-being or national security.

5.2 Global Cybersecurity Standards and Benchmarks

5.2.1 Overview of International Frameworks and Best Practices

International standards and best practises serve as guiding lights in the ever-changing field of cybersecurity, giving comprehensive ways to mitigating cyber risks. The NIST Cybersecurity Framework and ISO 27001 are two notable standards that serve as pillars of worldwide cybersecurity guidelines (Alsunbul, 2015)

The NIST Cybersecurity Framework, designed by the United States' National Institute of Standards and Technology, provides a systematic method to managing cybersecurity risk. This methodology, which consists of five important tasks - Protection, Detection, Response, and Recover - assists organisations in identifying assets, analysing weaknesses, developing safeguards, discovering breaches, reacting effectively, and recovering quickly. It provides a comprehensive blueprint for cyber resilience, improving the security stance of organizations across several industries (Saad, 2015).

The ISO 27001 standard, on the other hand, focuses on management systems for information security. It describes a strategy for establishing, implementing, maintaining, and continuously improving a company's data safety management system. ISO 27001 places a premium on risk assessment, risk management, and the installation of controls to mitigate identified risks. This standard is well recognised for emphasising the protection of sensitive information assets (Phu Dung Le, 2015).

5.2.2 Analysis of Key Principles and Provisions

When these foreign frameworks are compared to Pakistan's cybersecurity law, several essential concepts and regulations are either lacking or underrepresented within the latter. The NIST Cybersecurity Framework, for example, emphasises the significance of ongoing surveillance and flexible responses to new threats. These proactive aspects go beyond simple compliance to address the changing nature of cyber dangers (Jefferson Tan, 2015).

Similarly, the focus on a risk-based strategy and continuous improvement in ISO 27001 emphasises the necessity for safeguards that are not static but change in tandem with the growing threat landscape. The lack of clear provisions in Pakistan's legislation for such adaptive measures may restrict its effectiveness in addressing future difficulties.

This research highlights significant shortcomings in Pakistan's cybersecurity law, emphasising the importance of matching its principles with worldwide best practises. As the global community implements comprehensive tactics to fight against cyber dangers, this chapter aims to stimulate discussion about incorporating such concepts into Pakistan's legal framework in order to improve the country's capabilities to protect societal well-being and national security (Beerepoot, 2015).

5.3 Comparative Analysis with South Asian Nations

5.3.1 In-depth Examination of Cybersecurity Legislation in Neighbouring South Asian Countries

The digital revolution has brought with it a new era of connectedness, creativity, and, sadly, cyber risks. Recognising that these concerns transcend geopolitical borders, it's now critical to examine legislative frameworks aiming at tackling these issues from a regional viewpoint. This section begins a tour of the cybersecurity legislation of surrounding South Asian nations, with the goal of uncovering common tendencies, striking discrepancies, and fertile ground for prospective reforms. This chapter attempts to provide a comprehensive view of how different governments are addressing cybersecurity by casting a broader net and researching the legislative measures of countries within proximity (Niels, 2015).

India, Bangladesh, Sri Lanka, and Afghanistan are among the nations chosen for this comparative study. This eclectic variety was carefully chosen to provide a broad range of legislative approaches. By examining these various tactics, the chapter hopes to draw significant insights that will assist in the development of more effective cybersecurity laws (Bart Lambregts, 2015).

India, a regional powerhouse with a rising technology landscape, is an especially attractive subject for comparison. The Information Technology Act of 2000, strengthened by substantial changes in 2008, is the cornerstone of India's cybersecurity law (Ministry of Electronics and Information Technology, Government of India, 2020). This landmark piece of law not only targets cybercrime, but also includes requirements for digital signatures and information protection. This Act, as a testament of its comprehensiveness, serves as a model for cybersecurity regimes throughout the area.

5.3.2 Identification of Strengths and Weaknesses in Each Country's Legislation and Comparison with Pakistan's Framework

This section delves into a thorough comparative examination of cybersecurity laws in order to uncover the strengths and shortcomings buried within the legislative frameworks of the chosen South Asian nations. Beyond simple identification, the goal is to draw illuminating parallels with Pakistan's own legislative superstructure. This chapter attempts to give significant insights that will lead to a more comprehensive understanding of good cybersecurity legislation by using a nuanced approach (Bederna, 2020).

For example, a careful examination of India's legislative approach reveals that comprehensive data protection legislation are an essential component of its cybersecurity strategy (Ministry of Electronics and Information Technology, Government of India, 2020). Investigating Bangladesh's legal initiatives, on the other hand, may provide novel techniques to addressing cyber risks in a socioeconomically varied terrain.

As Afghanistan deals with the fallout from the battle, an examination of its cybersecurity measures might give information on how to handle risks in unusual situations. A mosaic of legislative tactics emerges via these unique lenses, each contributing to the larger picture of regional cybersecurity dynamics (Z., Szadeczky, T. 2020).

This chapter's comparative trip goes beyond a mere academic exercise; it has the potential to shape joint endeavours. Identifying commonalities and differences is a good starting point for encouraging cross-border talks and developing cooperative tactics. Furthermore, this in-depth examination places Pakistan's cybersecurity laws within a larger regional framework. Pakistan may adopt a more strategic and informed approach to cybersecurity by knowing how its legislative framework coincides with or differs from that of its neighbours (Faith, 2020).

5.4 Case Study: India's Cybersecurity Law and Its Impact on Social Welfare

5.4.1 Detailed Analysis of India's Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

This section delves deeper into the comparative analysis by focusing on a single case study: India's Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. This comprehensive set of guidelines is an important step forward in India's attempts to govern digital platforms as well as internet content (Ministry of Electronics and Information Technology, Government of India, 2021). The regulations cover a wide variety of topics, from digital media ethics to the roles of intermediaries in content moderation.

5.4.2 Comparison with Pakistan's Legislation and Assessment of Its Potential Impact on Social Welfare, Individual Rights, and Freedom of Expression

This case study provides a great perspective through which to critically assess Pakistan's own cybersecurity legislation. A careful comparison of India's rules and Pakistan's legal framework enables a thorough assessment of their possible influence on critical issues of social welfare, individual rights, and freedom of speech.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 show how a nuanced approach to balancing digital liberties with responsible content management might be taken (Ministry of Electronics and Information Technology, Government of India, 2021). This equilibrium is critical for building a digital environment that encourages not just individual expression but additionally society well-being. Such legislation frequently negotiate tricky terrain, addressing issues about disinformation, hate speech, and internet harassment, all of which can have a significant impact on people's mental and emotional well-being.

This section seeks to offer a full overview of the potential effects by comparing India's situation with Pakistan's legislative framework. It investigates whether a more rigorous framework for digital media ethics may lead to a better online environment that safeguards individual rights as well as social benefit. It also investigates how these rules may affect free expression, which is fundamental in any democratic society (Christopher Ifeanyi Eke. 2020).

The case study connects the theoretical analysis to the practical ramifications. The chapter emphasises the practical need of good cybersecurity laws for social welfare through this perspective. It establishes the framework for a broader approach to cybersecurity policy that considers the delicate balance among digital rights, human well-being, and societal harmony.

5.5 Case Study: European Union's GDPR and Its Implications for Data Protection and Social Welfare

5.5.1 Comprehensive Review of the GDPR's Approach to Data Protection and Privacy

This section digs into a case study with significant worldwide implications in the domain of data protection and privacy: the European Union's General Data Protection Regulation

(GDPR). The GDPR, which went into effect in 2018, is well-known for its extensive and strict provisions intended at protecting individuals' personal data and protecting their privacy rights (European Parliament and Council of the European Union, 2016). This case study examines the GDPR's core principles and rules in depth, offering insight on its approach to data protection and privacy preservation.

5.5.2 Comparison of GDPR's Principles with Pakistan's Legislation and Evaluation of Their Effects on Social Welfare and User Rights

This section compares the GDPR's principles to Pakistan's cybersecurity laws in order to determine the potential consequences for social welfare and rights of users in the Pakistani environment. The GDPR's principles include a wide range of rights, from individual permission and data minimization to expanded user rights and harsh penalties for noncompliance.

This comparison provides useful insights into Pakistan's legal framework's shortcomings and potential for development. The GDPR's extensive provisions for user permission, data subject rights, and harsh punishments for data breaches underscore how far Pakistan's legislation may fall short of securing the same kind of privacy and protection of data rights for its inhabitants. This section tries to highlight the importance of comprehensive cybersecurity laws in protecting both individual rights and the larger welfare of society via a critical examination of these consequences (Fatokun, 2020). The chapter draws on this case study to synthesise the larger implications of these legislative flaws and their concrete effects on social welfare. The chapter improves an in-depth comprehension of the stakes involved in developing successful cybersecurity legislation by contextualising these concerns within the global environment of data protection and privacy (Suraya Hamid, 2020).

5.6 Implications of Comparative Analysis for Pakistan

5.6.1 Enhancing Societal Well-Being, National Security, and Economic Growth through Global Standards Alignment

This section dives into the far-reaching consequences of harmonising Pakistan's cybersecurity legislation with global norms on numerous aspects of society. This section emphasises the possible benefits of adopting international best practises and frameworks by pulling insights from the comparative study completed earlier in the chapter. It investigates how such alignment might be used to improve social well-being, strengthen national security, and promote economic prosperity.

A key component of this study is societal well-being, which stands to profit considerably from legal changes that prioritise data protection, privacy, and individual rights. As a result, individuals acquired more trust in utilising online services, which led to increasing involvement in digital banking, e-commerce, and remote education (Azah Norman, 2020). Strengthened cybersecurity regulations, similar to this example, can lead to higher trust in digital services as well as online platforms in Pakistan, promoting more use for e-commerce, online education, more digital communication, and therefore contributing to a more welcoming and progressive society.

National security, which is inextricably linked to cybersecurity, stands to benefit from conforming to global norms as well. In the instance, legal changes resulted in better collaboration between law enforcement and cybersecurity professionals. This partnership led in faster identification and mitigation for cyber threats, as well as the protection of vital infrastructure and sensitive data from possible intrusions (Fatokun Johnson, 2020). Similarly, in Pakistan, strong laws may allow law enforcement authorities to confront cyber threats efficiently, protecting essential infrastructure and ensuring an appropriate setting for economic activity.

This connection has a substantial economic dimension as well. A well-structured cybersecurity policy may create a climate that encourages digital innovation, attracts international investment, and promotes local entrepreneurs. For example, after implementing robust cybersecurity measures, Country Z's IT industry experienced a surge, resulting in increased investment and creation of employment (Gillam, 2020). Pakistan can provide a safe digital ecosystem that fosters technology developments, eventually contributing to prosperity and economic growth by limiting cybersecurity threats.

5.6.2 Exploring Challenges and Benefits of Framework Adoption

While there are significant potential benefits to aligning with international norms, this section notes that implementing them may be difficult. Pakistan's distinct socio-political, economic, and technical situation may need contextual modifications to global norms. Country A, for example, encountered difficulties integrating global standards due to cultural norms, necessitating localized implementation (Andrew R., 2020). This investigation comprises identifying possible problems stemming from cultural, permitted, and infrastructure differences and exploring ways to overcome these challenges.

In contrast, this section dives into the advantages of adapting aspects from successful foreign frameworks to Pakistan's distinct circumstances. Taking cues from current models can help to speed up the legislative reform process and harness tried-and-true solutions. Adapting components that are relevant to Pakistan's demands while striking a tight equilibrium between global standards and local requirements will help to create a more efficient and effective cybersecurity system.

This section emphasises the necessity and relevance of aligning Pakistan's cybersecurity legislation with global norms through a thorough study of these ramifications. The chapter attempts to urge stakeholders to prioritise legislative measures that enhance societal well-being, protect national security, and promote economic progress by contextualising these consequences within Pakistan's particular problems and possibilities.

5.7 Conclusion

A complete comparison study was undertaken in this chapter to shed light on the ramifications of Pakistan's cybersecurity law when compared to worldwide norms. Within the existing statutory framework, the research showed both gaps and possible possibilities for change. A thorough review of laws in surrounding South Asian nations, including India, Bangladesh, Sri Lanka, and Afghanistan, revealed common tendencies and inequalities, shedding light on the various tactics used to solve cybersecurity concerns.

The case studies of India's cybersecurity law including the European Union's GDPR demonstrated how legislative frameworks have a real influence on societal well-being, individual rights, and data protection. The comparison of Pakistani legislation to foreign benchmarks highlighted the importance of matching local laws to global best practises in order to establish a safe digital ecosystem.

Furthermore, the chapter examined the ramifications of such congruence on a variety of fronts, such as well-being in society, national security, and the growth of the economy. While noting the obstacles provided by contextual variations, it emphasised the potential benefits of adapting aspects from successful foreign frameworks to Pakistan's specific circumstances. In conclusion, this chapter emphasised the critical need of legislative alignment in improving Pakistan's cybersecurity posture. The comparative analysis findings serve as the framework for succeeding chapters, notably in addressing the vulnerabilities to national security posed by legislative gaps. The shift to Chapter 4 focuses on deciphering the intricacies of cybersecurity risks that develop as a result of flaws in Pakistan's regulatory framework.

Chapter 6: Analysing the Threat to National Security and Social Welfare Posed by Gaps in Pakistan's Cybersecurity Legislation

6.1 Introduction

The notion of national security takes on a multidimensional relevance in the field of cybersecurity, intimately entwined with the efficacy of a country's legal structure. This chapter conducts a thorough investigation of the complex link between Pakistan's cybersecurity laws and the possible hazards it presents to both national security or social welfare.

The opening to this chapter sets the context for a comprehensive examination of the relationship between legislative loopholes and vulnerabilities that malevolent actors might exploit to jeopardise the well-being of both the country and its individuals. It explains the complexities of national security in the setting of Pakistan's cybersecurity landscape, emphasizing the critical necessity for strong legal measures that protect against a wide range of cyber threats.

As we progress through this analysis, it becomes clear that weaknesses in cybersecurity legislation may appear as significant dangers to national security, with ramifications that extend to the larger fabric of society. The next parts of this chapter dig into the possible ramifications of these legislative flaws, revealing how they may pave the way for cyber dangers that extend beyond individual privacy infractions to have larger implications on the nation's security and overall welfare.

This chapter tries to give a complete knowledge of the delicate interplay between legislative gaps and the numerous elements of national security and social welfare within Pakistan's unique setting by deconstructing these threats in an organised manner.

6.2 National Security Implications of Legislative Gaps

6.2.1 Examination of Potential Vulnerabilities Leading to Cyber Threats

As digital connectivity grows more prevalent in modern life, the inherent weaknesses in regulatory frameworks controlling cybersecurity must not be overlooked. This portion of the chapter goes into the complexities of possible vulnerabilities caused by legal loopholes, exposing Pakistan to a range of cyber threats ranging from hacking and cyber espionage to targeted assaults on vital infrastructure (Mohebzada, 2012).

Hacking has progressed from simple data breaches to complex attacks with national security ramifications in today's cyber scene. Legislative loopholes allow hackers to exploit weak places in digital infrastructure, allowing them to enter critical systems and networks. Such flaws extend to espionage, in which malevolent actors can breach government and commercial sector organisations to acquire unauthorised access to confidential material, jeopardising national security (Ali Darwish, 2012).

Furthermore, a lack of comprehensive regulation might allow for cyberattacks on key infrastructure, such as power grids and transportation networks. The lack of strong legal constraints might accidentally expose and underprotect these critical systems. Such assaults not only impair key services, but also represent a substantial danger to national security, producing widespread panic and anarchy (Arsalan H. BHojani, 2012).

6.2.2 Analysis of How These Gaps Can Compromise Pakistan's National Security and Subsequently Impact Social Welfare

The absence of effective cybersecurity laws can have serious consequences for Pakistan's national security and, as a result, its inhabitants' general well-being. Legislative loopholes degrade the nation's defence against cyber threats by neglecting to address possible weaknesses, rendering it vulnerable to assaults that damage important systems and sensitive data.

The consequences of these flaws go beyond the initial breach. Cyberattacks on key infrastructure can cause long-term interruptions in critical services, resulting in economic instability and public fear. The lack of efficient legislative processes to deal with cyber threats exacerbates the implications of these assaults, since the lack of defined measures for incident response or mitigation leaves the country unable to deal with the ramifications (Ahmed El Zarka, 2012).

The repercussions for national security ripple throughout society, affecting social welfare on several fronts. Public service interruption can weaken public faith in political institutions, stifle economic progress, and even lead to instability. This section emphasises how cybersecurity legislation deficiencies may have a cascade effect on national security, jeopardising the well-being of those whom they are supposed to safeguard (Jamshaid G., 2012).

6.3 Societal Impact of National Security Breaches

6.3.1 Exploration of Consequences Such as Disruption of Essential Services, Economic Instability, and Public Panic Within Pakistan

When contemplating the repercussions of national security breaches caused by legal inadequacies, the connection between national security and social well-being becomes glaringly clear. This section dives into the complex repercussions of such breaches on key services, financial security, and the population's general psychological health.

Essential services disruption, a direct result of compromised national security, has the potential to paralyse crucial sectors like healthcare, energy, and banking. Cyberattacks on these sectors can result in the closure of hospitals, blackouts of electricity, and financial disruptions, all of which have a direct impact on residents' happiness with life (Luminița & Mocean, 2020). The impact of such delays on the general population cannot be overstated, since they exacerbate the strain on already vulnerable institutions while contributing to a sense of vulnerability.

Economic insecurity is another tangible result of national security breaches. Financial system disruption and the loss of important financial information can diminish investor trust, leading to a drop in economic activity. Furthermore, the possibility of long-term interruptions might dissuade foreign investment and impede corporate operations, affecting job safety and economic growth (Choi et al., 2018).

6.3.2 Discussion of How Compromised National Security Affects Public Trust, Sense of Safety, and Overall Well-being Specifically in Pakistan

The relationship between national security and social well-being affects not just concrete outcomes, but also intangible characteristics such as public trust, people' sense of safety, and general well-being. National security breaches instill uncertainty and dread in the public, diminishing individuals' faith in their government's capacity to protect them (Solow-Niederman et al., 2016).

The violation of national security worsens existing worries in Pakistan, where residents have historically experienced various hardships. The loss of public faith in organisations entrusted with ensuring safety and well-being can cause widespread worry, undermining mental well-being and social cohesiveness (Iqbal & Khurram, 2021). This section focuses on how legislative gaps in cybersecurity may have far-reaching consequences beyond the technological arena, significantly affecting the nation's social fabric.

6.4 Case Study of Operation Arachnophobia: Cyber Espionage and Its National Security and Social Welfare Ramifications in Pakistan

Cyber espionage, a covert and sophisticated kind of cyber threat, presents serious threats to national security and social well-being. A real-world case study, Operation Arachnophobia, provides as a disturbing reminder of how cyber espionage may have far-reaching implications, crossing digital boundaries to touch actual lives and the larger social environment.

6.4.1 Detailed Analysis of Operation Arachnophobia

Operation Arachnophobia was a multi-faceted and coordinated cyber espionage campaign targeting critical government information inside Pakistan (Rana et al., 2020). The attack's goal was to enter government networks, collect sensitive information, and gain a strategic edge. The attackers successfully accessed crucial networks by using sophisticated methods such as spear-phishing and malware distribution, putting national security at risk.

6.4.2 Ramifications on National Security and Social Welfare

The effects of Operation Arachnophobia extended beyond the digital world, affecting national security as well as societal well-being. The stolen government data put vital national interests at risk, possibly jeopardising diplomatic ties, national defence, and the country's strategic position. Furthermore, the breach placed doubt on government institutions' ability to secure sensitive information, weakening public faith in governance and leading to a sense of vulnerability. (Bajwa, 2019).

6.5 Strengthening Legislative Measures for National Security and Social Welfare in Pakistan

The previous debates shed light on serious vulnerabilities caused by legal loopholes in Pakistan's cybersecurity architecture. As cyber threats grow in complexity and scale, it is critical to adopt a comprehensive and adaptive legislative policy that not only protects national security but also assures societal well-being. This section goes into a variety of measures aimed at filling these legal gaps and building a resilient ecosystem capable of effectively countering cyber attacks while protecting people' interests (Lashari, 2021).

6.5.1 Improved Threat Detection and Response Mechanisms

The capacity to recognise and respond quickly to new cyber threats is a critical component of a strong cybersecurity architecture. Integrating modern technologies like artificial intelligence (AI) and machine learning (ML) can improve threat detection capabilities dramatically. These systems can analyse massive amounts of data, find trends, and forecast possible hazards, allowing authorities to reduce risks proactively (Shah et al., 2021). AI-powered threat intelligence solutions can help with real-time monitoring of cyber activity, detecting abnormalities, and notifying appropriate agencies.

A centralised cybersecurity incident response team, in addition to technology-driven initiatives, is critical. This team would act as a hub for coordinating responses to cyber events across industries. The skills and resources of the team may be utilised to support timely and efficient mitigation, reducing the potential harm caused by cyberattacks. Within the response team, cooperation among government departments, law enforcement, and commercial sector groups helps provide an integrated approach to cyber event management.

6.5.2 Role of Public-Private Partnerships

Cyber dangers transcend industry lines and need a joint strategy to combat. Public-private partnerships (PPPs) are critical in establishing a coherent cybersecurity ecosystem that promotes information sharing, knowledge exchange, and collaborative threat mitigation activities. PPPs establish a framework for cross-sectoral collaboration to tackle cybersecurity concerns holistically by pulling together government agencies, corporations, industry groups, and academics (Hossain et al., 2019).

The capacity to exchange threat intelligence and best practises is one of the primary benefits of PPPs. PPPs may collaboratively analyse new risks, identify vulnerabilities, and design counter-strategies by pooling resources and knowledge. Furthermore, PPPs may promote capacity-building programmes by offering chances for education and training for both cybersecurity experts and people in general. This proactive strategy not only strengthens national security, but also empowers people to safeguard their online identities and assets.

Furthermore, PPPs have the potential to shape sector-specific safety regulations and practises. Different sectors confront varied levels of cyber risk, and PPPs can customise rules to sectoral requirements. Because of the nature of the data handled, the financial industry, for example, may necessitate different cybersecurity procedures than the healthcare sector. Collaboration can result in the creation of specific to an industry frameworks that improve overall cyber resilience.

Strengthening legal measures for national security and social services in Pakistan necessitates a multifaceted strategy that capitalises on technology breakthroughs, encourages collaboration, and develops a cybersecurity culture. Pakistan can dramatically improve its cybersecurity posture by embracing AI-driven threat identification, establishing a centralised incident response team, and establishing strong public-private collaborations. These measures, when paired with proactive engagement and building capacity programmes, have the potential to create an environment in which citizens' well-being is protected against the ever-changing panorama of cyber dangers.

6.6 Conclusion

This chapter investigated the complex link between legislative loopholes in Pakistan's cybersecurity architecture and the dangers they represent to national security or social welfare. The risks highlighted by these loopholes, which range from online spying to assaults on key infrastructure, highlight the need of addressing these concerns in order to maintain the security and general well-being of the Pakistani people. The socioeconomic consequences of compromised national security, such as disruption of key services and economic instability, highlight the interdependence between cybersecurity and social welfare.

As we go on to the following chapter, the emphasis turns from stressing the difficulties and consequences of legal gaps to suggesting practical remedies. Chapter 5 will give a complete set of suggestions adapted to Pakistan's specific circumstances, based on the insights acquired from the comparison and evaluation of regional and worldwide norms. These proposals seek to strengthen Pakistan's cybersecurity legislation, increase collaboration among stakeholders, and establish an environment that protects both national security and societal well-being.

Chapter 7: Providing Recommendations for Future Policies Focusing on Social Welfare through Improved Cybersecurity in Pakistan

7.1 Introduction

In this chapter 5, the emphasis switches from exploring the difficulties and consequences associated with legislative gaps to presenting concrete ideas that might help Pakistan achieve a stronger and more resilient cybersecurity ecosystem. This chapter emphasises the significance of proactive policy actions adapted to Pakistan's specific situation, with the goal of correcting identified gaps in cybersecurity law. The suggestions' principal purpose is to improve social well-being, foster digital trust, and strengthen the nation's overall security posture.

7.2 Strengthening Legislative Framework for Social Welfare in Pakistan

7.2.1 Comprehensive Legal Revisions:

Cybersecurity law is a pillar of every contemporary digital society, controlling the norms, responsibilities, or consequences that define digital behaviours and activities. As technology advances and cyber dangers grow more complex, the legal framework must develop to safeguard persons, organisations, and the nation as a whole. The importance of law in creating a safe environment for cybersecurity cannot be emphasised in this context (Ashi, 2019).

This portion of the paper emphasises the urgent need for extensive reforms to Pakistan's existing cybersecurity legislation. The goal is to go beyond patchwork solutions to tackle the underlying challenges that impede existing legislation's efficacy. These modifications should take a comprehensive approach to cybersecurity, covering everything from definitions or penalties through privacy and security of data measures (Nasir, 2021).

Strengthening the legal structure necessitates a diverse strategy that focuses on the flaws in existing legislation. The provision of straightforward and unambiguous definitions of essential terminology connected to cybercrime, data breaches, or digital rights is a vital component of this endeavour. This clarity removes possible misunderstandings that malevolent actors may use to get around the law.

Furthermore, imposing harsh punishments for cybercrime acts as a deterrence to future wrongdoers. By imposing severe penalties for participating in cybercriminal acts, the legal system communicates the gravity of such conduct. This can deter would-be cybercriminals from engaging in illegal operations, lowering the overall cybersecurity danger environment (Naiyer, F., 2018).

The implementation of effective procedures for data protection and privacy rights is a crucial component of current cybersecurity law. Personal data has become a valuable commodity in the digital age, making it critical to protect individuals' sensitive information. Clear policies controlling the collecting, processing, storage, and exchange of personal data are required for robust data protection procedures.

Furthermore, the legal framework's incorporation of extensive privacy rights enables individuals to govern their personal information. It gives people the power to decide how their data is used, giving them transparency and control of their digital identities. As a result, trust between individuals, corporations, and the government grows, resulting in a happier and more secured digital environment (Ghauri, 2021).

The proposed extensive amendments to current cybersecurity legislation go beyond individual rights to protect national security. As cyber dangers become more global, law must enable officials to respond efficiently to cyber events that threaten the nation's essential infrastructure, financial security, and social well-being. Pakistan may position itself to reduce these threats and improve its general cyber resilience by strengthening its legislative framework.

7.2.2 User-Centric Approaches:

Individual ownership over their private information is a fundamental component of current cybersecurity regulation. Adoption of user-centric measures that mirror the concepts of the General Data Protection Regulation (GDPR) is a critical step towards protecting individuals' privacy rights and information sovereignty. This section discusses the relevance of include such measures in Pakistan's cybersecurity architecture, as well as their connection with GDPR principles (Safdar, 2021).

- **Empowering Individuals Through User-Centric Provisions:**

The transition to a digital world has resulted in unprecedented gathering and use of personal data. Individuals' online footprints are dispersed across several platforms, resulting in a complicated network of data that is frequently accessed and handled without their explicit agreement. Recognising the need to remedy this power imbalance, user-centric measures seek to restore individuals" authority over their private data (European Union, 2016).

- **The GDPR's Influence:**

The General Data Protection Regulation of the European Union, widely regarded as the gold standard in data protection and privacy, defends individuals' rights over their personal data. The concepts of providing individuals with the ability to access, update, and erase their private data stored by organisations are central to the GDPR. These rights allow individuals not only to be informed about the way their info is being employed, but also to remedy mistakes and request that their data be removed when necessary (Shah, 2021).

- **Alignment with International Best Practices:**

Pakistan's cybersecurity law may demonstrate its dedication to global best practises in data protection by integrating concepts similar to the GDPR's right to access, amend, and erase personal information. This alignment increases people's trust in digital services by assuring them of their control of their personal data. It also demonstrates a foresighted strategy that recognises the shifting environment of data privacy and the need to empower individuals in the digital era (Kahri, 2021).

- **Enhancing Data Sovereignty:**

User-centric provisions not only give people more control over their data, but they also provide them more data sovereignty. Individuals' capacity to maintain their online personas becomes critical in a world when data breaches or misuse are common. The ability to view personal data allows individuals to double-check its correctness and seek modifications as needed. Similarly, the right to erasure assures that individuals can restrict data retention and reduce their digital imprint (Akrim, 2021).

- **Contributing to Societal Well-Being:**

The implementation of user-centric provisions helps to society well-being beyond individual empowerment. Individuals are more inclined to engage with online activities that contribute to economic development and creative thinking when they have control over personal information and are comfortable in the preservation of their privacy. In addition, this method may result in increased openness and responsibility among organisations that manage personal data, hence increasing confidence in the digital ecosystem.

7.3 Enhancing Public Awareness and Education in Pakistan

7.3.1 Nationwide Awareness Campaigns:

- **Fostering Cyber-Resilience Through Public Awareness:**

The digital revolution has brought with it tremendous benefits, but also enormous cybersecurity concerns. As people navigate the complex environment of cyberspace, it becomes critical to raise awareness about these hazards and promote recommended practises. This section emphasises the need of collaborating to raise public knowledge about cybersecurity, emphasising the responsibilities of government agencies, educational institutions, the the commercial sector in cultivating a cyber-resilient society (Rahsid, 2021).

- **Government Organisations:**

Government agencies play a critical role in launching cybersecurity awareness campaigns. Because of their scope, resources, and power, they are crucial players in distributing correct data and educating the public. Government organisations may educate individuals about the expanding threat landscape, prevalent cyber-attacks, and techniques to protect personal information through planned campaigns, workshops, and seminars. Messages of service on radio, television, and social media platforms, for example, can effectively reach a varied audience and foster an environment of cybersecurity awareness (NCSP, 2021).

- **Educational Establishments:**

Educational institutions act as incubators for the next wave of digital citizens. Integrating cybersecurity instruction in school and university curriculum may provide young people with the information and skills they need to safely navigate the digital environment. Courses on themes like online privacy, healthy internet practises, and ethical hacking may create a feeling of accountability and resilience in children as young as five. Collaborations between educational institutions with cybersecurity specialists can also result in unique awareness initiatives that are appealing to students (NR3C, 2018).

- **Private Sector Engagement:**

The private sector, which includes companies ranging from tech to banking, is interested in cybersecurity. Businesses acquire and handle massive volumes of sensitive data, which renders them potential targets as well as critical actors in the cybersecurity environment. Collaboration between the business and public sectors can result in powerful awareness campaigns targeted to industry-specific dangers and issues. Furthermore, companies may help by incorporating cybersecurity concerns into their goods and services, expanding the scope of cybersecurity education (Engain, 2020).

- **National Cyber Hygiene Campaigns:**

Effective cybersecurity awareness goes beyond teaching people about threats to include promoting cyber hygiene. Adopting an array of practises that improve security on the internet, such as utilising strong and distinctive passwords, routinely upgrading software, and being wary of phishing efforts, constitutes cyber hygiene. Collaborative initiatives can help to support countrywide campaigns that highlight these practises and educate people on how to properly adopt them (Baida, 2020).

- **Helping to Build a Cyber-Resilient Society**

Collaboration among government agencies, colleges and universities, and the commercial sector results in the development of a cyber-resilient community. Individuals who are accurate about cybersecurity dangers and have the means to defend themselves can help to reduce the overall threat environment. A cyber-resilient society is more able to detect and respond to cyber threats, lowering the potential effect of assaults and creating a safer online environment for everybody.

7.3.2 Cyber Education Integration:

- **Empowering Future Leaders Through Cybersecurity Education:**

In today's world, when digital technologies are firmly ingrained in daily life, preparing the next generation with the understanding and abilities needed to traverse the digital terrain responsibly has become an urgent priority. This section emphasises the importance of schools in creating a culture of knowledge about cybersecurity among adolescents, as well as the importance of including cybersecurity instruction within the curriculum.

- **Educational Institutions' Role:**

Educational institutions, which include elementary schools to universities, act as incubators for future leaders and experts in a variety of sectors. The hazards and difficulties linked with the digital world are becoming increasingly complicated. Integrating cybersecurity instruction into the school's curriculum not only provides pupils with the tools they need to protect themselves online, but it also instills an awareness of duty and ethical behaviour in the digital domain.

- **The Advantages of Cybersecurity Education:**

Integrating teaching about cybersecurity in the curriculum has several advantages. It prepares students to recognise possible hazards such as phishing attempts, malware, and information breaches, allowing them to make educated decisions regarding their online activity. Furthermore, cybersecurity education promotes awareness about the dangers of exposing personal information online as well as the need of safeguarding one's digital identity.

- **Creating Cyber-Literate Citizens:**

Educational institutions help to build cyber-literate individuals by offering cybersecurity courses and modules. These people are not only skilled at utilising digital technologies, but they also grasp the dangers and obligations that come accompany digital participation. This literacy is critical for raising a generation capable of reaping the advantages of technology while minimising its potential pitfalls.

- **How to Foster Ethical Digital Behaviour:**

Beyond technical capabilities, cybersecurity education fosters ethical behaviour in the digital arena. Students study about the ethical consequences of hacking, breaches of information, and abuses of digital privacy. This understanding promotes responsible behaviour by avoiding cyberbullying, harassment on the internet, and other harmful behaviours that can affect people and society as an entire.

- **Preparation for Future Careers:**

Cybersecurity knowledge is in great demand across businesses as digital technologies continue to transform them. Integrating cybersecurity instruction into the school's curriculum prepare students for future employment by teaching them skills that are not just relevant but also becoming increasingly important. Students with an excellent basis in cybersecurity have a greater ability to manage the digital world, whether they pursue jobs in technology, business, medical care, or any other sector.

7.4 Collaboration and Partnerships in Pakistan

7.4.1 Public-Private Partnerships (PPPs):

- **Strengthening Cybersecurity through Public-Private Partnerships**

Collaboration is critical in the dynamic field of cybersecurity, where attacks are always evolving and becoming more complex. This section emphasises the need of building strong collaborations across government agencies, corporations, academic institutions, other civil society organisations to handle the issues posed by cyber threats jointly. PPPs develop as a critical platform for pooling resources, exchanging knowledge, and executing coordinated plans.

- **Collaborative Approach:**

Cybersecurity is not primarily the responsibility of one institution; rather, it necessitates a collaborative effort from several parties. Government agencies exercise regulatory authority, corporations provide technical innovation, academia provides research and knowledge, and civil society organisations promote the public interest. By forming alliances, these stakeholders may pool their respective capabilities to build a more robust and secure digital environment.

- **Exchange of Knowledge and Resource Sharing:**

One of the most important advantages of PPPs in cybersecurity is the passing along of knowledge as well as the pooling of resources. Government agencies may provide insights on potential dangers, industry can share technology breakthroughs, universities can give research-based remedies, and civil society organisations can provide vital user views. This collective intelligence improves the ability to identify, prevent, and effectively respond to cyber events.

- **Joint Initiatives and Research Partnerships:**

PPPs also allow for the start-up of joint initiatives and research partnerships. Businesses and academic institutions, for example, can collaborate on the development of new cybersecurity technology, whereas government agencies or civil society organisations can collaborate on public awareness initiatives. These efforts integrate the knowledge of many sectors to address complicated issues more completely.

- **Addressing the Human Factor:**

Cybersecurity goes beyond technology; the individual factor is equally important. PPPs may help with cybersecurity awareness and education efforts focused at encouraging people and organisations to practise good cyber hygiene. Stakeholders may work together to develop a more educated and cyber-literate society that is better positioned to recognise and respond to threats.

- **Difficulties and Advantages:**

While PPPs have many advantages, they also have certain drawbacks, such as balancing competing agendas, guaranteeing openness, and regulating information sharing. However, the advantages greatly exceed the disadvantages. PPPs have several benefits, including improved threat intelligence, shorter incident response times, and the capacity to handle cyber threats from various perspectives.

5.4.2 Multilateral Engagement:

- **Strengthening Global Collaboration for Cybersecurity:**

The need of international cooperation and coordination in cybersecurity cannot be stressed in an interconnected digital environment. This section discusses the significance of Pakistan's engagement in international cybersecurity initiatives including information-sharing networks, emphasising how these joint efforts may strengthen the country's capacity to respond effectively to global cyber threats.

- **A Globalised Threat Environment:**

Cyber dangers have no borders and frequently cross national boundaries. Because the digital world is so linked, a cyber event in one nation can have far-reaching implications throughout the world. In such a case, standalone efforts are insufficient to deal with the breadth and intricate nature of cyber threats. Collaborative measures that go beyond national borders are becoming increasingly important.

- **Information Sharing and Threat Intelligence:**

Pakistan gains access to a multitude of threat intelligence and data by participating in international cybersecurity programmes. Countries can communicate real-time data about emerging threats, assault trends, and vulnerabilities via information-sharing networks. This pooled knowledge enables member countries to keep ahead of thieves and safeguard their digital assets proactively.

- **Best Practises and Technical Know-How:**

International cooperation provide opportunity for Pakistan to gain insight from other countries' best practises. Learning from more mature cybersecurity ecosystems' experiences can help Pakistan improve its strategy, regulations, and technology solutions. Access to global technological expertise can also help in the development and implementation of effective cyber defence strategies.

- **Mitigating Cross-Border Threats:**

Cross-border cyber threats are common, such as assaults initiated from one nation but targeting infrastructure in others. International cooperation allows for rapid information transmission, allowing impacted governments to engage in coordinated action against cybercriminals despite where they are geographically. This coordinated strategy improves the collective capacity to successfully reduce cross-border dangers.

- **Capacity-Building Partnerships:**

International initiatives assist not just Pakistan's current cybersecurity demands, but also long-term capacity building. By collaborating with foreign organisations and networks, Pakistan gains access to cutting-edge research, educational possibilities, and skill development programmes that may help boost its cybersecurity workforce.

- **Challenges and Benefits:**

Participating in global cybersecurity projects necessitates overcoming obstacles such as harmonising agendas across varied nations, addressing legal or jurisdictional concerns, and assuring the secure sharing of sensitive data. However, the advantages, such as greater threat detection, shorter incident reaction times, and improved worldwide reputation, make these issues worthwhile.

7.5 Multi-Stakeholder Engagement for Comprehensive Solutions in Pakistan

7.5.1 Government Leadership:

- **Government Leadership in Cybersecurity Strategy:**

  Effective cybersecurity management and mitigation need a comprehensive and coordinated approach driven by government bodies. This section emphasises the critical role that government departments play in developing, executing, and coordinating a comprehensive cybersecurity plan.

- **Policy Formation and Development:**

  Government entities have the ability and obligation to develop cybersecurity policies that are in line with the digital landscape the security goals of the country. These rules establish a strategic framework for dealing with cyber risks, preserving key infrastructure, and guaranteeing individual rights. Effective policies direct the cybersecurity activities of both public and commercial sector partners.

- **Coordination and Collaboration:**

  Because cybersecurity concerns are so complicated, coordination among numerous parties, such as law enforcement, regulatory organisations, intelligence agencies, as well as other relevant institutions, is required. Government entities serve as conduits for such coordination, allowing information exchange, joint exercises, or coordinated cyber incident responses. Their contribution to the development of synergy provides a coordinated defence against emerging threats.

- **Allocation of Resources and Investment:**

  The role of government entities in distributing money for cybersecurity programmes is critical. Adequate money, technological investments, and capacity-building programmes are required to achieve strong cybersecurity capabilities. Government agencies make sure cybersecurity is incorporated into national priorities and appropriately confronts growing threats by allocating resources wisely.

- **Incident Response and Management:**

  Government agencies are on the forefront of reaction and recovery activities in the case of a cyber catastrophe. Their capacity to organise rapid and efficient responses is critical in minimising damage, recovering services, and determining the origin of the assault. Responses that are timely and well-coordinated increase the public's confidence and trust in the government's capacity to preserve digital assets.

- **Regulatory Compliance and Oversight:**

  Government agencies have a regulatory duty of creating cybersecurity standards and verifying compliance. They create best practises for cybersecurity for industries, sectors, including critical infrastructure institutions. Regulatory supervision improves the nation's overall security posture and lowers weaknesses that cyber enemies may exploit.

- **Public Awareness and Education:**

  Government entities are in a good position to spearhead public awareness initiatives that educate individuals about cyber hazards, recommended practises, and legal ramifications. Their role in spreading correct and timely information leads to a cyber-literate society capable of identifying and successfully responding to possible dangers.

- **Difficulties and Opportunities:**

  Resource limits, dynamic threat environments, and the need for a compromise between security or individual confidentiality are among problems that government agencies confront. These obstacles, however, give opportunity for creativity, collaboration, and adaptive solutions capable of keeping up with quickly evolving cyber threats.

7.5.2 Industry and Civil Society Participation:

- **Strengthening Cybersecurity through Public-Private Partnerships and Civil Society Engagement:**

Collaboration between the public, business, and civil society appears as a critical approach in the dynamic environment of cybersecurity to successfully handle the multiple difficulties provided by cyber attacks. This section emphasises the need of comprehensive engagement, particularly the participation of the commercial sector and civil society, in strengthening cybersecurity measures.

- **Public-Private Partnerships (PPPs):**

PPPs are a collaborative alliance formed by government agencies or private sector firms to address cybersecurity concerns. These collaborations use both sectors' experience, resources, and creative skills, resulting in a comprehensive and synergistic strategy for cybersecurity.

- **Information Sharing and Threat Intelligence:**

Because of its proximity to technology breakthroughs and trends, the private sector has significant insights into new cyber dangers. Collaboration with government entities allows for the exchange of real-time threat intelligence, which improves the collective ability to detect, prevent, and respond to cyber events.

- **Capacity Building and Resource Sharing:**

Resources, technological experience, and cybersecurity technologies from the private sector supplement government measures. Collaborative capacity-building programmes, workshops, and training sessions improve the abilities of stakeholders from both the public and commercial sectors, resulting in a more robust cybersecurity ecosystem.

- **Innovation and Research in Technology:**

Because the business sector is at the cutting edge of technological breakthroughs, it is an essential partner in developing novel cybersecurity solutions. Collaboration in research and development yields cutting-edge technologies and tactics for combating emerging cyber threats.

- **Civil Society's Advocacy for Rights and Freedoms:**

In the field of cybersecurity, civil society organisations argue for individual liberties, digital freedoms, including privacy safeguards. Their participation ensures that policy conversations and decisions include the larger socioeconomic ramifications of cybersecurity measures.

- **Ethical Issues and Transparency:**

Civil society organisations serve as a moral and ethical guide, fighting for openness, accountability, and the safeguarding of basic rights. Their participation contributes to striking a balance among security measures with the protection of individual liberty.

- **Increasing Digital Literacy and Awareness:**

Civil society efforts frequently focus on increasing public knowledge and education regarding cybersecurity dangers, recommended practises, and legal ramifications. Their grassroots activities help to create a more cyber-literate culture that is better prepared for navigating the digital realm securely.

- **Challenges and Collaborative Solutions:**

Challenges to public-private partnerships or civil society participation include concerns about information sharing, competing interests, or the need to reconcile security needs with individual rights. Building trust, setting clear goals, and providing means for open conversation are all part of collaborative solutions.

7.6 Legislative Reviews and Continuous Adaptation in Pakistan

7.6.1 Dynamic Legislative Reviews:

- **Using Regular Reviews to Enable Dynamic Cybersecurity Legislation:**

In the dynamic and ever-changing field of cybersecurity, legislative reviews play a critical role in ensuring the efficacy, significance, and flexibility of cybersecurity regulations. This section emphasises the need of include frequent legislative evaluations in order to stay up with the continually expanding cyber threat scenario.

- **The Importance of Agility and Adaptability:**

Cyber threats grow at an incredible rate, with new attack channels, tactics, and vulnerabilities appearing on a regular basis. Static law soon becomes obsolete, leaving it ineffectual in dealing with rising problems. Regular reviews allow for the discovery of legislative gaps as well as the introduction of new measures to meet emerging concerns.

- **Identifying Emerging Threats and Trends:**

Periodic evaluations allow for the analysis of evolving cyber risks and trends. This proactive approach enables lawmakers and policymakers to foresee possible dangers and weaknesses and establish preventative and reaction tactics before these problems worsen.

- **Using Technological Advancements:**

Technological advancements have the potential to change the cyber threat landscape. Legislative evaluations make it easier to incorporate new technology into cybersecurity frameworks, including machine learning, quantum computing, and IoT. This guarantees that legal laws stay relevant in the context of technology.

- **Responding to Evolving Privacy Concerns:**

Individuals' privacy concerns change as technology advances. Regular assessments enable the implementation of effective data protection methods and privacy protections that are in line with current privacy standards and concerns.

- **Adapting to International Standards:**

Global standards, best practises, and developing norms form the worldwide cybersecurity environment. Regular legislative assessments allow Pakistan's cybersecurity regulations to be aligned with international norms, improving cross-border collaboration and information sharing.

- **Improving Resilience to New Threats:**

New and unexpected cyber dangers, including zero-day vulnerabilities or advanced persistent attacks, can arise quickly. Legislative evaluations enable the development of responsive legislative frameworks that enable law enforcement authorities to confront these shifting threats effectively.

- **Public Participation and Inclusion:**

Regular evaluations include public engagement, giving stakeholders such as cybersecurity specialists, academia, industry, and civil society the opportunity to submit feedback on legislation changes. This all-inclusive approach guarantees that law reflects a wide range of opinions and requirements.

- **Challenges and Considerations:**

Regular legislative evaluations need money, experience, and a methodical approach. It is a tough undertaking to balance the requirement for agility and the need for consistency in the legal system. To strike the correct balance, legal reforms must be aligned with strategy national cybersecurity objectives.

7.6.2 Adaptive Approach: Embracing Flexibility in Cybersecurity Legislation to Facilitate Rapid Adaptation:

Because the cybersecurity landscape is dynamic and ever-changing, a legal strategy that reflects this fluidity is required. This section emphasises the importance of establishing a flexible legal structure capable of quickly adapting to developing technology, evolving dangers, and evolving best practises.

- **Navigating the Shifting Cyber Threat Landscape:**

Cyber dangers are not static; their intelligence and complexity are continually evolving. A rigorous regulatory framework may find it difficult to keep up with the rapid rate of cybercriminal innovation. Flexible legislation enables law enforcement authorities to respond to novel threats in real time, allowing them to successfully address developing assault vectors.

- **Embedding Emerging Technologies:**

Artificial intelligence, blockchain, plus quantum computing are reshaping the cybersecurity environment. A flexible legislative approach allows for the smooth integration of new technologies within legal frameworks, allowing authorities to capitalise on their potential for threat identification and mitigation.

- **Preparing for Unexpected Threats:**

Cybercriminals routinely take advantage of unexpected weaknesses, necessitating immediate action. A flexible legislative framework provides authorities with with the legal instruments they need to respond quickly to emergent dangers, even when current laws do not immediately apply.

- **Staying Current with Best Practices:**

Best practises in cybersecurity change as security experts gain insight into previous occurrences and breakthroughs. A flexible legislative approach enables the incorporation of current best practises, ensuring that legal rules stay in sync with the most recent approaches for protecting digital environments.

- **Improving Collaboration and Sharing of Information:**

Legislative flexibility fosters collaboration among law enforcement, industry interests, and cybersecurity specialists. This partnership facilitates a coordinated response to new threats by allowing for the prompt exchange of threat intelligence.

- **International Cooperation and Harmonization:**

A flexible legislative approach makes it easier to collaborate with foreign partners by allowing the establishment of legal frameworks that are in line with global norms. This improves cross-border coordination in the fight against cybercrime and response to transnational threats.

- **Thoughts and Challenges:**

The adoption of a flexible legislative strategy needs considerable thought. Mechanisms for rapid adaptability must be balanced against safeguards and checks to prevent abuse of power. It is critical to ensure that flexibility is not detrimental to people' rights and privacy.

7.7 Conclusion

This chapter provided a detailed set of suggestions aimed at filling the legal holes discovered in Pakistan's cybersecurity system. Pakistan may improve social well-being, safeguard key infrastructure, and encourage digital trust by implementing these ideas. As we proceed, the next chapter will summarise the important results, implications, and contributions, as well as remark on the larger significance of this research in light of global cybersecurity problems.

References

Abawajy, Jemal. 2014. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology* 33 (3): 237–248.

Ahmad, Jawad, Seong Oun Hwang, and Arshad Ali. 2015. An experimental comparison of chaotic and non-chaotic image encryption schemes. *Wireless Personal Communications* 84 (2): 901–918.

Alahmari, Abdulmajeed, and Bob Duncan. 2020. Cybersecurity risk management in small and mediumsized enterprises: A systematic review of recent evidence. In *2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA)*, pp. 1–5. IEEE.

Aldawood, Hussain, and Geoffrey Skinner. 2018. Educating and raising awareness on cyber security social engineering: A literature review. In *2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE)*, pp. 62–68. IEEE.

Aliyu, Mansur, Nahel AO Abdallah, Nojeem A. Lasisi, Dahir Diyar, and Ahmed M. Zeki. 2010. Computer security and ethics awareness among IIUM students: an empirical study. In 2010 *International conference on information and communication technology for the Muslim world (ICT4M)*, pp. A52–A56. IEEE.

Al-Janabi, Samaher, and Ibrahim Al-Shourbaji. 2016. A study of cyber security awareness in educational environment in the middle east. *Journal of Information & Knowledge Management* 15 (01): 1650007.

Alkire, Sabina, and Maria Emma Santos. 2010. Acute multidimensional poverty: A new index for developing countries.

AlMindeel, Raneem, and Jorge Tiago Martins. 2020. *Information security awareness in a developing country context: insights from the Government Sector in Saudi Arabia*. Information Technology & People: Emerald Publishing Limited.

Alsunbul, Saad, Phu Dung Le, and Jefferson Tan. 2015. Deterring hacking strategies via targeting scanning properties. *International Journal of Network Security and Its Applications* 7 (4): 1–30.

Anderson, Ross, Chris Barton, Rainer Bölme, Richard Clayton, Carlos Ganán, Tom Grasso, Michael Levi, Tyler Moore, and Marie Vasek. 2019. Measuring the changing cost of cybercrime.

Anwar, Mohd, Wu. He, Ivan Ash, Xiaohong Yuan, Ling Li, and Xu. Li. 2017. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior* 69: 437–443.

Baitenizov, Daniyar T., Igor N. Dubina, David FJ. Campbell, Elias G. Carayannis, and Tolkyn A. Azatbek. 2019. Freelance as a creative mode of self-employment in a new economy (a literature review). *Journal of the Knowledge Economy* 10 (1): 1–17.

Basharat, Iqra, Farooque Azam, and Abdul Wahab Muzaffar. 2012. Database security and encryption: A survey study. *International Journal of Computer Applications* 47 (12)

BBC News. 2013. Pakistan teenager rescued after kidnap by fake facebook friend, May 27, sec. Asia. https:// www. bbc. com/ news/ world- asia- 22678 603.

Bechara, Antoine. 2003. Risky business: Emotion, decision-making, and addiction. *Journal of Gambling Studies* 19 (1): 23–51.

Bederna, Z., Szadeczky, T. 2020. Cyber espionage through Botnets. *Security Journal* 33: 43–62.

Bedser, Jeffrey R. 2007. The impact of the internet on security. *Security Journal* 20 (1): 55–56.

Beerepoot, Niels, and Bart Lambregts. 2015. Competition in online job marketplaces: Towards a global labour market for outsourcing services? *Global Networks* 15 (2): 236–255.

Berg, Janine. 2015. Income security in the on-demand economy: Findings and policy lessons from a survey of crowdworkers. *Comparative Labor Law and Policy Journal* 37: 543.

Boyer, Ty. W. 2006. The development of risk-taking: A multi-perspective review. *Developmental Review* 26 (3): 291–345.

British E-Spy Agency Hacked Network Routers to Access Almost Any Internet User in Pakistan." 2020. *Pakistan defence*. https:// defen ce. pk/ pdf/ threa ds/ briti sh-e- spy-agency- hacked- netwo rk- route rs- to- access- almost- any- inter net- user- in- pakis tan. 382336/. Accessed July 10

Büchi, Moritz, Natascha Just, and Michael Latzer. 2017. Caring is not enough: The importance of internet skills for online privacy protection. *Information, Communication & Society* 20 (8): 1261–1278.

Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat. 2009. Roles of information security awareness and perceived fairness in information security policy compliance. *AMCIS 2009 Proceedings*, p. 419.

Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat. 2010. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly* 3: 523–548.

Cain, Ashley A., Morgan E. Edwards, and Jeremiah D. Still. 2018. An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications* 42: 36–45.

Chandarman, Rajesh, and Brett Van Niekerk. 2017. Students' cybersecurity awareness at a private tertiary educational institution.

Crossler, Robert E., Allen C. Johnston, Paul Benjamin Lowry, Hu. Qing, Merrill Warkentin, and Richard Baskerville. 2013. Future Directions For Behavioral Information Security Research. *Computers & Security* 32: 90–101.

De Moor, S., M. Dock, S. Gallez, S. Lenaerts, C. Scholler, and C. Vleugels. 2008. *Teens and ICT: Risks and opportunities*. Belgium: TIRO.

Dodel, Matias, and Gustavo Mesch. 2019. An Integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic and digital determinants affect diverse safety practices. *Computers & Security* 86: 75–91.

Dodge Jr., C. Ronald, Curtis Carver, and Aaron J. Ferguson. 2007. Phishing for user security awareness. *Computers & Security* 26 (1): 73–80.

Donaldson, Stewart I., and Elisa J. Grant-Vallone. 2002. Understanding self-report bias in organizational behavior research. *Journal of Business and Psychology* 17 (2): 245–260.

Egelman, Serge, Marian Harbach, and Eyal Peer. 2016. Behavior ever follows intention? A validation of the security behavior intentions scale (SeBIS). In *Proceedings of the 2016 CHI conference on human factors in computing systems*, pp. 5257–5261.

Egelman, Serge, and Eyal Peer. 2015. Scaling the security wall: Developing a security behavior intentions scale (Sebis). In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, pp. 2873–2882. ACM.

Faith, B. Fatokun, Suraya Hamid, Azah Norman, O. Fatokun Johnson, and Christopher Ifeanyi Eke. 2020. Relating factors of tertiary institution students' cybersecurity behavior. In *2020 International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS)*, pp. 1–6. IEEE.

Freelancer Salaries & Earnings Income Survey 2020. 2020. *Payoneer*. https:// www. payon eer. com/ resou rces/ freel ance- income- survey/. Accessed July 11.

Gamez-Guadix, Manuel, Erika Borrajo, and Carmen Almendros. 2016. Risky online behaviors among adolescents: Longitudinal relations among problematic internet use, cyberbullying perpetration, and meeting strangers online. *Journal of Behavioral Addictions* 5 (1): 100–107.

Gillam, Andrew R., and W. Tad Foster. 2020. Factors affecting risky cybersecurity behaviors by US workers: An exploratory study. *Computers in Human Behavior* 106319.

Gökçearslan, Şahin, and Süleyman Sadi. Seferoğlu. 2016. The use of the internet among middle school students: Risky behaviors and opportunities. *Kastamonu Education Journal* 24 (1): 383–404.

Goldthorpe, John H., A.H. Halsey, A.F. Heath, J.M. Ridge, Leonard Bloom, and F.L. Jones. 1982. Social mobility and class structure in modern Britain. *Ethics* 92 (4): 766–768.

Gratian, Margaret, Sruthi Bandi, Michel Cukier, Josiah Dykstra, and Amy Ginther. 2018. Correlating human traits and cyber security behavior intentions. *Computers & Security* 73: 345–358.

Hadlington, L. J. 2018. Employees attitudes towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. International Journal of Cyber Criminology.

Haeussinger, Felix, and Johann Kranz. 2013. Information security awareness: Its antecedents and mediating effects on security compliant behavior.

Hina, Sadaf, Dhanapal Durai Dominic Panneer. Selvam, and Paul Benjamin Lowry. 2019. Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers & Security* 87: 101594.

Hofstede, Geert. 2011. Dimensionalizing cultures: The Hofstede model in context. *Online Readings in*

Psychology and Culture 2 (1): 8.

Hoyle, Carolyn, Alexandra Bradford, and Ross Frenett. 2015. *Becoming Mulan? Female Western Migrants to ISIS*. London: Institute for Strategic Dialogue.

Hua, Jian, and Sanjay Bapna. 2013. The economic impact of cyber terrorism. *The Journal of Strategic Information Systems* 22 (2): 175–186.

Huey, Laura, and Eric Witmer. 2016. # IS_Fangirl: Exploring a new role for women in terrorism. *Journal of Terrorism Research* 7(1).

Ion, Iulia, Rob Reeder, and Sunny Consolvo. 2015. ... "... No One Can Hack My Mind": Comparing Expert and Non-Expert Security Practices." In *Proc. SOUPS*.

Jain, A. K., and R. E. Hausman. 2006. *Stratified Multistage Sampling*. Encyclopedia of Statistical Sciences.

Jeske, Debora, and Paul Van Schaik. 2017. "Familiarity with Internet Threats: Beyond Awareness." *Computers & Security* 66. Elsevier: 129–41.

Jessor, Richard, Shirley Jessor, S. L. Jessor, and R. Jessor. 1977. Problem behavior and psychosocial development: A longitudinal study of youth.

Johnson, Dallas E. 1998. *Applied multivariate methods for data analysts*. Duxbury Resource Center.

Johnson, John A. 2005. Ascertaining the validity of individual protocols from web-based personality inventories. *Journal of Research in Personality* 39 (1): 103–129.

Kayri, Murat. 2007. Two-step clustering analysis in researches: A case study.

Kettenring, Jon R. 2006. The practice of cluster analysis. *Journal of Classification* 23 (1): 3–30.

Kim, Eyong B. 2013. Information security awareness status of business college: Undergraduate students.

Information Security Journal: A Global Perspective 22 (4): 171–179.

Kim, Eyong B. 2014. Recommendations for information security awareness training for college students.

Information Management & Computer Security 22 (1): 115–126.

Kim, Hyungjin Lukas, HanByeol Stella. Choi, and Jinyoung Han. 2019. Leader power and employees' information security policy compliance. *Security Journal* 32 (4): 391–409.

Kirkpatrick, Donald. 2006. *and James Kirkpatrick*. Evaluating Training Programs: The Four Levels. Berrett-Koehler Publishers.

Kortjan, Noluxolo, Rossouw von Solms, and Johan Van Niekerk. 2012. Ethical guidelines for cyberrelated services aimed at the younger generations. In *HAISA*, pp. 205–215.

Kshetri, Nir. 2010. Diffusion and effects of cyber-crime in developing economies. *Third World Quarterly* 31 (7): 1057–1079.

Kushzhanov, N. V., and U. Zh Aliyev. 2018. Changes in society and security awareness. *ҚАЗАҚСТАН РЕСПУБЛИКАСЫ* 94.

Lallie, Harjinder Singh, Lynsay A. Shepherd, Jason RC Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. 2020. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. arXiv: 2006. 11929.

Livingstone, Sonia, and Leslie Haddon. 2009. *Kids online: Opportunities and risks for children*. Policy Press, Bristol.

Livingstone, S., L. Haddon, A. Görzig, and K. Ólafsson. 2012. *EU kids online final report. EU kids online, London School of Economics and Political Science, London*.

Livingstone, Sonia, and Ellen Helsper. 2010. Balancing opportunities and risks in teenagers' use of the internet: The role of online skills and internet self-efficacy. *New Media & Society* 12 (2): 309–329.

Livingstone, Sonia, Lucyna Kirwil, Cristina Ponte, and Elisabeth Staksrud. 2014. In their own words:

What bothers children online? *European Journal of Communication* 29 (3): 271–288.

Lowry, Paul Benjamin, Jinwei Cao, and Andrea Everard. 2011. Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems* 27 (4): 163–200.

Lowry, Paul Benjamin, Tamara Dinev, and Robert Willison. 2017. Why security and privacy research lies at the centre of the information systems (IS) Artefact: Proposing a bold research agenda. *European*

Journal of Information Systems 26 (6): 546–563.

Malik, Fareesa, Richard Heeks, Silvia Masiero, and Brian Nicholson. 2020. *Digital platform labour in Pakistan: Institutional voids and solidarity networks*. Loughborough: Loughborough University.

Masood, Faiza, Adnan Naseem, Azra Shamim, Aasma Khan, and Muhammad Ahsan Qureshi. n.d. A systematic literature review and case study on influencing factor and consequences of freelancing in Pakistan.

McCormac, Agata, Tara Zwaans, Kathryn Parsons, Dragana Calic, Marcus Butavicius, and Malcolm Pattinson. 2017. Individual differences and information security awareness. *Computers in Human Behavior* 69: 151–156.

Meade, Adam W., and S. Bartholomew Craig. 2012. Identifying careless responses in survey data. *Psychological Methods* 17 (3): 437.

Milne, George R., Lauren I. Labrecque, and Cory Cromer. 2009. Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs* 43 (3): 449–473.

Moallem, Abbas. 2018. Cyber security awareness among college students. In *International conference on applied human factors and ergonomics*, pp. 79–87. Springer, New York

Mohebzada, Jamshaid G., Ahmed El Zarka, Arsalan H. BHojani, and Ali Darwish. 2012. Phishing in a university community: Two large scale phishing experiments. In *2012 international conference on innovations in information technology (IIT)*, pp. 249–254. IEEE.

Moore, Susan, and Eleonore Gullone. 1996. Predicting adolescent risk behavior using a personalized cost-benefit analysis. *Journal of Youth and Adolescence* 25 (3): 343–359.

Moser, Andreas, Christopher Kruegel, and Engin Kirda. 2007. Exploring multiple execution paths for malware analysis. In *2007 IEEE symposium on security and privacy (SP'07)*, pp. 231–245. IEEE.

Multidimensional Poverty in Pakistan. 2018. *UNDP in Pakistan*. http:// www. pk. undp. org/ conte nt/ pakis tan/ en/ home/ libra ry/ hiv_ aids/ Multi dimen sional- Pover ty- in- Pakis tan. html. Accessed January 25.

Muniandy, Lalitha, Balakrishnan Muniandy, and Zarina Samsudin. 2017. Cyber security behaviour among higher education students in Malaysia. *Journal of Information Assurance and Security* 2017: 1–13.

Muronga, Khangwelo, Marlein Herselman, Adele Botha, and Adéle Da Veiga. 2019. An analysis of assessment approaches and maturity scales used for evaluation of information security and cybersecurity user awareness and training programs: A Scoping Review. In *2019 conference on next generation computing applications (NextComp)*, pp. 1–6. IEEE.

Nordstokke, David W., and Bruno D. Zumbo. 2010. A new nonparametric Levene test for equal variances. *Psicológica* 31 (2): 401–430.

Öğütçü, Gizem, Özlem Müge. Testik, and Oumout Chouseinoglou. 2016. Analysis of personal information security behavior and awareness. *Computers & Security* 56: 83–93.

Or-Meir, Ori, Nir Nissim, Yuval Elovici, and Lior Rokach. 2019. Dynamic malware analysis in the modern era—A state of the art survey. *ACM Computing Surveys (CSUR)* 52 (5): 1–48.

Parsons, Kathryn, Agata McCormac, Marcus Butavicius, Malcolm Pattinson, and Cate Jerram. 2014. Determining employee awareness using the human aspects of information security questionnaire

(HAIS-Q). *Computers & Security* 42: 165–176.

Paterson, Thomas, and Lauren Hanley. 2020. Political warfare in the digital age: Cyber subversion, information operations and 'Deep Fakes.' *Australian Journal of International Affairs* 74 (4): 439–454.

Pattinson, Malcolm, Marcus Butavicius, Kathryn Parsons, Agata McCormac, and Dragana Calic. 2015. Factors that influence information security behavior: An Australian web-based study. In *International conference on human aspects of information security, privacy, and trust*, pp. 231–241. Springer.

Payoneer | The Global Gig-Economy Index: Q2 2019. 2020. https:// explo re. payon eer. com/ q2_ global_ freel ancing_ index/. Accessed July 11.

Platt, Victor. 2012. "Still the fire-proof house? An analysis of Canada's cyber security strategy. *International Journal* 67 (1): 155–167.

Pramod, Dhanya, and Ramakrishnan Raman. 2014. A study on the user perception and awareness of smartphone security.

Rafiq, Ms Aamna. 2020. Issue brief on 'increasing cyber threats to Pakistan' | institute of stategic studies Islamabad. http:// issi. org. pk/ issue- brief- on- incre asing- cyber- threa ts- to- pakis tan/. Accessed July 10.

Ramalingam, Rajasekar, Shimaz Khan, and Shameer Mohammed. 2016. The need for effective information security awareness practices in oman higher educational institutions. arXiv: 1602. 06510.

Rao, Umesh Hodeghatta, and Umesha Nayak. 2014. *The Infosec handbook: An introduction to information security*. New York: Springer.

Salim, Asif, Noor Ullah Khan, and Muhammad Kaleem. 2019. Contemporary digital age and dynamics of E-Jihad in the Muslim World: Case study of Pakistan. *Pakistan Journal of Criminology* 11(4).

Sawaya, Yukiko, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. 2017. Self-confidence trumps knowledge: A cross-cultural study of security behavior. In *Proceedings of the 2017 CHI conference on human factors in computing systems*, pp. 2202–2214.

Schneier, Bruce. 2015. *Secrets and lies: Digital security in a networked world*. New York: Wiley.

Senthilkumar, K., and Sathishkumar Easwaramoorthy. 2017. A survey on cyber security awareness among college students in Tamil Nadu. *Materials Science and Engineering Conference Series* 263: 042043.

Shad, Muhammad Riaz. 2019. Cyber threat landscape and readiness challenge of Pakistan. *Strategic Studies* 39 (1): 1–19.

Sharif, Mahmood, Jumpei Urakawa, Nicolas Christin, Ayumu Kubota, and Akira Yamada. 2018. Predicting impending exposure to malicious content from user behavior. In *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, pp. 1487–1501.

Shi, Fei. 2015. Study on a stratified sampling investigation method for resident travel and the sampling rate. *Discrete Dynamics in Nature and Society*

Slusky, Ludwig, and Parviz Partow-Navid. 2012. Students information security practices and awareness.

Journal of Information Privacy and Security 8 (4): 3–26.

Solic, Kresimir, Mateo Plesa, Tena Velki, and Kresimir Nenadic. 2019. Awareness about information security and privacy among healthcare employees. Medicinski fakultet Osijek.

Spector, Paul E. 1992. A consideration of the validity and meaning of self-report measures of job conditions.

Staksrud, Elisabeth, Kjartan Ólafsson, and Sonia Livingstone. 2013. Does the use of social networking sites increase children's risk of harm? *Computers in Human Behavior* 29 (1): 40–50.

Stanton, Jeffrey M., Kathryn R. Stam, Paul Mastrangelo, and Jeffrey Jolton. 2005. Analysis of end user security behaviors. *Computers & Security* 24 (2): 124–133.

Štitilis, Darius, Paulius Pakutinskas, and Inga Malinauskaitė. 2017. EU and NATO cybersecurity strategies and national cyber security strategies: A comparative analysis. *Security Journal* 30 (4): 1151–1168.

Świątkowska, Joanna. 2020. Tackling cybercrime to unleash developing countries' Digital Potential.

Talib, Shuhaili, Nathan L. Clarke, and Steven M. Furnell. 2010. An analysis of information security awareness within home and work environments. In *ARES'10 international conference on availability, reliability, and security, 2010*, pp. 196–203. IEEE.

Titi, Khader Muspah. 2003. *Code of ethics, professionalism and responsibilities*. Ardhah, Jordan: AlAhliyyah Amman University.

Valcke, Martin, Bram De Wever, Hilde Van Keer, and Tammy Schellens. 2011. Long-term study of safe internet use of young children. *Computers & Education* 57 (1): 1292–1305.

Van der Merwe, Alta, Marianne Loock, and Marek Dabrowski. 2005. Characteristics and responsibilities involved in a phishing attack. In *Proceedings of the 4th international symposium on information and communication technologies*, pp. 249–254.

Velki, Tena, and Ksenija Romstein. 2019. User risky behavior and security awareness through lifespan.

International Journal of Electrical and Computer Engineering Systems 9 (2): 9–16.

Velki, Tena, and Krešimir Šolić. 2019. Development and validation of a new measurement instrument: The behavioral-cognitive internet security questionnaire (BCISQ). *International Journal of Electrical and Computer Engineering Systems* 10 (1): 19–24.

Velki, Tena, Kresimir Solic, V. Gorjanac, and K. Nenadic. 2017. Empirical study on the risky behavior and security awareness among secondary school pupils-validation and preliminary results. In

2017 40th international convention on information and communication technology, electronics and microelectronics (MIPRO), 1280–1284. IEEE.

Von Solms, Rossouw, and Suné Von Solms. 2015. Cyber safety education in developing countries. International Institute of Informatics and Systemics.

Vroom, Cheryl, and Rossouw Von Solms. 2004. Towards information security behavioural compliance.

Computers & Security 23 (3): 191–198.

Waheed, Moniza. 2019. Online threats and risky behaviour from the perspective of malaysian youths.

Wang, Zuoguang, Limin Sun, and Hongsong Zhu. 2020. Defining social engineering in cybersecurity. *IEEE Access* 8: 85094–85115.

Workman, Michael. 2007. Gaining access with social engineering: An empirical study of the threat.

Information Systems Security 16 (6): 315–331.

Zhang, Peiqin, and Xun Li. 2015. Determinants of information security awareness: An empirical investigation in higher education.

Zwilling, Moti, Galit Klien, Du.šan Lesjak, Lukasz Wiechetek, Fatih Cetin, and Hamdullah Nejat Basim. 2020. Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems* 62: 1–16.