

Challenges to Cyber Security Policy in Pakistan: A Critical Discourse



By

Zahra Michelle Khan

(Registration No: 00000401488)

Department of Strategic Studies

Centre of International Peace & Stability

National University of Sciences and Technology (NUST)

Islamabad, Pakistan

(2024)

Challenges to Cyber Security Policy in Pakistan: A Critical Discourse



By

Zahra Michelle Khan

(Registration No: 00000401488)

A thesis submitted to the National University of Sciences and Technology, Islamabad, in partial fulfillment of the requirements for the degree of

Masters in Strategic Studies

Supervisor: Dr. Rubina Waseem

Centre of International Peace & Stability

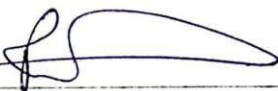
National University of Sciences and Technology (NUST)


Islamabad, Pakistan


(2024)

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS Thesis written by Ms. Zahra Michelle Khan (Registration No. 00000401488), of Centre of International Peace & Stability has been vetted by undersigned, found complete in all respects as per NUST Statutes/ Regulations/ Masters Policy, is free of plagiarism, errors, and mistakes and is accepted as partial fulfillment for award of Masters degree. It is further certified that necessary amendments, as pointed out by GEC members and foreign/ local evaluators of the scholar, have also been incorporated into the said thesis.

Signature: 
Name of Supervisor: Dr. Rubina Waseem
Date: _____

Signature (HoD): 
Date: _____

Signature (Dean/Principal): 
Date: _____

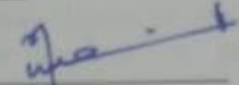
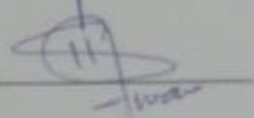
ASSOCIATE DEAN
Centre for International Peace and Stability
NUST Institute of Peace and Conflict Studies
Islamabad

National University of Sciences & Technology

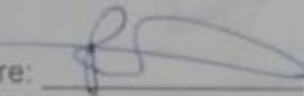
MASTER THESIS WORK

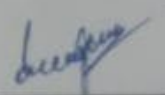
We hereby recommend that the dissertation prepared under our supervision by **Ms. Zahra Michelle Khan** & Regn no.00000401488 Titled: "Challenges to Cyber Security Policy in Pakistan: A Critical Discourse" be accepted in partial fulfillment of the requirements for the award of **MS Strategic Studies** degree and awarded grade _____ (Initial).

Examination Committee Members

1. Name: **Dr. Muhammad Makki** Signature: 
2. Name: **Dr. Humairah Shafi** Signature: 
3. Name: _____ Signature: _____

Supervisor's name: **Dr. Rubina Waseem**

Signature: 
Date: _____




Head of Department

Date

COUNTERSIGNED

Date: _____



Dean/Pi

ASSOCIATE DEAN
Centre for International Peace and Stability
1257 H-10/10-1, Islamabad
10000

FORM TH-1A
(MUST BE TYPE WRITTEN)

CERTIFICATE OF APPROVAL

This is to certify that the research work presented in this thesis, entitled "**Challenges to Cyber Security Policy in Pakistan: A Critical Discourse**," was conducted by Ms. Zahra Michelle Khan under the supervision of Dr. Rubina Waseem. No part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to the Department of Peace & Conflict Studies in partial fulfillment of the requirements for the degree of Master of Science in the Field of Strategic Studies, Centre of International Peace and Stability, National University of Sciences and Technology, Islamabad.

Student Name: Zahra Michelle Khan

Signature:  _____

Examination Committee:

a) External Examiner 1: Dr. Muhammad Makki

Signature:  _____

(Designation and Office Address) _____

b) External Examiner 2: Dr. Humaira Shafi

Signature:  _____

(Designation and Office Address) _____

Name of Supervisor: Dr. Rubina Waseem

Signature:  _____

Name of Dean/HOD: Dr. Ansar Jamil

Signature:  _____

AUTHOR'S DECLARATION

I, Zahra Michelle Khan, hereby state that my MS thesis titled "Challenges to Cyber Security Policy in Pakistan: A Critical Discourse" is my own work and has not been submitted previously by me for taking any degree from the National University of Sciences and Technology, Islamabad or anywhere else in the country/ world.

At any time if my statement is found to be incorrect even after I graduate, the university has the right to withdraw my MS degree.

Name of Student: Zahra Michelle Khan

Date: 08/18/2024

PLAGIARISM UNDERTAKING

I solemnly declare that the research work presented in the thesis titled "Challenges to Cyber Security Policy in Pakistan: A Critical Discourse" is solely my research work with no significant contribution from any other person. Small contribution/ help wherever taken has been duly acknowledged and that complete thesis has been written by me.

- I understand the zero tolerance policy of the HEC and National University of Sciences and Technology (NUST), Islamabad towards plagiarism. Therefore, I as an author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used
- as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of MS degree, the University reserves the rights to withdraw/revoke my MS degree and that HEC and NUST, Islamabad has the right to publish my name on the HEC/University website on which names of students are placed who submitted plagiarized thesis.

Student Signature:  _____

Name: Zahra Michelle Khan

Date: 18/08/2024

DEDICATION

Dedicated to Taaha, my best friend and twin flame, and my beautiful pets Josephine Joestar and Sandy Mc. Sanderson.

To anyone who feels like they can't do it, you can. Write that thesis, one page at a time. Know that everything you need to make your dreams come true is already within yourself. You just have to find it. You do not fear. You do not falter. You do not yield.

ACKNOWLEDGEMENTS

Writing is perhaps the greatest of human inventions, binding together people who never knew each other, citizens of distant epochs. Books break the shackles of time. A book is proof that humans are capable of working magic.

- Carl Sagan, Cosmos

If I were to acknowledge everyone who made this thesis possible, the acknowledgments alone would be larger than the research. For a product of my intelligence is never truly mine; it's an amalgamation of every person I've ever met who imparted knowledge to me. From the first moments when my soul was created and God blessed it with the ability to rationalize, to strangers who taught me lessons that would always be a part of who I am. To start off with the acknowledgments, I'm grateful to anyone who's ever dared to contribute to knowledge since the beginning of time. Humans don't exist in solitude. We carry the legacy of those before us, building from their ideas and knowledge, just as they will do from mine in the future.

In terms of academics, my biggest gratitude lies with my supervisor, Dr. Rubina Waseem, who is everything a person can hope for in a supervisor. It is rare to find teachers who adjust to neurodivergent work processes and see you for your potential, not your ability to stick to schedules. And to my co-supervisors, Dr. Humaira Shafi and Dr. Muhammad Makki, who've been inspirational in every meaning of the word. Part of the reason why my research is as good as it is was because I wanted to make them proud. However, outside of my thesis committee, the biggest possible contribution is owed to Prof. Dr. Tughral Yamin, the person who taught cybersecurity so well that it became the heart of my thesis.

Yet academics are only one side of research. My friends deserve equal praise for keeping me motivated and supported enough to have achieved this milestone. My best friend Taaha, 'half of my soul' as the poets would say. The better half, if you ask me. I could never have done it without you because you're the person who first heard the idea and believed in me enough to help make it happen. My other best friend, Ismah, is the reason my proposal was submitted in the first place. You have a way with words that bring out the human aspect in any research, a trait academia needs more of. You're the soul of my research, and it wouldn't have been the same without you. And, of course, Hashir, my baby brother, who has always stepped up in crisis.

I suppose it takes a village to write a thesis because it took one to shape the person who wrote it. God, my biggest ally, you've been kind enough to let me achieve anything I set my mind to, and I hope you feel this kind towards me for decades to come. But it is the poets, the writers, and the artists to whom I owe my soul. Van Gogh, for teaching me the meaning of painting my thesis in my own brand of yellow; Wilde for the wit and charisma that makes my writing style so interesting; Kafka for sharing the sentiment of solitude needed to produce the work I know to be my best; and Dostoevsky, for giving me hope that this heavy feeling is a sign of intelligence. Lastly, I acknowledge Sarah J. Mass for penning the character Nesta Archeron, a mirror of myself, that enabled me to climb this mountain - and climb I did.

Table of Contents

LIST OF TABLES	XIII
LIST OF SYMBOLS, ABBREVIATIONS, AND ACRONYMS	XIV
Abstract	XVI
Chapter 1	1
INTRODUCTION	1
1.1 Hypothesis	3
1.2 Research Objectives	3
1.3 Research Questions	4
1.4 Theoretical Framework	4
1.4.1 The Theory of Securitization	5
1.4.2 Integrated-System Theory	7
1.5 Research Methodology	8
1.5.1 Method of Research	9
1.5.2 Research Design	9
1.5.3 Data Collection	10
1.5.4 Data Analysis	10
1.6 Literature Review	10
1.6.1 Cybersecurity and Cyberspace	11
1.6.2 Threats to Cyber Security	12
1.6.3 Cyber Security Policy in Pakistan	14
1.7 Organization of Study	15
Chapter 2	17
CONCEPTUALIZATION AND LITERATURE REVIEW	17
2.1 Defining Cyber Security	17
2.1.1 Defining Cyber Security Via Existing Literature	19
2.1.2 Why A Proper Definition is Essential	20
2.2 Cyber Security Policy	21
2.2.1 Government and International Perspectives	22

2.2.2 Formulating Effective Cybersecurity Policies _____	23
2.3 Cyber Security Landscape in Pakistan _____	26
2.3.1 Cyberattacks and Cybercrime _____	28
2.4 Literature Gap _____	29
Conclusion _____	30
Chapter 3 _____	31
TRENDS AND PATTERNS OF CYBER SECURITY FORMATION _____	31
3.1 Introduction to Key International Cybersecurity Standards _____	32
3.2 Examination of Frameworks from Leading Cybersecurity Nations _____	34
3.2.1 The United States Cybersecurity Framework _____	34
3.2.2 Singapore’s Strategic Cybersecurity Measures _____	35
3.2.3 Israel’s Cybersecurity Innovation and Collaboration _____	36
3.3 A Cross-National Comparison: Pakistan’s Preparedness and Global Practices _____	37
3.3.1 International Cybersecurity Alignment: Successful Practices from Around the Globe 38	
3.4 Collaboration between State and Public Cybersecurity Efforts _____	41
3.4.1 Global Best Practices in Public-Private Partnerships _____	42
3.5 Opportunities for Pakistan to Enhance Public-Private Collaboration _____	46
Conclusion _____	47
Chapter 4: _____	48
CHALLENGES TO CYBER SECURITY POLICY FORMATION _____	48
4.1 Background _____	48
4.2 Challenges to Cyber Security Policy Formation _____	50
4.2.1 Global Level _____	50
4.2.2 State Level _____	53
4.2.3 Implementation Level _____	55
4.3 Challenges Unique to Pakistan’s Cybersecurity Landscape _____	57
4.3.1 Critical Infrastructure _____	58
4.3.2 Establishment of CERTs _____	59
4.3.3 Regional Framework _____	60

4.3.4	Multi-Level Approach	60
4.3.5	Precautionary Measures	61
4.3.6	Cyber-Defense Prioritization	61
	Conclusion	62
Chapter 5:		63
CONCLUSIONS		63
5.1	Analysis of Research Findings	64
5.1.1	Verification of Hypothesis	65
5.2	Existing Policies and Frameworks	66
5.3	Current Threats and Vulnerabilities	67
5.4	Stakeholder Analysis	68
5.5	Planning Stages for a Sound Cybersecurity Policy	69
5.5.1	Defining Objectives and Goals	69
5.5.2	Conducting Risk Assessments	71
5.6	Framework for Cybersecurity Policy Development	72
5.6.1	Governance Structure	72
5.6.2	Cybersecurity Laws	74
5.6.3	Policy Components	76
5.7	Implementation Strategies	79
5.7.1	Resource Allocation	79
5.7.2	Capacity Building and Training	79
5.7.3	Public Awareness and Education	80
5.7.4	Technology and Innovation	80
5.8	Monitoring and Evaluation	81
5.8.1	Continuous Improvement Mechanisms	82
	Conclusion	83
BIBLIOGRAPHY:		85

LIST OF TABLES

1.0	Key Performance Indicators (KPIs) Used Worldwide	79
-----	--	----

LIST OF SYMBOLS, ABBREVIATIONS, AND ACRONYMS

AI	Artificial Intelligence
CERT	Computer Emergency Response Team
CISCP	Cyber Security Information Sharing Partnership
CSA	Cybersecurity and Security Agency
DBIR	Data Breach Investigations Report
DDoS	Distributed Denial of Service
FBI	Federal Bureau of Investigation
FBR	Federal Board of Revenue
FFIEC	Federal Financial Institutions Examination Council
GDPR	General Data Protection Regulation
HSD	Hague Security Delta
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IFTA	Investigation for Fair Trial Act
INCD	Israel National Cyber Directorate
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITU	International Telecommunication Union
KISA	Korea Internet & Security Agency
KPI	Key Performance Indicator
ML	Machine Learning
NADRA	National Database and Registration Authority
NATO	North Atlantic Treaty Organization

NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PECA	Prevention of Electronic Crimes Act
PKCERT	Pakistan Computer Emergency Response Team
PPP	Public-Private Partnership
PTA	Pakistan Telecommunication Authority

Abstract

The growing digitization of the world and the development of information and communication technology in cyberspace have exposed states to a plethora of cyber threats. With its current ranking at 79 out of 183 states on the Global Cybersecurity Index, Pakistan is vulnerable to cyber security threats that can impact its national security. Although it introduced the National Cyber Security Policy in 2021, the implementation of cybersecurity practices is lacking. The gaps in Pakistan's cyber security culture have made it difficult to securitize cyberspace and prevent vulnerabilities to non-traditional cyber threats.

The main issue to be addressed is how cybersecurity policy is formatted in Pakistan and what factors hinder the formation, development, and execution of a sound policy. It compares recent cybersecurity efforts such as the National Cybersecurity Policy of 2021 and the PTA Cybersecurity Strategy 2023-2028. These domestic policies are analyzed against international frameworks such as NIST, GDPR, and more, with a focus on the ways in which other developed and developing states have aligned their respective policies.

Using a qualitative approach, this research is exploratory in nature and focuses on data collection via stakeholder interviews and literature analysis. The stakeholders include cybersecurity officials, cybersecurity operatives, students of cybersecurity, and hackers, ethical and non-ethical. This research aims to address the challenges to cyber security policy in Pakistan and draw upon the ways in which policymaking for this sector can be improved.

Keywords: Cybersecurity Policy, Cyber threats, Information and communication technology, National security, Non-traditional cyber threats, Pakistan

Chapter 1

INTRODUCTION

In the past few decades, the unprecedented and relentless advancement of technology and information systems has plunged states into an era of enhanced digital transformation. This has also increased the dependence of states on cyberspace for various aspects of public and private affairs. Since information and communication technologies constitute a social aspect of national power, they must be protected against threats.¹

The increasing reliance on the digital sphere has exposed governments, businesses, and individuals to a growing array of cybersecurity threats characterized by both their frequency and sophistication. The concept of "cybersecurity" has arisen as a pivotal concern, serving as a linchpin in the stability and functionality of modern societies. As the global awareness of cybersecurity threats increases, states and international communities are presented with the challenge of crafting comprehensive cybersecurity policies that protect their national interests and state critical infrastructure within an ever-changing and dynamic cyberspace landscape.²

Cybersecurity, a multifaceted and dynamic domain, consists of strategies, technologies, practices, and education constructed to protect internet-reliant systems from security challenges. This is essential to protect the confidentiality, availability, and credibility of information systems that have

¹ Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, *Cyberpower and National Security* (University of Nebraska Press: Potomac Books, 2009), 24.

² Jawad Hussain Awan et al., "Security of EGovernment Services and Challenges in Pakistan," *2016 SAI Computing Conference (SAI)*, July 13, 2016, 1082–85.

become an integral aspect of statecraft and bureaucratic functioning.³ A multitude of cybersecurity threats, spanning cybercrime and espionage to state-backed cyber assaults, present substantial risks to nations, and the outcomes of successful cyber breaches can range from financial losses to geopolitical tensions.

Despite recognizing cybersecurity as a pressing global concern, there is no universally accepted definition of the term. Since there is no singularly agreed-upon definition, states tend to interpret it differently, resulting in challenges when formulating comprehensive cybersecurity policies. The lack of a standardized definition can be attributed to the diverse interpretations of what constitutes a "cybersecurity threat" and how each state faces a different set of cybersecurity threats based on the vulnerabilities open for exploitation. Nevertheless, it is imperative for governments to establish a clear understanding of cybersecurity to effectively address the associated challenges.

As these threats impact cybersecurity in various states, the same applies to Pakistan, the case at hand. In the last decade alone, Pakistan has increased its internet base with over 130 million broadband subscribers and a 54.48% penetration.⁴ In the year 2021, the Federal Investigation Agency received about 102,000 cyber-crime-related complaints.⁵ However, in the recent year of 2023, the use of cyber-threats for political exploitation, such as the wire-tapping of the Prime

³ Myriam Dunn Cavelty and Andreas Wenger, "Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science," *Contemporary Security Policy* 41, no. 1 (October 14, 2019): 5–32.

⁴ Pakistan Telecommunication Authority, "Telecom Indicators | PTA," Pta.gov.pk, 2023, <https://www.pta.gov.pk/en/telecom-indicators>.

⁵ Haiqa Khan, "Navigating Pakistan's Digital Revolution: Cybercrimes, Reporting, and Safeguarding," *The Friday Times*, August 19, 2023, <https://thefridaytimes.com/19-Aug-2023/navigating-pakistan-s-digital-revolution-cybercrimes-reporting-and-safeguarding>.

Minister's office⁶ and leaking of confidential documents and conversations, all point to the ever-lacking cybersecurity landscape in the state.

Although there are cyber security measures in place, such as the Pakistan Telecommunication (Re-Organization) Act 1996, Electronic Transaction Ordinance 2002, Investigation for Fair Trial Act (IFTA) 2013, Prevention of Electronic Crime Act (PECA) 2016, and the National Cyber Security Policy 2021, they do not capture the reality of the challenges to cyber security in Pakistan. There are many factors that impact cyber security policy development in the state, but the most apparent one would be the lack of preparedness and critical infrastructure to support legislative endeavors on the subject. This research looks to analyze the existing cyber security policy of Pakistan, compare it to the policies of other states, highlight challenges to policy formation, and develop recommendations to promote better cyber security policy in the state.

1.1 Hypothesis

A comprehensive cyber security policy can address the upcoming security challenges to Pakistan.

1.2 Research Objectives

- To determine the challenges to Pakistan's cyber security policy
- To highlight how a comprehensive cyber security policy can be drawn

⁶ Syed Irfan Raza, "Leaks Reveal Massive Breach in Security at PM Office," Dawn, September 26, 2022, <https://www.dawn.com/news/1712044>.

- To explore the impact a comprehensive cyber security policy will have on Pakistan

1.3 Research Questions

1. What are the challenges to cyber security policy in Pakistan?
2. What factors play an important role in making a comprehensive cybersecurity policy?
3. What impact will a comprehensive cyber security policy have?

1.4 Theoretical Framework

Since the past decade, cybersecurity has become such an important strategic field that states try their best to accumulate the most gains and securitization at the same time. However, with the changing threats to national security, the rise of the non-traditional security sector, and increased dependence on cyberspace, it is essential to theorize the impact of cyber security on a state level and how it subsequently impacts policy-making in the relative field.

This study is supported by the Securitization Theory of the Copenhagen School, along with a plethora of management and organizational theories to understand how the cyber threat should be addressed. Combining the two helps understand what the cyber threat is and how to actively address it in the form of a comprehensive cyber security policy.

1.4.1 The Theory of Securitization

As the security threats of the decade continue to grow into the non-traditional realm and new facets and security challenges to states surface, the Copenhagen School sheds light on what securitization is and how new threats impact security. Barry Buzan's theory of national security⁷, as outlined in his book "People, State, and Fear," provides a valuable framework for analyzing the research topic.

Buzan's theory expands the traditional view of security beyond military concerns to encompass multiple sectors and threats. It includes five sectors: military, political, economic, societal, and environmental security. Applying Buzan's theory to the research topic, we can gain a deeper understanding of the multifaceted challenges Pakistan faces in the realm of cyber security.⁸ It also addresses whether cyber-security threats can impact securitization since they meet the criteria outlined by Buzan that if the problem is not tackled, then everything else will be irrelevant as it has the ability to extensively impact the well-being of the state.⁹

1. Military Security:

In the context of cyber security, military security pertains to the protection of Pakistan's military infrastructure and communication systems. Cyberattacks on military systems can have severe national security implications. The research will investigate the vulnerabilities and challenges that

⁷ Barry Buzan, *People, States & Fear: An Agenda for International Security Studies in the Post-Cold War Era* (Colchester: Ecpr Press, 1983).

⁸ Muhammad Riaz Shad, "Cyber Threat Landscape and Readiness Challenge of Pakistan," *Strategic Studies* 39, no. 1 (April 24, 2019): 1–19.

⁹ Barry Buzan, Ole Waever, and Jaap de Wilde, "Security: A New Framework for Analysis," *International Journal* 53, no. 4 (1998).

Pakistan's military faces in securing its cyber infrastructure. This may include threats from rival nations and non-state actors and the measures taken to protect military assets from cyberattacks.

2. Political Security:

Political security, according to Buzan, involves the stability and continuity of the state. In the context of cyber security, it helps one to understand cyber threats can destabilize Pakistan's government and political institutions. This includes potential threats to the integrity of elections, disruption of government operations, and attacks on critical infrastructure.

3. Economic Security:

Cybersecurity is closely linked to economic security. In Pakistan, a growing digital economy is at risk from cyber threats that could disrupt financial systems, compromise intellectual property, and harm trade and economic growth. Applying Buzan's theory explains how challenges to cyber security can affect economic stability and growth. This includes exploring the vulnerabilities in Pakistan's financial sector, trade networks, and intellectual property protection.

4. Societal Security:

Societal security is about protecting the well-being of the population. In the context of cyber security, this means safeguarding citizens from cybercrimes, identity theft, and the misuse of personal data. Challenges to cyber security can impact the everyday lives of Pakistani citizens, which, according to Buzan, is just as important to the state's security. This includes privacy concerns, the spread of disinformation, and the psychological impact of cyber threats.

5. Environmental Security:

Environmental security, under the Securitization Theory, involves the protection of the environment and resources of the state. When looked at through a cyber security lens, it means safeguarding the power grids, water supply systems, and other elements of critical infrastructure from cyberattacks. It can also be used to explain how environmental security is at risk if the critical infrastructures mentioned above are hacked into and tampered with. This can also be used to instigate instances of environmental and biological warfare.

By applying Buzan's theory of national security to the study of cyber security policy in Pakistan, the research can offer a holistic view of the challenges faced by the nation in the absence of a proper cyber security policy. It emphasizes the interconnectedness of these security sectors and highlights the need for a comprehensive approach to address the complex cyber security issues in a nation like Pakistan. This framework enables a deeper and more nuanced understanding of how challenges in the cyber domain can have far-reaching implications for Pakistan's overall security and well-being.

1.4.2 Integrated-System Theory

Initially proposed for informational security management, the Integrated System Theory was recently highlighted by Hong, Chi, Chao, and Tang in their paper ‘An Integrated System Theory for Information Security Management.’¹⁰ It combined the approaches of security policy theory, risk management theory, control and auditing theory, management system theory, and contingency theory to explain how information security can be better understood with scope for strategies and

¹⁰ Kwo- Shing Hong et al., “An Integrated System Theory of Information Security Management,” *Information Management & Computer Security* 11, no. 5 (December 2003): 243–48.

policy construction. Although the approach covers the impact of information security on organizations, it can be extended to cybersecurity at the state level.¹¹

Much like information security, cyber security is also highly dependent on information and communication technologies and the rapid digitalization of the world. It is also equally misunderstood when seen as a security threat, especially at a national security level. This approach helps bridge the dissonance in cyber security policy making where the political aspect of the threat is not analyzed under the scientific and management aspects of it. Cybersecurity is a multidisciplinary field that is meant to be understood using a combination of scientific, political, and management studies lens.¹²

1.5 Research Methodology

Research can vaguely be defined as choosing a specific topic and conducting a scientific and systemic search on it. Research methodology, however, is based on several procedures, techniques, and schemes that make research more objective and unbiased.¹³ The use of a proper methodology, especially in social sciences, helps remove biases to the best of a researcher's ability.

The methodology for this research is as follows:

¹¹ Kateryna Chyzhmar et al., "State Information Security as a Challenge of Information and Computer Technology Development," *Journal of Security and Sustainability Issues* 9, no. 3 (March 25, 2020): 819–28.

¹² Reeshad S. Dalal et al., "Organizational Science and Cybersecurity: Abundant Opportunities for Research at the Interface," *Journal of Business and Psychology* 37, no. 1 (February 4, 2021).

¹³ Donald Polkinghorne, *Methodology for the Human Sciences : Systems of Inquiry* (Albany: State University Of New York Press, 1983), 273.

1.5.1 Method of Research

The research method chosen is qualitative research. Qualitative research focuses on the data-centric approach and works to find explanations of hidden meanings and multiple perspectives. It allows participants to become the dominant representation of the topic rather than simply compacting the data into depersonalized descriptions that do not have any social interaction and human experiences in the larger cultural context.¹⁴

Qualitative research is the chosen methodology for this study because it enables a deep exploration of the subject matter. It allows for an in-depth understanding of the challenges faced by Pakistan's cyber security policy by capturing the rich experiences and insights of key informants.

1.5.2 Research Design

Research design helps make research more logical and gives it structure; keeping this in mind, the design for this topic exploratory in nature. An exploratory research design focuses on formulating a research problem for a more precise and comprehensive understanding of the subject.¹⁵ This approach is well-suited to investigate a complex and relatively underexplored topic like the challenges to cyber security policy in Pakistan.

¹⁴ Patricia A. Adler, Peter Adler, and Robert S. Weiss, "Learning from Strangers: The Art and Method of Qualitative Interview Studies," *Contemporary Sociology* 24, no. 3 (May 1995): 420.

¹⁵ Ranjit Kumar, *Research Methodology: A Step-By-Step Guide for Beginners*, 5th ed. (London: Sage, 2019).

1.5.3 Data Collection

In-depth interviews will be the primary data collection method. The research will involve semi-structured interviews with a purposive sample¹⁶ of key stakeholders involved in cyber security policy in Pakistan. These participants may include government officials, cybersecurity experts, legal experts, and industry professionals. The interviews will be open-ended, encouraging participants to provide detailed insights into the challenges they perceive and the strategies they employ to address them.

1.5.4 Data Analysis

The research focuses on the state-level analysis of cyber security policy in Pakistan. This means that the study will examine how challenges are perceived and managed within the context of the Pakistani state. Data gathered from the in-depth interviews will be analyzed using thematic analysis. This process involves identifying recurring themes, patterns, and relationships in the qualitative data. The analysis will aim to construct a nuanced understanding of the challenges faced by Pakistan's cyber security policy

1.6 Literature Review

Although the literature available on challenges to cyber security policy in Pakistan is scarce, plenty of work has been done on cybersecurity, its challenges, and future prospects. Western academicians have undertaken similar topics in regard to cyber security policy formation in the

¹⁶ Sarah Curtis et al., "Approaches to Sampling and Case Selection in Qualitative Research: Examples in the Geography of Health," *Social Science & Medicine* 50, no. 7-8 (April 2000): 1001–14.

U.S., E.U., and other regions. The given literature is arranged thematically from a broader scope to a more specific understanding, making use of theories of cyberspace, cyber security threats to states and Pakistan, cyber security policy formulation, and challenges.

1.6.1 Cybersecurity and Cyberspace

The term ‘cyber’ is highly contested and often used interchangeably with ‘internet,’ which should not but rather be seen as the command and control of the computer systems.¹⁷ According to Binxing Fang, cyberspace should be seen as a time-dependent set of connected information systems that human beings use to communicate and interact.¹⁸ However, a threat to the security of such a cyber-space could not encompass why it is a matter of national security. Expanding the traditional idea of cyberspace to Roscini’s definition¹⁹, we can add telecommunications, command systems, embedded processors, and many offline modes of communication as part of it.

Based on this, cyber-threats would encompass an attack or breach of the aforementioned computer systems, whether to bring harm to the systems and their users or to exploit the data from the systems. If you categorize them based on intention and the actor posing the danger, cyber threats can consist of cybercrime, cyberterrorism, cyberwar, cyberespionage, and almost everything in between. Therefore, cyber-security, in the words of Bayuk et al. is seen as the *technologies, methods, and practices in place to safeguard, detect, and recover from damage based on the confidentiality, integrity, and availability of information in cyberspace*. An understanding of the

¹⁷ Andrew Fetter, “Is Trident Safe from Cyber Attack?,” 2016, <https://www.europeanleadershipnetwork.org/wp-content/uploads/2017/10/Is-Trident-safe-from-cyber-attack-1.pdf>.

¹⁸ Binxing Fang, *Cyberspace Sovereignty : Reflections on Building a Community of Common Future in Cyberspace* (Singapore: Springer ; Beijing, China, 2018), 3.

¹⁹ Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press, 2014), 6.

terms and incidents in cyber-security culture, along with a universally agreed-upon definition for them, is essential when drafting a comprehensive policy.

Cyber-attacks tend to target the critical infrastructure of a state, as it has the most potential for causing damage.²⁰ The most important sectors of critical infrastructure consist of information and communication, the finance sector, energy and food production, transportation networks, and human services. The vulnerability of these areas is also highlighted under the sectors of national security mentioned by Barry Buzan as military, political, economic, societal, and environmental security.

Attacking the communication systems and roads via a cyber attack could impact the state during an armed conflict when mobilizing forces; targeting the food and energy production centers as well as the financial sectors can cause a political and economic crisis; similarly, hacking into the computerized systems at hydro plants, industries, and other such institutions can initiate a natural disaster that affects the environmental security of the state.

1.6.2 Threats to Cyber Security

Depending on the level of cyber-dependence of states, the threat to cyber security can vary. For a state like the U.S., where broadband proliferation is 94% in urban areas and over 60% in rural areas, cybersecurity threats encompass both state and daily-level events. However, along with cyberspace proliferation, states like the U.S. have developed their cyber security measures and

²⁰ Tughurl Yamin, "Cyberspace Management in Pakistan," *Governance and Management Review* 3, no. 1 (2018): 46–61.

critical infrastructure to be better protected against the threat from rogue states, non-state actors, or even individual hackers.²¹

Since communication systems are so complex yet painstakingly simple at the same time, a majority of actors ranging from freelancers, terrorists, and fringe groups to the kid in the basement could pose a threat to state institutions, critical infrastructure, and security sectors.²² If these threats are left unchecked, then they can pose a serious risk to the sovereignty of Pakistan.²³

These threats can either be prevented or dealt with once they occur. The prevention of cyber security threats comes under cyber-security readiness and strategies to protect information systems against foreign attacks.²⁴ However, once the attack occurs, it is essential for the state to have CERTs, solutions, and strategies in place to identify the attack, stop it in time, and recover any lost information or tampering in the information system.

Threats to cyber security in Pakistan were first taken seriously when the US National Security Agency (NSA) stole confidential information, and the state was plunged into a state of vulnerability.²⁵ According to the International Telecommunication Union's Global Cybersecurity

²¹ Matthew Crosston, "Virtual Patriots and a New American Cyber Strategy: Changing the Zero-Sum Game," *Strategic Studies Quarterly* 6, no. 4 (2012): 100–118.

²² Tughlur Yamin, "Cyberspace Management in Pakistan," *Governance and Management Review* 3, no. 1 (2018): 46–61.

²³ Muhammad Imad Ayub Khan, "Cyber-Warfare: Implications for the National Security of Pakistan.," *NDU Journal* 33 (2019): 117–32.

²⁴ Muhammad Riaz Shad, "Cyber Threat Landscape and Readiness Challenge of Pakistan," *Strategic Studies* 39, no. 1 (April 24, 2019): 1–19.

²⁵ Jawad Hussain Awan et al., "Security of EGovernment Services and Challenges in Pakistan," *2016 SAI Computing Conference (SAI)*, July 13, 2016, 1082–85.

Index of 2020, Pakistan ranked 79th out of 183 countries.²⁶ This was twelve places lower than its rank of 67th in 2017. Its belligerent neighbor India, on the other hand, ranked 10th, showing a clear disproportionality in cybersecurity between the two states. Similarly, the Cold Start doctrine of India includes cyber-attacks as a type of unconventional tactic in warfare. Along with these threats to state existence, Pakistan has time and again faced cyber attacks on private and public banks, state institutions, and bureaucratic offices. In terms of malware attacks, it has some of the highest incident rates in the region, showing that cyber threats exist on an individual, societal, and state level.²⁷

1.6.3 Cyber Security Policy in Pakistan

Policymaking in Pakistan tends to be reactive more than proactive, and the state's cybersecurity policy is no exception to this. Khan and Awar discuss how the cybersecurity regulations of the state evolved from protection against financial theft online through the Electronic Crimes Act (2002) to safeguarding citizen rights via the Prevention of Electronic Crimes Act (2016).²⁸ They discussed how regulations regarding cyber-security in Pakistan often lack implementation as the sectors it has been drafted for are not as tech-advanced as it is claimed on paper. Although preventive and response strategies may be made, without the proper infrastructure and personnel, it is wasted since it can't be used properly.

²⁶ International Telecommunication Union, "Global Cybersecurity Index 2020" (Geneva: ITU Publications, 2020).

²⁷ Muhammed Fahim Khan and Aamer Raza, "Cybersecurity and Challenges Faced by Pakistan," *Pak. Journal of International Affairs* 4, no. 1 (2021).

²⁸ Umair Parvaiz Khan and Muhammad Waqar Khan, "Cybersecurity in Pakistan: Regulations, Gaps and a Way Forward," *Cyberpolitik* 5, no. 10 (2020).

In her article ‘Challenges of Securitising Cyberspace in Pakistan,’ Aamna Raqif argues that due to the multiple variables that institutions in Pakistan tackle at the same time, a proper cyber security policy is never drafted.²⁹ She highlights how the influence of the audience, legislation by the state vs. the nation, and various other aspects challenge the creation of a policy or framework that aptly addresses challenges to cybersecurity in Pakistan. Similarly, Sara Ahmed critiques that although Pakistan presented a National Cyber Security Policy in 2021, its implementation is heavily reliant on the state’s flexibility with cyber-security strategies and highlights the importance of international cooperation to securitize cyberspace.³⁰

From the aforementioned studies, there is a gap in the literature where cyber security policymaking in Pakistan has not been directly addressed. Even when the cyber security policies are scrutinized, they have not been done via an inter-disciplinary lens and have failed to look into the factors that affect the construction of a comprehensive cyber security policy. This research looks to use these lacunae and identify how a more comprehensive cyber security policy can be made for Pakistan to help it combat the upcoming security challenges.

1.7 Organization of Study

The first chapter of the study will be the introduction, which focuses on the reason for conducting the research and the methodology used. It will look to explain the aims and objectives of the

²⁹ Aamna Rafiq, “Challenges of Securitising Cyberspace in Pakistan,” *Strategic Studies* 39, no. 1 (April 24, 2019): 90–101, <https://doi.org/10.53532/ss.039.01.00126>.

³⁰ Sara Ahmed, “Cyber Security Threat and Pakistan’s Preparedness: An Analysis of National Cyber Security Policy 2021,” *Pakistan Journal of Humanities and Social Sciences Research* 5, no. 1 (June 30, 2022): 25–40.

research and apply the *Theory of Securitization* and the *Integrated System Theory* to challenges to cybersecurity policymaking in Pakistan. It will also contain a literature review that will identify the existing trends of study on the topic, identify the gaps in the literature, and set the scope for the research.

The second chapter will look into Pakistan's cyber security policy landscape and the challenges to making a comprehensive policy. It will analyze important documents such as the National Cyber Security Policy of 2021 and draw out its shortcomings whilst incorporating the knowledge accumulated by policy experts and stakeholders on the topic. It will then identify the challenges to cyber security in the state.

Many factors that contribute to crafting a comprehensive cybersecurity policy will be highlighted in the third chapter of the research. It will also encompass what the impact of a good policy will be on the national security of the state. This chapter will make use of the information collected via interviews and other data collection methods.

Lastly, the final chapter of the research will give recommendations on how to make a sound cybersecurity policy for Pakistan. It will consist of everything from the planning stages to implementation and ways in which Pakistan's cybersecurity culture can be enriched. The given solutions will be limited to the scope of the study and understanding of the researcher, but they will draw on input from various stakeholders across multiple disciplines for better representation.

Chapter 2

CONCEPTUALIZATION AND LITERATURE REVIEW

One of the most critical aspects of addressing the challenges to cyber security policy is to define what cyber security is and what cyber security policy entails. A proper conceptualization of the terms helps one understand how to incorporate this sphere of national security into our greater national security strategy. This chapter focuses on defining cyber security and arranging the studied literature in a thematic way for better analysis.

Cyber security is defined as the “*measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.*” under the Merriam-Webster dictionary. Although this definition is concise, it overlaps with definitions of information security, IT security, and similar terms. This leads to the existing issue of the thoughtless use of the term cyber security and its implications on the literature that stems from it.

Since cyber security is multidisciplinary and involves aspects of technology, information security, management, policy-making, and national security, to name a few, the definition of the term is also flexible, depending on how it is being used. This literature review aims to help define cyber security and conceptualize it whilst looking into the cyber security landscape in Pakistan and how cyber security policymaking has been studied over the years.

2.1 Defining Cyber Security

The term 'cyber' is a subject of ongoing debate, often used interchangeably with 'internet' and similar other terms. Before being able to define cyber security, it is essential to understand what

‘cyber’ refers to and how it impacts the broader definition. According to Andrew Futter, *“it should be distinguished as the command and control of computer systems.”* The area or medium in which this is practiced is commonly referred to as cyberspace.

Cyberspace is a network of computers and devices created by mankind to facilitate communication and information-sharing infrastructure. Cavalry notes that it is often mistaken for the ‘internet’, but in reality, the internet is just a component of cyberspace not cyberspace as a whole. The working definition of cyberspace by Lorentz and Ottis is *“cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems.”* Although it is an integral part of communications, there is no commonly agreed-upon definition of cyberspace.

With the advancements in cyberspace, new stakeholders have become involved in its security, e.g., states, non-state actors, local governments, individuals, etc. When discussing the definition of cyber security, it is essential to understand that this definition is influenced by who the stakeholders in question are and what they’re trying to protect. On the surface level, cyber security can be seen as *“measures taken to protect cyberspace and all that it encompasses.”* but this definition does not address to what extent and from what threats.

According to the International Telecommunications Union:

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user’s assets. Organization and user assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in

the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- *Availability*
- *Integrity, which may include authenticity and non-repudiation*
- *Confidentiality*

In the context of this research, cyber security is seen in regard to the threat to the sovereignty of the state, its socio-political functioning, and national security. To further understand it, we take a look at the dominant cyber security legislature in various states of the international system and compare how the terms have been used.

2.1.1 Defining Cyber Security Via Existing Literature

In their study, Falessi et al. proposed that there is no commonly agreed-upon definition of cyber security in EU legislation as the term is often used in a broad application³¹. The EU's use of cyber security focuses on protecting information systems against any unauthorized breach and the ways in which it can be prevented and countered in the face of an incident. This is shared by Fuster & Jasmontaite, who studied EU cyber security legislation and drew upon the lack of coherence in its policies.³² Another author who shares a similar view is Wamala, who believes that cyber security

³¹ N. Falessi et al., "National Cyber Security Strategies: An Implementation Guide," Heraklion, 2012, <https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide>.

³² G. G. Fuster and Lina Jasmontaite, "Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights," in *The Ethics of Cybersecurity*, ed. M. Christen, B. Gordjin, and M. Loi (Springer Cham, 2020).

is a branch of information security.³³ He examined the uncertainty of the terminology used in EU policies and proposed a differentiation between the two. However, recent developments in EU legislature have shown that they have begun to opt for the term ‘cyber defense’ when it comes to state-level threats involving cyberspace and ‘cyber security’ at the organizational and enterprise level.³⁴

It is to be noted that most of the dominant cyber security literature, especially that which shapes the definition of the term, is Western and predominantly American. Cybersecurity has been a key area of U.S. national security since the early 1990s.³⁵ Russia has always been a key component in the US cyber security strategy as it is mostly concerned with state level espionage, information leaks and possible threat of physical attacks via compromised computer systems. Shively notes that in the recent years, the idea of US cyber security was mainly concerned about the state and how computer systems could be used to impact its sovereignty.³⁶ This view is what is most suitable to the scope of this research as well, since it deals with the challenges to Pakistan’s cyber security policy.

2.1.2 Why A Proper Definition is Essential

From an epistemic point of view, definitions of terms are essential as they influence the way knowledge about those terms is constructed. Without a proper definition for cyber security,

³³ F. Wamala, “ITU National Cybersecurity Strategy Guide,” 2011, <http://www.itu.int/ITUUD/%20cyb/cybersecurity/docs/itu-nationalcybersecurity-%20guide.pdf>.

³⁴ Artur Staszczuk, “European Parliament Position on EU Cyber Security and Defense Policy,” *Reality of Politics* 1, no. 10 (March 31, 2019): 122–33.

³⁵ Lawrence J. Trautman, “Cybersecurity: What about U.S. Policy?,” *Journal of Law, Technology and Policy* 1 (2015).

³⁶ Jacob Shively, “Cybersecurity Policy and the Trump Administration,” *Policy Studies* 42 (June 28, 2021): 1–17.

policymaking is already set up for failure. A good policy requires policymakers to define the parameters of the subject and suggest measures accordingly. If cybersecurity, information security, and information systems security are constantly confused and used interchangeably, then it would be fruitless to expect a policy that meets its objectives.

In a state like Pakistan where legislative measures for cyber-crime and information security are often left unimplemented due to loopholes in the definition and text of the policy, it is essential to be able to explain what cyber security is and how the policy for it will be implemented. A proper definition of the term will also enable states to persecute those who breach the cybersecurity of the state and potentially criminalize certain acts as well. Therefore, a proper definition of cybersecurity or a lack thereof has far-reaching consequences for policymaking.

2.2 Cyber Security Policy

Crafting effective cybersecurity policies requires knowledge of the history of cyber threats. The exponential growth of digital technologies has given rise to increasingly sophisticated threats, ranging from traditional malware to complex ransomware attacks and state-sponsored cyber espionage. Notably, scholars such as Chad Anderson argue that the cyber threat landscape is dynamic, and constantly adapting to technological advancements, which adds to the complexity of cyber security issues and, hence, poses challenges to policy-making.³⁷ Moreover, critical

³⁷ Chad Anderson, Richard L. Baskerville, and Mala Kaul, “Information Security Control Theory: Achieving a Sustainable Reconciliation between Sharing and Protecting the Privacy of Information,” *Journal of Management Information Systems* 34, no. 4 (October 2, 2017): 1082–1112.

infrastructure is closely linked with digital technologies, such as energy grids and financial systems, which further amplifies the potential impact of cyber threats (Buchanan, 2019).

In response to this evolving landscape, cybersecurity policies must adapt to address emerging threats. A study by Smith et al. (2020) emphasizes the importance of adopting a proactive approach, employing predictive analytics and threat intelligence to anticipate and counteract potential cyber threats, which is crucial considering the ever-changing nature of cyber threats. Furthermore, the integration of artificial intelligence (AI) and machine learning (ML) into cybersecurity frameworks is highlighted as a promising avenue for enhancing threat detection and response capabilities.³⁸

2.2.1 Government and International Perspectives

The role of government in shaping cybersecurity policy is paramount, as it establishes the legal and regulatory framework within which organizations operate. A comprehensive review of cybersecurity policies across different countries reveals a wide array of approaches, with variations in regulatory stringency, public-private collaboration, and incident response mechanisms.

In the United States, for instance, the National Institute of Standards and Technology (NIST) has been significant in developing cybersecurity frameworks that guide both public and private sector organizations.³⁹ The NIST Cybersecurity Framework places emphasis on a risk-based approach, encouraging organizations to assess and prioritize their cybersecurity measures based on potential

³⁸ Nachaat Mohamed, “Current Trends in AI and ML for Cybersecurity: A State-of-The-Art Survey,” *Cogent Engineering* 10, no. 2 (October 25, 2023).

³⁹ NIST, “Cybersecurity Framework,” National Institute of Standards and Technology, 2023, <https://www.nist.gov/cyberframework>.

threats and vulnerabilities. In contrast, the European Union has adopted a more regulatory-driven approach with the General Data Protection Regulation (GDPR), which not only focuses on data privacy but also imposes stringent cybersecurity requirements on organizations handling personal data.⁴⁰

At the international level, collaboration among nations is crucial in addressing the global nature of cyber threats. For example, the Tallinn Manual 2.0, is a non-binding legal framework drafted by international legislators for applying existing international law to cyberspace.⁴¹ Scholars such as Susan Brenner stress on the need for international norms and agreements and argue that cyber threats transcend borders, calling for an immediate and collective effort to establish rules of engagement and etiquette in the digital sphere.⁴²

2.2.2 Formulating Effective Cybersecurity Policies

Formulating cybersecurity policies that are effective and efficient is a complex and multifaceted process that requires a combination of technical expertise, legal considerations, and a deep understanding of the evolving threat landscape. Academics and practitioners offer diverse perspectives on the constituents of a robust cybersecurity policy, necessitating the need for a comprehensive and adaptive approach.

⁴⁰ EU - Information Commissioner's Office, "Essential Guide to the General Data Protection Regulation (GDPR)," *Guide to the General Data Protection Regulation (GDPR)*, March 22, 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711097/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf.

⁴¹ Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge, United Kingdom ; New York, Ny, Usa: Cambridge University Press, 2017).

⁴² Susan W. Brenner, "Cybercrime: Criminal Threats from Cyberspace," *Choice Reviews Online* 48, no. 02 (October 1, 2010).

Risk-Based Approach:

One prevailing view in the literature is the advocacy for a risk-based approach to cybersecurity policy formulation. Anderson emphasizes the importance of comprehending and prioritizing risks based on the potential impact on organizational assets.⁴³ One maneuver that has proven to be helpful is a risk-based approach which allows organizations to distribute resources efficiently, focusing on critical vulnerabilities and threats. The NIST Cybersecurity Framework, widely recognized in the field, is grounded in this approach, guiding organizations to identify, protect, detect, respond to, and recover from cybersecurity risks.

Legal and Regulatory Frameworks:

The legal and regulatory landscape provides a strong foundation for cybersecurity policies. Brenner argues that a well-formulated cybersecurity policy must have a strong legal foundation, ensuring that stakeholders adhere to established norms and regulations. The GDPR in the European Union furthers this viewpoint by not only outlining technical security measures but also imposing legal obligations on entities handling personal data. In the event of a cybersecurity breach, the legislation drawn provides a basis for accountability and consequences.

Public-Private Collaboration:

A recurring theme in the literature is collaboration between the public and private sectors as a crucial element of effective cybersecurity policies and their implementation. Clarke and Knake argue for the need for partnerships between government agencies, law enforcement, and private

⁴³ Chad Anderson, Richard L. Baskerville, and Mala Kaul, "Information Security Control Theory: Achieving a Sustainable Reconciliation between Sharing and Protecting the Privacy of Information," *Journal of Management Information Systems* 34, no. 4 (October 2, 2017): 1082–1112.

organizations to share threat intelligence, coordinate incident response efforts, and develop best practices that prevent possible dangers to the digital sphere and its users.⁴⁴ Hence, a more streamlined plan of action, Public-private collaboration strengthens the collective defense against cyber threats, leveraging the expertise and resources of both sectors.

Human-Centric Approach:

Cybersecurity policies are not solely about technology; they also involve human behavior and awareness. Green and Smith (2021) argue for a human-centric approach that considers the role of employees and users in maintaining a secure environment. In order to mitigate the cybersecurity threats, a collective effort on the user's end is imperative in sustaining a safer digital space. Training and awareness programs are deemed essential components of cybersecurity policies, aiming to reduce the likelihood of human error and increase overall security posture. Moreover, there is a higher sense of accountability and responsibility on an individual, and a more localized level.

Technological Integration:

The rapid evolution of technology requires cybersecurity policies to integrate cutting-edge solutions. Jones and Brown (2018) have placed great importance on the role of artificial intelligence and machine learning in improving cybersecurity capabilities. These technologies offer advanced threat detection, anomaly analysis, and automated response mechanisms, which align with the dynamic nature of cyber threats.

⁴⁴ Robert K Knake and Richard A Clark, *Cyber War : The next Threat to National Security and What to Do about It* (Abu Dhabi, Uae: The Ecssr, 2012).

Continuous Monitoring and Adaptation:

Another point of emphasis in the literature is the adoption of adaptive cybersecurity policies in the face of rapidly evolving threats. Smith et al. (2020) argue for continuous monitoring and adaptation, emphasizing the need to stay ahead of emerging threats that come about with every small technological development. This perspective goes hand in hand with the idea that cybersecurity is an ongoing process, not a one-time implementation, and requires consistent updates to address new susceptibilities and attack vectors.

International Cooperation and Norms:

Scholars such as Schmitt (2017) stress the importance of international collaboration and the development of required norms and etiquette in cyberspace. A truly effective cybersecurity policy, from this perspective, goes beyond national borders and calibrates with global efforts to lay the foundations of engagement and responsible behavior in the digital realm.

2.3 Cyber Security Landscape in Pakistan

In this era of rapid digital advancements and heightened geopolitical tensions, ensuring a secure cyber landscape is crucial for the well-being and survival of nations, and Pakistan is no exception to this. Like most countries in the Global South, Pakistan embraced internet connectivity in the 1990s with limited penetration that has since reached 54.48%. Although cyber-security is a much-researched topic in Pakistan, it is often viewed from a singular perspective that does not bridge the interdisciplinary nature of the issue. Trends in literature tend to focus on cyberspace and the threats to it.

Cyberspace is seen as an essential component of national security, particularly because of the growing focus on non-traditional security threats to the state. One of the main reasons why cyberspace is seen as necessary is because the state's critical infrastructure, along with public and private institutions, rely on it. According to Akram et al., cyberattacks on Pakistan's infrastructure have the capability to have a debilitating effect on the state, especially in times of unrest or war, which opens up a new front of vulnerabilities that belligerent states can target.⁴⁵

Although there is a divergence in opinion when looking at whether Pakistan is working towards improving its cybersecurity landscape, one thing is certain: changes in international trends are having an effect on the state's priorities. Since 2010, Pakistan's cybersecurity landscape has seen improvement through the introduction of legislative efforts, especially the National Cyber-Security Policy. This was pertinent given the trends of cyber crimes targeting banks, power companies, private businesses, and state institutions. Through the nature of these crimes, it was highlighted that attackers can be miles away from the state and still deal a comprehensive amount of damage due to our weakened cyber-landscape.

Dr. Tughral Yamin identifies the lack of organizational architecture to implement cyber-security policies and how there is no official method of establishing and reinforcing a cyber-security framework in the state.⁴⁶ He highlights how most states have existing frameworks that they update with incident responses, but Pakistan lacks the basic infrastructure to develop the framework in a cohesive way. This view is also shared by Sara Ahmed, who analyzed the preparedness of

⁴⁵ Muhammad Shehzad Akram, Moneeb Jaffar Mir, and Abdul Rehman, "Dimension of Cyber-Warfare in Pakistan's Context," *Journal of Positive School Psychology* 7, no. 6 (2023): 82–94.

⁴⁶ Tughral Yamin, "Cyberspace Management in Pakistan," *Governance and Management Review* 3, no. 1 (2018): 46–61.

Pakistan's cyber security infrastructure and found that although recent developments had made it inspired by international frameworks, there was still a lot to be done on the implementation level.⁴⁷

Similarly, scholars like Irta Fatima claim that Pakistan could benefit from regional cooperation in matters of cyber security, and taking this aspect of security seriously could potentially help the state improve its credibility.⁴⁸ This goes hand in hand with the growing trend of e-commerce and digitization of businesses, where cybersecurity is needed to protect payments, investments, customer data, and business information. Many scholars have noted the impact of cyber threats on Pakistan's financial sector, especially banking and private businesses.⁴⁹

2.3.1 Cyberattacks and Cybercrime

The existing literature breaks down illegal acts in cyberspace under (i) cyberattacks and (ii) cybercrime. Cyberattacks tend to be caused by non-state and often foreign actors looking to threaten state institutions and public sector organizations. This includes hackers, actors, and states that try to tap into our critical infrastructure, central banks, and institutions like NADRA. Cybercrime, on the other hand, is related to all national and mostly public-related cybersecurity breaches of information and data security. This can include stealing data from customers from businesses, using electronic means to spread radicalization, and much more.

⁴⁷ Sara Ahmed, "Cyber Security Threat and Pakistan's Preparedness: An Analysis of National Cyber Security Policy 2021," *Pakistan Journal of Humanities and Social Sciences Research* 5, no. 1 (June 30, 2022): 25–40.

⁴⁸ Irta Fatima, "Pakistan's Cyber Threat Landscape and Prospects of Regional Cooperation on Cyber Security," *Spotlight on Regional Studies* 40, no. 11 (November 2022).

⁴⁹ Aamna Rafiq, "Challenges of Securitising Cyberspace in Pakistan," *Strategic Studies* 39, no. 1 (April 24, 2019): 90–101.

Umair Pervez Khan and Muhammad Waqar Answar highlight the importance of proper cyber security policies in a state like Pakistan by delving into how cyber-reliant the state is, and there is no proper policy framework in place to reduce cyberattacks and cybercrime.⁵⁰ They emphasize the use of cyberspace to pose threats to the state by nonstate actors ranging from hackers to terrorist groups.

2.4 Literature Gap

From the conducted literature review, the main themes of cybersecurity in Pakistan and its challenges can be ascertained. Where most scholars tend to focus on the lack of critical infrastructure to implement cybersecurity policies as the main reason for the dismal state of cybersecurity in Pakistan, few have given importance to the quality of policymaking itself.

The majority of the literature deals with challenges to cybersecurity and cyberspace in the state, with emphasis on the securitization of cyberspace as a means of direct military threat to Pakistan. Not only does this try and shift the nature of the security threat to a more traditional one, but it also takes away the vulnerabilities that some scholars stressed in areas such as the financial sector, political institutions, and public offices. There aren't many studies that consider a holistic or multi-disciplinary approach to the issue, bridging the divide between strategic policy-making and computer science.

⁵⁰ Umair Pervez Khan and Muhammed Waqar Khan, "Cybersecurity in Pakistan: Regulations, Gaps and a Way Forward," *Cyberpolitik Journal* 5, no. 10 (2020).

This study aims to focus on the challenges faced by cybersecurity policy in Pakistan and open a critical discourse on the issue. It will look into where current policies are lacking and why is it difficult to draft a proper cybersecurity policy in Pakistan. Once the challenges and shortcomings are identified, it moves forward to assess the ways in which these issues can be mitigated and will focus on delivering an implementable cybersecurity policy at the end. Not only will this bridge the gap in existing literature, but it is bound to open a broader avenue of research by exploring a new area.

Conclusion

This chapter actively focused on conceptualizing cyber security and providing emphasis on a proper definition. It helped distinguish the topic of research from similar fields such as information security, data security, and computer security. By actively defining what cybersecurity entails, we can effectively outline the scope of the study and what it hopes to achieve. The extensive literature review helped identify the themes in cybersecurity literature and how they apply to this research. Starting from a more generalized theme of cybersecurity and narrowing it down to cybersecurity landscape in Pakistan, we find trends and schools of thought that create a clear understanding of the subject matter. Conclusively, the chapter provided an important theoretical and conceptual base for the research.

Chapter 3

TRENDS AND PATTERNS OF COMPREHENSIVE CYBER SECURITY FORMATION

The previous chapter helped ascertain the conceptualization and existing literature for cybersecurity and cybersecurity policy-making in Pakistan. It gave us a strong base for understanding and implementing information attained through research. This chapter takes that understanding and uses it to put forth trends of cybersecurity policies and practices. It helps establish the idea of an overall cyber security culture and how Pakistan can learn from international cybersecurity practices.

In cybersecurity, ‘culture’ refers to policies that define cyber practices and the attitudes or behaviors an individual or an organization displays towards the cyber threat and security measures.⁵¹ On the other hand, the ‘cyberspace landscape’ encompasses enforcing diverse standards and protocols that are solution-oriented against certain security challenges and threats faced by different nations.⁵² There has been a growth of cyber threats in both complexity and scale, which points out the need to compare the cybersecurity practices of a nation with international standards.

⁵¹ Uchendu, Betsy, Jason RC Nurse, Maria Bada, and Steven Furnell, “Developing a cyber security culture: Current practices and future needs,” *Computers & Security* 109 (2021): 102387.

⁵² Singh, Bhupinder, “Unleashing Alternative Dispute Resolution (ADR) in Resolving Complex Legal-Technical Issues Arising in Cyberspace Lensing E-Commerce and Intellectual Property: Proliferation of E-Commerce Digital Economy,” *Revista Brasileira de Alternative Dispute Resolution-Brazilian Journal of Alternative Dispute Resolution-RBADR* 5, no. 10 (2023): 81-105.

The purpose of this state-global unified efforts is not only to enhance protection against international cyber threats but also to facilitate international cyber diplomatic cooperation and mutual trust among the nations and/or private organizations.⁵³ In the wake of growing cyber threats, Pakistan is trying to enhance its cybersecurity framework in accordance with global standards. The purpose is to not only save the everyday business of the state but also bridge the gaps in cyber national security. This purpose can be achieved by understanding the best practices used in other states and regions and complying with international standards that ensure the effective management of cyber risks.

3.1 Introduction to Key International Cybersecurity Standards

The ‘international cybersecurity landscape’ of cybersecurity can be defined as the technological and policy measures governed by standards and frameworks designed to protect organizations, governments, and individuals from the extensive and diverse nature of cyber threats.⁵⁴ These standards have proved to be instrumental in establishing a robust cybersecurity posture on the global level and in playing a significant role in promoting mutual trust-based international cooperation.

Among major international standards for client information management cyber security, is the ISO/IEC 27001 standard that seeks to equip the organizations with specifications required for

⁵³ Nir Kshetri, *Cybersecurity Management: An Organizational and Strategic Approach* (Toronto: University of Toronto Press, 2021).

⁵⁴ Sarah Backman, “Risk vs. Threat-Based Cybersecurity: The Case of the EU,” *European Security* 32, no. 1 (2023): 85-103.

information security management systems (ISMS).⁵⁵ This system assists the organizations in managing their crucial security assets such as financial information, intellectual property arrangements, details of employees, or all other sources of information that are entrusted with the organization in its business-to-business or business-to-client interactions.⁵⁶ In ISMS, a great emphasis is on adopting a ‘continuous improvement approach’ to data security through flexible upgradation systems in the ever-evolving cyber threat landscape.

The NIST Cybersecurity Framework, developed by the National Institute of Standards and Technology for the United States, offers a useful computer security policy framework through which private sector organizations in the US can assess and improve their ability to prevent, detect, and respond to cyber-attacks. It provides a flexible, repeatable, and adaptive approach to organization-associated risks.⁵⁷

The European Union’s General Data Protection Regulation (GDPR) is not only a standard of regulation in the protection of information but also a benchmark in cyber security. It has set a high standard for data privacy laws globally. Its requirements are not only for European companies but are also for any business that markets goods or services to the EU residents. This approach of

⁵⁵ Omar A. Fonseca-Herrera, Alix E. Rojas, and Hector Florez, “A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard,” *IAENG International Journal of Computer Science* 48, no. 2 (2021): 213-222.

⁵⁶ “Ibid.”

⁵⁷ Gregory B. White and Natalie Sjelin, “The NIST Cybersecurity Framework,” in *Research Anthology on Business Aspects of Cybersecurity*, (Hershey, PA: IGI Global, 2022), 39-55.

regulation to data protection by design and by default encourages an initiative-taking mechanism of data security with a remarkable effect on international business practices.⁵⁸

3.2 Examination of Frameworks from Leading Cybersecurity Nations

The frameworks developed by leading cybersecurity nations such as the United States, Singapore, and Israel provide exemplary models that can be adapted by other countries striving to enhance their cybersecurity postures. Each of these nations employs distinct strategies tailored to their specific needs and capabilities, which has led to the creation of highly effective cybersecurity environments.

3.2.1 The United States Cybersecurity Framework

A comprehensive framework to cybersecurity risk management in the US include the NIST Cybersecurity Framework, an outcome of a presidential executive order, that aims at national cybersecurity, the framework categorizes best practices into five functions: Identify, Protect, Detect, Respond, and Recovery.⁵⁹ This framework is capable of helping organizations of all sizes (human and capital resources) and types to manage their cyber risks in an effective and systematic manner. It has proved to be useful in holistic provisions of flexibility in cyber security within the frameworks that permit its implementation across various sectors, from businesses to citizens and

⁵⁸ Chris Jay Hoofnagle, Bart Van Der Sloot, and Frederik Zuiderveen Borgesius, “The European Union General Data Protection Regulation: What It Is and What It Means,” *Information & Communications Technology Law* 28, no. 1 (2019): 65-98.

⁵⁹ Sri Nikhil G. Gourisetti et al., *Facility Cybersecurity Framework Best Practices*, No. PNNL-30291 (Richland, WA: Pacific Northwest National Lab. (PNNL), 2020).

state security matters. Moreover, it is compatible with current cybersecurity practices as well as giving room to future innovations in cybersecurity.

In addition, the Federal Financial Institutions Examination Council (FFIEC) has also issues guidelines to financial institutions targeting the measures like cybersecurity awareness, data management and incident responses effectively.⁶⁰ These guidelines are crucial in maintaining the security of sensitive and important financial data. Thus, the guidelines demonstrate a well-designed approach that can be followed by other sectors that deal with high-stakes data.⁶¹

3.2.2 Singapore’s Strategic Cybersecurity Measures

The Singapore government has established a Cyber Security Agency (CSA) of Singapore to coordinate a national effort in combating the myriad of cyber threats.⁶² This initiative is guided by the three strategic objectives: building a resilient infrastructure, developing a safer cyberspace, and growing a vibrant cybersecurity awareness-based ecosystem. This includes improvement to the safety and security of the existing critical information infrastructures. To upgrade the efficiency of these systems, an adequately skilled and trained professional force of cybersecurity experts and promotion of international partnerships are also utilised as effective measures. Further, the CSA puts emphasis on proficient public education and awareness as one of the critical tenets of

⁶⁰ Federal Financial Institutions Examination Council, “Federal Financial Institutions Examination Council” (2016).

⁶¹ “Ibid.”

⁶² Cung Vu and S. Rajaratnam, *Cyber Security in Singapore* (Singapore: S. Rajaratnam School of International Studies, 2022).

comprehensive national cybersecurity in Singapore, which ensures a safe, secure, and resilient digital ecosystem.⁶³

3.2.3 Israel's Cybersecurity Innovation and Collaboration

By employing both governmental support and private sector innovation the cyber security landscape of Israel utilises a well-integrated approach which is maintained by the common citizens as well. The Israel National Cyber Directorate (INCD) was established for coordinating national cyber defense and developing policies that would integrate the military, academic, and industrial sectors.⁶⁴ What makes the Israeli strategy unique is the fact that with the obligatory military service has dedicated units in cyber intelligence. The units are in place to protect national interests and help create a culture of cybersecurity expertise that permeates effectively into society.⁶⁵ Israel's public-private model has been regarded as one of the pioneers in its nature globally. It can serve as a blueprint for effective collaboration in cybersecurity innovation and implementation against threats affecting the state's cyber security in both horizontal (among masses or businesses) as well as vertical domains (between state authorities and private entities, for instance).

All these frameworks from the United States, Singapore, and Israel, not only protect their national assets but also contribute to global standards of cybersecurity through international cooperation by setting high benchmarks. These countries strengthen the global ability against the cyber threats by sharing best practices to cybersecurity, which is crucial in a globally connected digital world.

⁶³ "Ibid."

⁶⁴ Eviatar Matania, Lior Yoffe, and Tal Goldstein, "Structuring the National Cyber Defence: In Evolution Towards a Central Cyber Authority," *Journal of Cyber Policy* 2, no. 1 (2017): 16-25.

⁶⁵ Monica Kaminska, "To Retaliate or Not: A Matter of Cyber Risk Perception," PhD diss., University of Oxford, 2021.

3.3 A Cross-National Comparison: Pakistan's Cybersecurity Preparedness and Global Practices

The policy and framework for cybersecurity in Pakistan primarily revolve around counteracting cyber threats and enhancing the protection of digitized infrastructure. The backbone of all such cyber-security initiatives is the National Cyber Security Policy 2021, which aims to protect national critical infrastructure and reduce vulnerability against cyber-attacks. This policy articulates strategic objectives that include the creation of an enabling, cyber-secure environment, the development of indigenous capacities, and the strengthening of international collaboration.⁶⁶

Despite these efforts, significant gaps in Pakistan's cybersecurity practices compared to international standards such as ISO/IEC 27001, NIST, and GDPR are evident. While the National Cyber Security Policy provides a broad framework, the specific guidelines and procedures for enforcement remain underdeveloped. Compared to ISO/IEC 27001, which recommends very detailed control and mechanisms for continuous improvement, the Pakistani framework does not set compliance requirements tightly and robustly that are considered the norm under a more mature regulatory environment.

Additionally, the data protection standards in Pakistan are also evidently weak. Unlike the GDPR, which has very stringent standards for data protection and massive penalties for non-compliance, Pakistan's data protection laws are relatively lenient and not strictly enforced, leaving personal and corporate data security exposed. The consequences of such a cybersecurity void are extremely

⁶⁶ Sara Ahmad, "Cyber Security Threat and Pakistan's Preparedness: An Analysis of National Cyber Security Policy 2021," *Pakistan Journal of Humanities & Social Sciences Research* 5, no. 1 (2022): 33.

severe for the country: Pakistan is increasingly vulnerable to various forms of cyber-attacks that can target its critical national infrastructure and potentially lead to an economic and security crisis. For example, an attack on a financial institution, as happened in 2021 against the National Bank of Pakistan, can result in significant financial losses, thereby undermining public confidence in the e-banking system.⁶⁷

Furthermore, poor cybersecurity measures deter foreign investment, as international companies are often reluctant to engage in markets where cyber risks are not adequately managed. Moreover, without stringent data protection mechanisms, personal information is at risk of being compromised, leading to privacy breaches and potential misuse of sensitive data. This scenario would lead to a security breach for the citizens and can invoke a heavy cost on international relations, as business and geopolitical ventures (such as the China-Pakistan Economic Corridor) usually require some assurance that their data are being used securely and compliantly with international standards and governing norms.

3.3.1 International Cybersecurity Alignment: Successful Practices from Around the Globe

The successful cybersecurity strategies of Estonia and South Korea, which have both aligned their national frameworks with international, can serve as the best cybersecurity insights for Pakistan.

⁶⁷ The Newspaper's Staff Reporter, "Cyberattack Disrupts National Bank of Pakistan Services; Recovery by Monday Likely," *Dawn*, October 31, 2021, <https://www.dawn.com/news/1655059>.

Estonia: Leading the Way in Cybersecurity

Estonia has now revised its cybersecurity strategy to be in line with NATO and EU practices that emphasize the restoration of digital services. This was after a massive Distributed Denial of Service (DDoS) attack in 2007, which crippled the crucial digital infrastructure of the country for several days by targeting government networks, financial institutions, and news media. This led to the establishment of the Estonian Information System Authority (RIA), which is tasked with the enforcement of regulations to comply with international best practices for infrastructure security in cyberspace.⁶⁸

Among the greatest achievements of Estonia after DDoS attack is the development of X-Road mechanism. It is a decentralized digital platform that interconnects safely with different services of the public and private sectors throughout the country.⁶⁹ This platform is developed in such a way that if part of the system is compromised, then the whole network does not collapse, thus averring any situation as occurred in the DDoS. Secondly, the e-Estonia initiative is also a highly dependable cybersecurity mechanism to protect the data of citizens and allow for the continuity of government operations.

Thus, Estonia, with its proactive approach to NATO and the Cooperative Cyber Defence Centre of Excellence, maintains a specialized body for cybersecurity, and the X-road system serves as an

⁶⁸ Dita Aulia Salma and Fahlesa Munabari, "Blockchain Technology: Cyber Security Strategy in Post-2007 Cyber-Attacks Estonia," *Deviance Jurnal Kriminologi* 7, no. 1 (2023): 32-45.

⁶⁹ Eric Blake Jackson, Richard Dreyling, and Ingrid Pappel, "A Historical Analysis on Interoperability in Estonian Data Exchange Architecture: Perspectives from the Past and for the Future," in *Proceedings of the 14th International Conference on Theory and Practice of Electronic Governance*, (2021): 111-116.

example of the value of agencies focusing on overseeing and enforcing security. Pakistan can also devise advanced functional bodies for execution and compliance of cybersecurity on similar lines.

South Korea: Comprehensive Cybersecurity Enhancement

Through a well-defined and articulated cybersecurity framework that adheres to international standards such as ISO/IEC 27001 and the NIST framework, South Korea has also responded robustly to cybersecurity challenges, particularly those posed by its northern neighbor: North Korea. Massive investments in cybersecurity technologies and research have been one of the key elements of the South Korean strategy, which works on strong public-private partnership models, thereby strengthening the country's cyber resilience.

Institutionally, the Korea Internet & Security Agency (KISA) has a central authority in dealing with the management of cybersecurity in South Korea.⁷⁰ The measures in place for this management employ the real-time monitoring of the cyber breach incidents and rapid response teams. The agency provides a secure internet that focuses on the management and the establishment of protection to cope with any cyber threat. The South Korea Private Cybersecurity Council has released the frameworks that facilitate cooperation between the governments and private sectors in relation to issues on information sharing and coordination of response with regard to cyber threats.⁷¹

⁷⁰ Yu-Kyung Kim, Myong-Hyun Go, Sonyong Kim, Jaeyeon Lee, and Kyungho Lee, "Evaluating Cybersecurity Capacity Building of ASEAN Plus Three through Social Network Analysis," *Journal of Internet Technology* 24, no. 2 (2023): 495-505.

⁷¹ "Ibid."

Establishment of an agency on the pattern of South Korea's KISA could enable better preparedness, monitoring, and response to incidents of a cyber nature in Pakistan. Similarly, the public-private collaboration model of South Korea can empower Pakistan to unleash the innovation and flexibility of the private sector in strengthening governmental cybersecurity initiatives.

3.4 Collaboration between State and Public Cybersecurity Efforts

Today's world is an interconnected cyber universe; thus, cybersecurity is a critical issue that transcends individual or singular organizational capabilities and brings up public-private partnerships (PPPs) as a point of necessity. The 'Public-Private Partnerships' in cybersecurity involve cooperative arrangements between the public sector bodies such as governmental agencies and private sector entities, i.e., research firms, software houses and dedicated cybersecurity institutions, to improve the security and resilience of cyberspace.⁷² These are crucial partnerships that leverage the strengths and resources of each sector in dealing with perplexed cyber threats, which could not be otherwise dealt with by a single entity. Significant funding and legislative support, regulations enforcement, and efforts coordination in the national and international security spectrum can only be guaranteed by sufficient financial muscle and administrative willpower of the governments.

On the other hand, infrastructure is often in the private sector, where most of the agile technological means are involved in rapid innovation. For this reason, they lead the market of specialized cyber

⁷² Ethem Ilbiz and Christian Kaunert, "Cybercrime, Public-Private Partnership and Europol," in *The Sharing Economy for Tackling Cybercrime*, (Cham: Springer International Publishing, 2023), 13-28.

security technologies and recognise and work on threat response trends. These private companies develop cutting-edge solutions in the field of cybersecurity to maintain a competitive position in the market. The public-private partnerships can solidify both comprehensive and dynamic defenses against cyber threats in both critical infrastructure resiliency and state-sponsored cyber espionage ransomware attempts.

3.4.1 Global Best Practices in Public-Private Partnerships

PPPs in cybersecurity demonstrate a variety of successful models of collaboration, each crafted to the specific security needs and strengths of both parties involved (state and private entity). The following examples, for instance, from the United States, Netherlands, and the ongoing Russia-Ukraine conflict explore a broader perspective of how the strategies are taking place across most advanced regions in international cyber culture.

United States: Cybersecurity and Infrastructure Security Agency (CISA)

The most popular example of public-private collaboration in the United States is the Cyber Information Sharing and Collaboration Program (CISCP), developed by the Cybersecurity and Infrastructure Security Agency (CISA) to launch several programs that will foster a collaborative relationship.⁷³ This program further facilitates the sharing of cybersecurity information during incidents and in routine operations to enhance situational awareness and defense against cyber threats. It has thus attracted high participation from varied industries whose collaboration has yielded efficient protective measures and response strategies that help lower the vulnerability to cyber-attacks in pertinent sectors.

⁷³ Petar Radanliev, “Cyber Diplomacy: Defining the Opportunities for Cybersecurity and Risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing,” *Journal of Cyber Security Technology* (2024): 1-51.

In December 2020, the SolarWinds attack was identified as compromising the Orion software update mechanism; thus, it was designated as a very sophisticated and elaborate supply chain cyber intrusion. The operation has been attributed to a Russian cyber-espionage attempt and affected about 18,000 organizations, including US government entities and even fortune 500 businesses.⁷⁴ FireEye, the leading cybersecurity firm, was the first to identify the problem within its own systems.⁷⁵ It further traced it to compromised software from SolarWinds. In the wake of that disclosure, SolarWinds and a number of cybersecurity firms and government agencies, including the FBI, CISA (Cybersecurity and Infrastructure Security Agency), and NSA (National Security Agency), spurred into a cooperative effort to assess the extent of the breach and take action to prevent further havoc. This collaborative response underscored the significance of joint efforts between the private sector and government bodies toward effective cybersecurity.

The Netherlands: A Comprehensive Cybersecurity Collaboration Model

The Netherlands has profiled itself as the front leading country in a comprehensive National Cyber Security Strategy, with a key focus on both prevention and response. This approach to the strategy brings private companies, academic institutions, and NGOs into collaboration, coordinated through the National Cyber Security Centre (NCSC).⁷⁶ The Dutch Cyber Security Alliance is a strong cooperation of government organizations, the business community, and knowledge institutions. It operates on all possible fronts, from the creation of new cybersecurity technologies

⁷⁴ Marcus Willett, "Lessons of the SolarWinds Hack," in *Survival April–May 2021: Facing Russia*, (Routledge, 2023), 7-25.

⁷⁵ Scott J. Shackelford, Anne Boustead, and Christos Makridis, "Defining 'Reasonable' Cybersecurity: Lessons from the States," *Yale JL & Tech.* 25 (2023): 86.

⁷⁶ Mmakoena Mpshane-Nkosi, "4IR and the Emergence of Digital Foreign Policy: A Global Comparative Study," PhD diss., University of Johannesburg, 2023.

to the exchange of threat intelligence and best practice methods among various other allied sectors, no matter how big or small they may appear.⁷⁷ On the other hand, the Hague Security Delta (HSD) also represents itself as an alliance to innovate security solutions and enhance knowledge. Themes of HSD include cybersecurity, national and urban security, and protection of critical infrastructures.⁷⁸

The DigiNotar Incident Response (2011) is a great example of the effectiveness of the Netherlands's PPPs. After the DigiNotar compromise, which involved the Dutch certificate authority, the NCSC worked very closely with the top experts from the private sector to contain its impacts. The actions involved revocation of trust in DigiNotar certificates and issuance of security updates across all systems affected in an accelerated manner.⁷⁹ Now, the NCSC has a 24/7 cybersecurity monitoring centre that exclusively contributes to the necessary information for cybersecurity being distributed among public and private partners. Such continuous exchange of information has proved useful for predicting potential cyber threats and responding to them with well-rehearsed action plans.

Public-Private Partnerships in Cybersecurity: Russia-Ukraine Conflict

Since the eruption of conflict with Russia, the Ukrainian PPPs have improved the state's cyber defense against numerous attacks aimed at destabilizing the government and critical infrastructure from Russia. Ukraine has engaged with global technology companies and cybersecurity firms to

⁷⁷ James A. Lewis, Erica D. Lonergan, Julia Voo, Melanie Garson, and Amy Ertan, *Evolving Cyber Operations and Capabilities* (Center for Strategic and International Studies, 2023).

⁷⁸ Melissa Hathaway and Francesca Spidalieri, "Cyber Readiness at a Glance" (2017).

⁷⁹ Erik Schrijvers, Corien Prins, and Reijer Passchier, *Preparing for Digital Disruption* (Springer Nature, 2021).

bolster its capabilities. In countering the Russian cyberattacks, Microsoft's assistance to Ukraine includes monitoring and responding to real-time cyber threat intelligence and technical support to strengthen the country's response capabilities.⁸⁰ Ukraine also worked with the preeminent American cybersecurity company, CrowdStrike, to help boost Ukraine's defense capabilities against Russian cyber maneuvers. The cooperation, according to reports, includes deploying advanced security systems designed to uncover and block the malware used by the Russian operators.

Russia, on the other hand, prefers to rely on domestic technology firms, quasi-private hacking groups, and state-sponsored cyber operations. While not formal PPPs, such relationships can take on a symbiotic nature and are state-encouraged. For instance, Fancy Bear (APT28), affiliated with private groups and Russian intelligence, is performing a very crucial role in cyber operations in Russia against Ukraine.⁸¹ This group has been conducting strategic cyber-attacks aimed at disrupting communication and gathering intelligence from Ukraine. In so doing, the Russian IT and cybersecurity companies are simply co-opted to produce technology and expertise that help boost the government's cyber espionage and warfare capabilities.

⁸⁰ Herbert Lin, "Russian Cyber Operations in the Invasion of Ukraine," *The Cyber Defense Review* 7, no. 4 (2022): 31-46.

⁸¹ Jaimie Lelonek, "Analyzing Russia's Conventional and Cyber Operations in Ukraine," PhD diss., Utica University, 2022.

3.5 Opportunities for Pakistan to Enhance Public-Private Collaboration

The examples from the United States and the Netherlands illustrate the value of public-private partnerships in enhancing national cybersecurity, offering insights that Pakistan can leverage. The collaborations demonstrated the benefits of rapid information sharing and joint efforts in mitigating cybersecurity threats. This view shows a national strategy of the Netherlands that underscores an integrated way of protection for national infrastructure and forging partnerships by all sides, government, industry, and academia, to promote innovation.

The cyber ecosystems, such as the Dutch Cyber Security Alliance and The Hague Security Delta, point to a framework whereby an initiative-taking cybersecurity culture dealing with present and future challenges is one that is most relevant for a country like Pakistan, which has strategic geopolitical challenges. In fact, by adopting some of the same PPP models, Pakistan can better its security against cyber threats through better threat intelligence, faster incident responses, and more hardened infrastructure that protects its critical national interests. This becomes, therefore, an enabler for cooperative economic and social development, which is a sustainable and safe digital environment.

Moreover, improving cybersecurity will require Pakistan to focus on enhancing public-private collaboration in key sectors that include finance, telecommunications, and energy. In this way, such sectors will then have a priority, and hence, there will be proper utilization of resources to achieve realization in the cyber strategic plan. The government may encourage the private sector to participate by providing various incentives in the nature of tax breaks, research grants, and streamlined regulatory procedures. The government should also take steps to create a conducive environment for collaborative research and development. This will encompass setting clear

partnership objectives, ensuring transparent communication, and aligning the stakeholders' interests. This will also be critical in establishing a well-defined framework of public-private partnerships in governance and operations that enhance the legitimacy and confidence in the efforts by guiding the initiatives.

Conclusion

Leading states in cybersecurity practices have one thing in common - they take inspiration from certain international standards and apply them to their domestic cybersecurity realities. This chapter looked at many important international standards such as ISO/IEC 27001, NIST framework, GDPR and more. It examined the cybersecurity policies and frameworks of leading states such as the United States, Israel, and Singapore whilst highlighting case studies of Estonia, the Netherlands, and South Korea. Pakistan can learn a lot from these states, especially with how they've adapted to various frameworks while creating ones of their own; towards the end of the chapter, we briefly look over the opportunities for Pakistan to enhance public-private collaboration - a cornerstone of a cyber-secure state.

Chapter 4:

CHALLENGES TO CYBER SECURITY POLICY FORMATION

Leading off the previous chapter, where we learned about various cybersecurity practices of cyber-secure nations worldwide, we now look into the challenges faced by states in forming a cybersecurity policy. This chapter highlights challenges on three levels, i.e., (i) global, (ii) state, and (iii) implementation level. At each level, states and cybersecurity stakeholders are faced with a set of challenges that impact their ability to fully secure themselves.

There are certain challenges are unique to the socio-political landscape of Pakistan and the second half of this chapter outlines them in detail. These challenges have been identified through research on Pakistan's cybersecurity policies and practice as well as by analyzing the input from the various cybersecurity stakeholders interviewed during the research process.

The aim of the chapter is to identify which challenges Pakistan is mostly impacted by and how they are to be dealt with. It takes into account new developments in the state's cybersecurity arsenal, such as the establishment of PKCERT and other endeavors, such as the PTA Cyber Security Strategy 2023-2028.

4.1 Background

With the growing nature of traditional and non-traditional security challenges faced by states, the most immediate reaction for policy formation and implementation is ad hoc public-private cooperation. Yet, cyber security is one such aspect that has not been addressed with the same regard worldwide. Cyber threats have defined the state and international security systems for many

decades, showing their potential and capacity for causing harm. However, the formation of a policy and providing solutions to these issues almost always rests on the states.

Many believe this is because of the delicate nature of targets that cyber threats attack, mainly people and privacy. For democratic countries, both people and privacy are sore subjects since they cannot exercise much control over either. In a free world, a democratic state's cyber security practices cannot resemble a panopticon, and the policy would be greatly rejected by the people.

Trends like these are what cause the different forms of cyber security attitudes seen in the US and Europe, where the former focuses on security over privacy and the latter does the opposite. Non-democratic states or illiberal democracies have a more 'iron-fist' approach to the issue, putting state security above any notion of people or privacy. Yet, semi-democratic states or democracies in transition tend to find themselves between a rock and a hard place when it comes to which approach to adopt.

Pakistan is no exception to this dilemma. Although it joined late to the global race to securitize cyberspace, it ruled out a much anticipated Cyber Security Policy in 2021. However, the policy itself was generic and did not meet the specific needs of the state. It also saw practically no implementation, especially given the state has gone through high-level security hacks and breaches since then. What is now needed is a revised policy with a more overarching approach that can be implemented in a larger capacity and reap better results.

This chapter aims to look at the various challenges faced in cyber security policy formation. It divides its approach into three distinct sections: global level, state level, and implementation level. By analyzing the general challenges to making good policy and looking at Pakistan's case in detail,

we hope to identify our shortcomings. The end of the chapter will take a look at the effect a good cyber security policy can have on the state and the need to make one.

4.2 Challenges to Cyber Security Policy Formation

Barry Buzan and Ole Weaver define securitization as “a discursive process through which an inter-subjective understanding is constructed within a political community to treat something like an existential threat to a valued referent object and to enable a call for the urgent and measures to exceptionally deal with the threat⁸².” In this sense, the government is the main responsible actor for cyber-security policy formation, but there are cyber threats that also impact organizations and businesses in the private sector. The challenges to forming a cohesive and effective cyber security policy can be divided into the following levels:

4.2.1 Global Level

With the advancement of information and communication technologies (ICTs), cyber security has become a global issue⁸³. According to Forbes, In 2023, there was a significant rise in cyberattacks, affecting over 343 million individuals. From 2021 to 2023, data breaches increased by 72%, setting a new record⁸⁴. Unlike most global issues, there is no international framework for cybersecurity.

⁸² Barry Buzan and Ole Waever, *Regions and Powers: The Structure of International Security* (Cambridge: Cambridge University Press, 2003).

⁸³ United Nations, “Cybersecurity: A Global Issue Demanding a Global Approach,” Un.org, December 12, 2011, <https://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html>.

⁸⁴ Mariah St. John and Brenna Swanston, “Cybersecurity Stats: Facts and Figures You Should Know – Forbes Advisor,” [www.forbes.com](https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/#:~:text=Cybersecurity%20Fast%20Facts&text=As%20the%20globe%20becomes%20more), February 24, 2024, <https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/#:~:text=Cybersecurity%20Fast%20Facts&text=As%20the%20globe%20becomes%20more>.

Cybersecurity Spending Trends

The year 2023 saw an increase in organizations paying for ransomware attacks regardless of where they happened. Even though the US is leading cybersecurity efforts worldwide, it paid the most in ransomware attacks. The global cost for ransomware attacks was \$20 billion in 2021 and is projected to increase to \$280 billion in 2031⁸⁵.

Regardless of the measures states have in place, they are put in a position where they have to pay hackers to retrieve data from breaches. Many companies and organizations have started to incorporate ransomware attack policies to pay off hackers as they value personal and organizational information. This trend of spending is more than what states globally spend on securitizing cyberspace itself and has led to nonchalant behavior towards cyber-attacks.

Dynamic Nature of Evolving Threats

Another challenge in creating global cyber security policies is that there isn't a stagnant nature of cyber threats. Cyber threats continue to evolve as ICTs develop and expand their impact. It is safe to say that although many leading states in cybersecurity defense have entire organizations dedicated to studying these threats, their solutions are more reactive than preventive⁸⁶. Similarly, the existing frameworks cannot take into account when a new type of threat will exploit a loophole in their policies.

⁸⁵ Esentire, "2023 Official Cybercrime Report," *Esentire*, 2023, <https://www.esentire.com/resources/library/2023-official-cybercrime-report>.

⁸⁶ Takudzwa Fadziso et al., "Evolution of the Cyber Security Threat: An Overview of the Scale of Cyber Threat," *Digitization and Sustainability Review* 3, no. 1 (September 2023): 1–12.

When cyber security professionals who dealt with organizations in various companies were asked about their views, they claimed that “Hackers are ahead of the game when it comes to global cyber security efforts. This is seen with any form of technology where opposing actors try and find loopholes. Although states can opt to choose a preventive approach, they cannot be safe enough from a new form of attack as long as they are connected to the internet.”

No Global Framework

Lastly, there is a lack of a global framework for a cohesive cybersecurity strategy. Even though the United Nations has reiterated that cyber security is a global threat, it is not treated as one. One of the main reasons why it is believed that there is a lack of global framework is that states might be expected to sign treaties to not use cyber attacks as a means of warfare, something which leading superpowers would never agree to.

There are organizations, such as the World Economic Forum, that see cyber security as the threat that it is. Around 90% of the 120 executives who were surveyed at the World Economic Forum’s Annual Meeting on Cybersecurity agreed that urgent action was needed to deal with global cybersecurity inequity⁸⁷. Yet, even though some states have fewer cybersecurity measures than others, the effects of cyber threats seem to affect all states regardless⁸⁸.

⁸⁷ World Economic Forum and Accenture, “Global Cybersecurity Outlook 2024 ” (World Economic Forum, January 2024).

⁸⁸ Muhammad Fakhru Safitra, Muharman Lubis, and Hanif Fakhurroja, “Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity,” *Sustainability* 2023 15, no. 18 (September 6, 2023).

4.2.2 State Level

Researchers have mainly concerned themselves with cybersecurity policy formation at the state level. This is because the state's cybersecurity threats and regulatory environment can greatly vary depending on its type of governance, geopolitical importance, and more. Each state has its own set of laws, resources, and threat landscapes, necessitating tailored cybersecurity approaches⁸⁹. However, this state-specific focus can lead to inconsistencies and fragmented policies across the nation, making it difficult to implement cohesive and unified cybersecurity strategies.

Lack of Understanding

One of the main issues our respondents identified was a lack of understanding between policymakers, state institutions, and organizations on cybersecurity threats and what is needed. In developed countries, cybersecurity policies are influenced by organizational research and state-of-the-art academia.

However, implementation of these policies is lost on the departments it is applied to. In states like Pakistan, those who make the policy aren't well-versed in cybersecurity, nor are they researchers. These policies are made with little understanding of the threats to the state with little to no focus on the feasibility of implementation.

⁸⁹ Francesco Mifsud, "Internal and External Challenges to an Effective Organisation-Wide Cyber Security Set of Policies.," Cybergate - Your Cyber Security Partner, October 10, 2022, <https://cybergateinternational.com/blog/internal-and-external-challenges-to-an-effective-organisation-wide-cyber-security-set-of-policies/>.

Security Over Privacy

Another challenge that states face when creating cybersecurity policies is whether to put the state's security first or the privacy of the citizens. In many cases, the state may need to ensure measures that may seem like they take away from the people's freedom of speech or expression⁹⁰.

Similarly, when cyberattacks happen, and the state loses citizen information, it is faced with the issue of either paying the hackers or holding their ground. In most policies, states opt to mention paying hackers as part of the plan to retrieve information⁹¹. Yet, in the eyes of some security theorists, it enhances the security threat and encourages hackers to make more attempts.

No 'One Model Fits All' Solution

Another challenge is the absence of a universal solution that can be applied to all cybersecurity scenarios. The diverse nature of cyber threats and the varying needs of different sectors mean that a one-size-fits-all approach is impractical. Certain organizations like banks tend to have more issues with protecting data breaches than stopping cyber attacks. On the other hand, security organizations might want to protect against any spyware being downloaded onto their computers.

Each organization, industry, and state may require customized cybersecurity policies tailored to their specific vulnerabilities and requirements. This diversity necessitates flexible and adaptive policy frameworks that can respond to the evolving cyber threat landscape⁹². Taking this challenge

⁹⁰ National Research Council (U.S and National Research Council (U.S.). Computer Science And Telecommunications Board, *At the Nexus of Cybersecurity and Public Policy : Some Basic Concepts and Issues* (Washington, Dc: National Academies Press, 2014).

⁹¹ *ibid.*

⁹² Thomas R Peltier, *Information Security Policies, Procedures, and Standards : Guidelines for Effective Information Security Management* (Boca Raton, Fla.: Auerbach, 2002).

into account, cybersecurity policies should not be seen as a plan or tool but rather as a safety web with a combination of proactive and reactive capabilities.

Organizational Competition

In states that have an organizational model of policy formation, it can be difficult to form a cohesive cybersecurity policy. This is because the organizations are often in competition with one another for resources, talent and technological advancement. Instead of thinking as a state unit, they tend to use their personal influence to push for policies.

This impacts many states, especially those with weak political systems. Sometimes, the critical infrastructure for ICTs varies greatly depending on the state institution, so a common policy doesn't work when they don't have the basics to support cyber security⁹³. A situation like this calls for reformation and a good cyber security infrastructure in states on which the policy can rest.

4.2.3 Implementation Level

Lastly, we have the implementation level. Oftentimes, there are good cybersecurity efforts and policy outlines put forward by states that tend to pass legislative reviews but are never put into effect⁹⁴. This is the area where most researchers find an issue with cybersecurity culture at the state and international levels. Oftentimes, policies are made to show that the state is taking an issue seriously, but the state doesn't put effort into its follow-up. A multitude of challenges on this level can hinder proper cybersecurity policy formation.

⁹³ Hugo Riggs et al., "Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure," *Sensors* 23, no. 8 (January 1, 2023): 4060, <https://www.mdpi.com/1424-8220/23/8/4060>.

⁹⁴ Syed Asad Abbas Bokhari, "A Quantitative Study on the Factors Influencing Implementation of Cybersecurity Laws and Regulations in Pakistan," *Social Science* 2023 12, no. 11 (2023): 629.

Lack of Funding

One of the first challenges is a lack of funds. The state, like any organization looking to improve its cybersecurity, has limited funds that it needs to use on security threats. Since cybersecurity is widely regarded as a non-traditional security threat, there are still governments that take it lightly. Hence they make policies with no intentions of implementing them.

On the other hand, sometimes very good policies are made, but they require the state to catch up to internal level readiness against cyber threats. This requires changes to the state's critical cyber infrastructure and the opening of new positions that overlook cyber security. The government often doesn't have enough funds to cover these requirements, and the measures are abandoned.

No Awareness Among People

People are at the heart of cybersecurity policies as they are the ones that run the ICTs that are effected by cyber threats. Studies have shown that a large number of cybersecurity breaches happen due to neglect and human error. You may have a good cyber defense system and a policy that focuses on measures, but until awareness is not a core part of the policy's steps, it cannot be a success.

Verizon's 2023 Data Breach Investigations Report (DBIR) detailed that 74% of cyber security breaches happen due to human error⁹⁵. Since humans are the people running state institutions and organizations, even the most perfectly constructed policy will fall short if it does not take human error into account.

⁹⁵ Verizon, "DBIR Report 2023," Verizon Business, 2023, <https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/>.

No Public-Private Cooperation

Policies also tend to fail in the implementation phase when there is no outline for public-private cooperation in addressing the state's cybersecurity challenges. When the public and private sectors operate separately to cater to their own security needs, there are often cybersecurity loopholes that hackers and other actors can exploit. The most basic vulnerabilities start to get exploited and this can only be curbed by a strengthened partnership between the two⁹⁶.

One of the biggest entities to be effected by cybersecurity breaches are businesses and private-sector enterprises. When their information is compromised, they end up paying millions of dollars in ransom. On the other hand, if the same funds were utilized to help develop and implement cybersecurity policies, the state could improve cyberspace securitization. This would lead to fewer breaches and a more sustainable cyber environment.

4.3 Challenges Unique to Pakistan's Cybersecurity Landscape

Although the aforementioned challenges apply to cybersecurity policy formation of states in general, the case study of Pakistan is more unique. Pakistan's cybersecurity landscape leaves much to be desired eventhough in the recent decade, significant improvements in cybersecurity culture have been made.

The National Cyber Security Policy of 2021 is a good initiative towards the development of a sound cyber security structure. However, there are several enablers that can influence the

⁹⁶ Eugenia Lostri, James Andrew Lewis, and Georgia Wood, "A Shared Responsibility: Public-Private Cooperation for Cybersecurity" (CSIS, March 2, 2022).

effectiveness of this policy, including resources, talent scarcity in the cybersecurity area, and awareness⁹⁷. There are some issues as to the lack of regulation since the legal frameworks and other measures are still evolving in the region.

Some legal rules and policies like the Electronic Transaction Ordinance 2002, Prevention of Electronic Crimes Act (PECA) 2016 and guidelines from State Bank of Pakistan and Pakistan Telecommunication Authority also provide some protection⁹⁸. Nonetheless, these laws are often accused of failing to provide an adequate and enforceable framework. The policy recognizes these constraints and seeks to overcome them, but the process has been rather gradual.

Regardless of the efforts that have been made, there are some stark challenges that stand in the way of proper cybersecurity policy development in Pakistan. Once these challenges are addressed, we can look towards forming a more inclusive policy that helps create a better cybersecurity culture and integration international, regional and national frameworks.

4.3.1 Critical Infrastructure

The most essential area Pakistan is currently lacking in is cyber-secure critical infrastructure. Although many state institutions such as NADRA, FBR, and more are digitizing with the growth of ICTs, the modernization and safety of the computer networks in these institutions are

⁹⁷ Ministry of IT & Telecom. *National Cyber Security Policy 2021*. Government of Pakistan, 2021. <https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf>.

⁹⁸ Government of Pakistan, *The Electronic Transaction Ordinance 2002*, accessed from <https://pkcert.gov.pk/wp-content/uploads/2023/07/Electronic-Transaction-Ordinance-2002.pdf>;

questionable⁹⁹. There are many contracted companies that work with the armed forces and even parliamentary offices that have been subjected to cyber breaches in the last few years.

As the state continues to digitise, updating offices with proper equipment to create a cyber-secure critical infrastructure is essential¹⁰⁰. Any hacks into these areas of interest would be detrimental for state security. And yet when the cybersecurity policies of the state are examined, there is no emphasis on how update the critical infrastructure or make it more secure¹⁰¹.

4.3.2 Establishment of CERTs

Until 2023, CERTs were not a major part of Pakistan’s cybersecurity framework. Although recent efforts by the government have led to the establishment of these rules, they have yet to be implemented. When cyber security professionals were asked about the effectiveness of these new CERT rules, they were not impressed. Like most legislation regarding cybersecurity policy in the state, these CERTs have also been established with no critical infrastructure to back up their work.

However, to give credit where due the new institution of PKCERT is focusing on spreading awareness and building organizational capacity. It is too early to tell how much of a success they will be but without proper CERTs, there can no proper formation and implementation of Pakistan’s cybersecurity policy.

⁹⁹ Jawad Hussain Awan et al., “Security of EGovernment Services and Challenges in Pakistan,” 2016 SAI Computing Conference (SAI), July 13, 2016.

¹⁰⁰ Muhammad Riaz Shad, “Cyber Threat Landscape and Readiness Challenge of Pakistan,” *Strategic Studies* 39, no. 1 (April 24, 2019): 1–19.

¹⁰¹ Sara Ahmed, “Cyber Security Threat and Pakistan’s Preparedness: An Analysis of National Cyber Security Policy 2021,” *Pakistan Journal of Humanities and Social Sciences Research* 5, no. 1 (June 30, 2022): 25–40.

4.3.3 Regional Framework

Many researchers have pointed out that Pakistan's cybersecurity framework has no link to other regional states that face similar issues. Pakistan, India and China are the most cyber-active states in the region with the first two growing their IT industries at unprecedented rates. Having a shared framework to address common issues not only helps build better policies but also widens the security net to fall back on¹⁰².

This is a challenge that has to be addressed. Pakistan's cyber security policy takes inspiration from international approaches and applies them to the state without seeing its compatibility with the state's cybersecurity landscape. A collection of frameworks in a regional setting could help identify loopholes and make a policy that is a better fit.

4.3.4 Multi-Level Approach

Another challenge to good cyber security policy formation in the state is that there isn't a multi-level approach to cyber security. It is generally seen as ensuring the security of the state institutions and organizations. Yet, there isn't much of an effort made to proliferate it into a top-bottom approach. As discussed earlier, most cyber attacks are the direct result of human error.

When the individual and computer system level of cybersecurity management isn't taken into consideration for national policies, the policy becomes ineffective. Cybersecurity professionals agree that policymaking in Pakistan does not involve enough experts in the field to bridge organizational-level practices and state-level frameworks to make policies that last.

¹⁰² Dr. Tughral Yamin, "Cyberspace Management in Pakistan," *Governance and Management Review* 3, no. 1 (2018).

4.3.5 Precautionary Measures

When reviewing the National Cybersecurity Policy 2021, it is evident that there aren't enough precautionary measures being suggested. The policy aims to tackle cyber breaches and attacks but doesn't put forward any plan to build cyberinfrastructure that can identify, stop, and resolve these threats. As explained by industry experts, a good cybersecurity policy outlines contingency plans on multiple levels in case of a security breach. The goal isn't to prevent breaches from happening, it is to minimize the damage caused by them and to identify a breach in time to stop it.

This is why it is evident that Pakistan's current policy trajectory is more reactive than proactive in nature. We must focus on positive endeavors such as the PTA-issued Cybersecurity Strategy 2023-2028 that outlines some of these infrastructural and technical measures. It mainly focuses on legal framework, cyber resilience, proactive monitoring and incident response, capacity building, cooperation and collaboration, and public awareness.

4.3.6 Cyber-Defense Prioritization

Lastly, we have the issue of cyber-defense prioritization. Pakistan faces a multitude of security challenges, many traditional in nature, that preoccupies its defense prioritization. There is a lack of civil-military partnerships in terms of creating good cybersecurity laws and cyber-defense systems. The military is believed to have advanced cyber-security structures, but they are not translated into state-level practices¹⁰³.

To create better policies that have enough state focus and implementation funds, it is essential that Pakistan makes cybersecurity a defense priority. With regard to the advancement India is achieving

¹⁰³ Syeda Sundus Anwar and Tughral Yamin, "Civil Military Cooperation (CIMIC) in Cyber Security Domain: Analyzing Pakistan's Prospects," *Global Strategic & Securities Studies Review* VI, no. I (March 30, 2021): 68–81.

in the field, Pakistan cannot afford to take its time catching up to speed. Once the government realizes the impact high-level cyber threats can have on state security, it would promote a more robust and responsible stance towards policy making.

Conclusion

Cybersecurity is an essential aspect of state security, especially in the case of Pakistan. Although states have started to make cybersecurity policies and frameworks to minimize cyber threats, there aren't many international or regional-level frameworks for states to follow. When creating a cybersecurity policy, there are many issues that states face, such as a lack of funds, choosing between state security and citizen privacy, the dynamic nature of threats, and more.

In the case of Pakistan, its cybersecurity landscape leaves much to be desired. Now that the challenges in creating an effective policy have been identified, one can move towards drawing suggestions and confusing research on how to improve it. Given how ICTs are evolving, Pakistan can no longer ignore the fact that cybersecurity is a security threat to the state. It must take a more robust stance towards strengthening the state's cyberinfrastructure if it is to stand strong in the digitized world of the future.

Chapter 5:

CONCLUSIONS

Cyber security has emerged as one of the most important aspects of national security, economic prosperity, and social well-being in modern society. For Pakistan, the role of cybersecurity has become even more significant due to the country's current process of digitalization. Although the country has been gradually developing digital solutions like e-governance, online banking, and smart cities, this creates new risks.¹⁰⁴ In this regard, cybersecurity measures are vitally important to ensure the prevention of malicious actions against key objects and data. First and foremost, in the present globalized society, cybersecurity is an essential part of the national defense that demands clear policies and strategies to prevent various threats.

Initially, there were doubts that the 2022 BrahMos missile incident could be a cybersecurity breach because the technology used the Internet of Military Things (IoMT), and it could be manipulated, leading to unauthorized launches or information theft.¹⁰⁵ There are also examples of significant cyber incidents, such as the 2018 and 2021 cyber-attacks on the Pakistani banking sector, which affected thousands of customers' information. Specific industries, including finance, healthcare, and energy, are experiencing the most damage.¹⁰⁶

¹⁰⁴ Sarfraz Batool, Shahzad Ali Gill, Saba Javaid, and Ali Junaid Khan, "Good Governance via E-Governance: Moving Towards Digitalization for a Digital Economy," *Review of Applied Management and Social Sciences* 4, no. 4 (2021): 823-836, accessed from: <https://ramss.spcrd.org/index.php/ramss/article/view/186>.

¹⁰⁵ Geetali Banerji, Yogesh Kumar, Yash Mittal, and Mayank Chaubey, "A Study on Internet of Military Things," *IITM Journal of Information Technology*, p. 31, <https://iitmjp.ac.in/wp-content/uploads/2024/03/BOOKLET-2024.pdf#page=31>.

¹⁰⁶ Laraib Aslam, Rabbia Khalid, Sibtain Ali Bukhari, Manisha Shabbir, Sundus Tehreem Bilal, and Sobia Aqil, "Click, Hack, Vanish: The Growing Threat of Cyberattacks on Pakistan's Financial Sectors," *Harf-o-Sukhan* 8, no. 2 (2024): 309-325, <https://www.harf-o-sukhan.com/index.php/Harf-o-sukhan/article/view/1323>.

Currently, Pakistan is in the process of constructing clear cybersecurity strategies and policies due to the growing concerns regarding threats and risks. The National Cyber Security Policy of 2021 is a good initiative towards the development of a sound cyber security structure.¹⁰⁷ However, there are several enablers that can influence the effectiveness of this policy, including resources, talent scarcity in the cybersecurity area, and awareness. However, there are some issues as to the lack of regulation since the legal frameworks and other measures are still evolving in the region. That is why there is a need for an overall and interconnected approach to cybersecurity policy.

The purpose of this chapter is to articulate the guidelines for constructing and implementing an efficient cybersecurity strategy for Pakistan. It will cover strategic planning, policy formation, execution, tracking, and international cooperation, with a focus on enhancing cybersecurity awareness in Pakistan. Importantly, the success of these efforts relies on the active participation and contributions of all stakeholders, underscoring the shared responsibility in safeguarding Pakistan's digital landscape.

5.1 Analysis of Research Findings

The conducted interviews showed that many stakeholders (be it academia, cybersecurity professionals, government employees, and hackers) believed that the current cybersecurity policies are merely decorative with close to no room for proper implementation. Out of the National Cyber Security Policy 2021 and PTA's Cybersecurity Policy 2023-2028, many interviewees preferred the latter. This is mainly because the newer policy had some focus on international and regional partnerships, yet it hasn't been put into effect. It is, however, seen as a step in the right direction.

¹⁰⁷ Ministry of IT & Telecom. *National Cyber Security Policy 2021*. Government of Pakistan, 2021. <https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf>.

The greatest issue that many professionals brought to light was the lack of a framework to bring the nation under a unified national cyber security culture. Depending on their field and organization, many believed certain sectors such as Banking and Fintech had better cybersecurity policies since they relied on privatized companies to provide them with better security. In terms of governmental organizations, telecom ministries and offices such as PTA had better frameworks to protect themselves against cyber threats.

Those who were in academia believed that Pakistan's cybersecurity culture did not collaborate enough with professionals in the field, resulting in policies like the National Cybersecurity Policy of 2021. This hindered implementation and led to the creation of policies that were merely decorative, never going beyond the surface-level understanding of cybersecurity. But, when discussing the narrative with PTA officials and those in governmental organizations, it became clear that these sentiments are being recognized at a national level.

With the establishment of organizations such as PKCERT and the majority of its team being led by prominent academic and professional figures in cybersecurity, it can be assumed that we're heading in the right direction. It is important to take this with a grain of salt as these efforts are still new and have yet to bear fruit. However, discussing with the involved stakeholders has brought about hopeful expectations for the future as there are many cyber-related projects underway.

5.1.1 Verification of Hypothesis

The rest of the data from primary and secondary research has been categorized into an in-depth analysis of the current state of cyber-security in Pakistan and the recommendation of a more concise

way to make a policy. The research findings also validate the hypothesis as bettering security policies and frameworks in Pakistan can effectively protect it from the upcoming security threats.

5.2 Existing Policies and Frameworks

In order to address cybersecurity issues in Pakistan, the National Cyber Security Policy 2021 and the PTA Cybersecurity Strategy 2023-2028 have been put into effect to provide a secure and protected cyber environment in areas such as cyber governance, active defense, protection of critical information infrastructure or CII, and public-private partnerships. Nevertheless, there is a myriad of challenges and gaps that remain even with these efforts in place. The policies identify the need for a central Cyber Governance Policy Committee (CGPC) for strategic direction and recommend an organizational structure for the implementation of the policy.¹⁰⁸ However, the strength of these structures is dented by poor implementation and lack of integration between sectors. The policies also identify legal frameworks and a continuous improvement approach; however, the operationalization of the policy is still weak and sporadic.

Some legal rules and policies like the Electronic Transaction Ordinance 2002, the Prevention of Electronic Crimes Act (PECA) 2016, and guidelines from the State Bank of Pakistan and the Pakistan Telecommunication Authority also provide some protection.¹⁰⁹ Nonetheless, these laws

¹⁰⁸ Ministry of IT & Telecom. *National Cyber Security Policy 2021*. Government of Pakistan, 2021, p. 8. <https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf>.

¹⁰⁹ Government of Pakistan, *The Electronic Transaction Ordinance 2002*, accessed from <https://pkcert.gov.pk/wp-content/uploads/2023/07/Electronic-Transaction-Ordinance-2002.pdf>;

are often accused of failing to provide an adequate and enforceable framework. The policy recognizes these constraints and seeks to overcome them, but the process has been rather gradual.

5.3 Current Threats and Vulnerabilities

Recent and infamous cases, including the cyber-attack on the banking sector, which led to the leakage of thousands of customers' data, demonstrate the vulnerability of the country to cyber threats. Other major threats include ransomware attacks, phishing campaigns, and espionage. It has been highlighted that one of the biggest risks is the use of hardware and software imported from abroad, which may contain backdoors and malware and make the systems prone to cyber threats.¹¹⁰ In addition, there is a deficiency of cybersecurity experts, as the number of professionals available to meet the current and future needs of digital literacy remains limited.¹¹¹ This gap means that many organizations are not prepared to respond to today's advanced level of cyber threats.

The policy also addresses issues with data governance and discusses the concept of data colonization, which refers to data management and processing outside the legal framework of Pakistan. This lack of control leads to cases of unauthorized access and exploitation of sensitive information, as indicated by the Ministry of IT & Telecom.¹¹² In particular, the absence of a unified approach and integrated mechanisms on the part of response teams for cybersecurity incidents hampers the overall cybersecurity situation.

¹¹⁰ Ministry of IT & Telecom. *National Cyber Security Policy 2021*. Government of Pakistan, 2021, p. 3. <https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf>.

¹¹¹ National Cyber Security Policy 2021, Government of Pakistan (2021), p. 2.

¹¹² National Cyber Security Policy 2021, Government of Pakistan (2021), p. 4.

5.4 Stakeholder Analysis

Cybersecurity cannot be a solo effort between two entities; it is a shared responsibility between the government, business, academia, and civil society. However, in Pakistan, such a successful partnership remains a challenge due to certain government and implementation hurdles.

Government Bodies: The government of Pakistan has also established the Ministry of Information Technology & Telecommunication (MoIT&T), which works on policy formulation and sector regulation. However, in most organizations, the process of deploying cybersecurity measures is impeded by bureaucratic rigidity and fragmentation. The National Cyber Security Centre and sector-specific Computer Emergency Response Teams (CERTs) exist but require enhancement and resources.

Private Sector: Among the key partners, private actors, especially companies that operate in sensitive fields, including finance and telecommunications, have become prominent in cybersecurity. However, the problem is that most private organizations are not in a position to invest in or even lack the technical know-how of implementing strong cybersecurity measures. However, there is a common resistance to disclosing information regarding cyber incidents as it is associated with adverse effects on reputation.

Academia: Universities and other academic institutions are likely to play a key role in cultivating professional talent in the cybersecurity field. Efforts such as the offering of cybersecurity degree programs by the Higher Education Commission (HEC) are encouraging, yet the difference between academic production and industrial demand is still considerable. Currently, 22

educational institutions are offering courses in cybersecurity; however, the quality of the learned lot produced is greatly affected by the lack of research and development funding and extensive research. It is, therefore, clear that there is more to be done to ensure that the available academic programs prepare students for the current and future challenges in the cybersecurity field.

Civil Society: It is important for people to learn about the threats posed and how they can protect themselves from them. But, the problem with most public awareness campaigns is that they are not well-coordinated and lack the necessary scope and intensity. To address the problem, there are some recommendations that are required to be implemented in order to educate the public more on the issue of cybersecurity and ways to prevent it.

5.5 Planning Stages for a Sound Cybersecurity Policy

Developing a sound cybersecurity policy takes a hands-on approach from the government, the state's cybersecurity professionals and of-course, the academia. Here are the proposed planning stages for creating such a policy:

5.5.1 Defining Objectives and Goals

In the case of Pakistan, there is a need for a well-articulated, comprehensive, sound cybersecurity policy that is anchored on clear objectives and goals. The following objectives should also be considered relevant to the national interest, economic well-being, and the rights of individuals to privacy and data protection. The primary objectives of the policy should include: The primary objectives of the policy should include:

Protecting Critical Information Infrastructure (CII): It is crucial to maintain the security and reliability of CII systems, including banking and energy systems, as well as communication networks. To this end, Pakistan may follow Estonia whose government has established measures to enhance the protection of its digital resources and thereby positioning the country as a leader in global cybersecurity.¹¹³

Enhancing Data Privacy and Security: It is important to protect personal and sensitive information from being accessed or stolen by unauthorized persons. The European Union’s General Data Protection Regulation (GDPR) can be used to learn from as it provides robust protection of data and people’s information and has been successful in its implementation.¹¹⁴

Promoting a Secure Digital Economy: Assuring the safety of purchasing products and services via the Internet through online certification and safe payment methods. The Smart Nation Singapore initiative, which states that cybersecurity is a key element in the city-state’s digitalization strategy, is instructive.¹¹⁵

Building Cybersecurity Capacity: The creation of a resourceful workforce qualified to confront new and evolving threats through education and training. Israel has identified education and training as a key area of focus in building a strong cybersecurity workforce, especially for its military personnel.¹¹⁶

¹¹³ Terry Gjelten, “Estonia, the Digital Republic,” *The New Yorker* (2017), <https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic>.

¹¹⁴ Peter Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, 1st ed. (Cham: Springer International Publishing, 2017), <https://doi.org/10.1007/978-3-319-57959-7>.

¹¹⁵ Singapore Government, “Smart Nation: A Digital Government,” (2018), <https://www.smartnation.gov.sg>.

¹¹⁶ Dan Senor and Saul Singer, *Start-up Nation: The Story of Israel’s Economic Miracle* (McClelland & Stewart, 2011).

5.5.2 Conducting Risk Assessments

Risk analysis is a critical process of risk management that helps in the identification and ranking of cybersecurity risks. This process involves assessing the risks that are posed by the key systems and the possible consequences that different types of cyber threats can have. A practical approach includes:

Identifying Assets and Threats: Defining the assets that are most valuable in the context of the digital environment and the threats that can affect them. For example, the United States' National Institute of Standards and Technology (NIST) Cybersecurity Framework outlines how to develop an inventory of assets and threats.¹¹⁷

Assessing Vulnerabilities: Identifying the gaps which exist within current systems that will make the networks vulnerable to hacking. This step needs periodic security audit and vulnerability assessments including risk assessment and risk analysis. Some strategies that can be taken from the UK's National Cyber Security Centre are they provide an all-encompassing Vulnerability Assessment Services for the public and private sectors.¹¹⁸

Evaluating Potential Impacts: Assessing the possible effects of different incidents in the cyberspace on national security, economic well-being, and human lives. This assessment enables one to rank risks in order of their importance as potential threats. For instance, in Japan, impact assessments are conducted before making any policy decisions regarding cybersecurity.¹¹⁹

¹¹⁷ NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (2018), <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

¹¹⁸ NCSC, "Vulnerability Assessment," (2020), <https://www.ncsc.gov.uk/>.

¹¹⁹ Japan Ministry of Internal Affairs and Communications, "Cybersecurity Strategy," (2015), http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/cybersecurity/index.html.

Developing Mitigation Strategies: Proposed measures for risk management where strategies have to be put in place to prevent the occurrence of identified risks. This entails taking preventive measures through the use of technical controls such as firewalls and intrusion detection systems and non-technical control measures through training and awareness. According to the Australian Cyber Security Centre, the Essential Eight mitigation strategies that Pakistan can adopt have been identified.¹²⁰

5.6 Framework for Cybersecurity Policy Development

From the conducted research, it was identified that Pakistan needed a thorough and concise framework for policy development. This can be done by establishing the following:

5.6.1 Governance Structure

National Cybersecurity Council (NCSC)

A strong governance structure is crucial in the formulation and enforcement of cybersecurity policies in Pakistan. It should define the roles, responsibilities, and relationships of the various participants to facilitate sound governance. There should be one common body that coordinates and has control over all the national cyber security programs, policy-making, and strategic direction of the country, for instance, the National Cyber Security Council (NCSC). This council should include members from the Ministry of Information Technology & Telecommunication

¹²⁰ Australian Cyber Security Centre, “Essential Eight Explained,” (2019), <https://www.cyber.gov.au/sites/default/files/2023-05/PROTECT%20-%20Essential%20Eight%20Explained%20%28May%202023%29.pdf>.

(MoIT&T), law enforcement, military, key ministries, and sensitive sectors such as finance and telecom. For example, in South Korea, the government and private sectors work hand in hand to come up with the best strategies for the NCSC, as evidenced by the enhanced national cybersecurity strategies.¹²¹

Sectoral Computer Emergency Response Teams & Provincial and Organizational Cybersecurity Offices

Moreover, Computer Emergency Response Teams (CERTs) should be created for specific sectors to address incidents of threats and collaboration with the NCSC. For instance, the Financial Services Information Sharing and Analysis Center (FS-ISAC) in the United States has one of the roles of promoting sector-specific cybersecurity in the financial sector by sharing intelligence information and best practices among members.¹²² In addition, the provincial and organizational cybersecurity offices play an important role in the enforcement of national cybersecurity policies and the management of incidents. This is why Germany has divided cybersecurity into regional approaches, where countermeasures are taken as soon as threats are identified.¹²³

¹²¹ National Cybersecurity Organisation: Republic of Korea, Sungbaek Cho, NATO CCDCOE Strategy Researcher, <https://ccdcoe.org/uploads/2022/12/ROK-Country-report.pdf>.

¹²² Pomerleau, P. L., Lowery, D. L., “The Evolution of Cybersecurity within the American Financial Sector,” in *Countering Cyber Threats to Financial Institutions: A Private and Public Partnership Approach to Critical Infrastructure Protection* (2020), 29-45, https://link.springer.com/chapter/10.1007/978-3-030-54054-8_3.

¹²³ Scott N. Romaniuk and Michael Claus, “Germany’s Cybersecurity Strategy: Confronting Future Challenges,” in *Routledge Companion to Global Cyber-Security Strategy* (Routledge, 2021), 73-88.

5.6.2 Cybersecurity Laws

PTA Cybersecurity Strategy 2023-2028, National Cyber Security Policy 2021; Prevention of Electronic Crimes Act (PECA) 2016

Currently, Pakistan does not have a comprehensive data protection law, but it has the National Cyber Security Policy 2021 and the Prevention of Electronic Crimes Act (PECA) 2016. However, there are some significant areas where these documents lack. The current National Cyber Security Policy 2021 emphasizes data protection, but the policy is general and lacks specific procedures and mechanisms for adequate data protection. Likewise, the PECA 2016 also has provisions regarding data protection but has been accused of having ambiguous and weak language as well as protection mechanisms. This non-clarity in the laws makes it difficult to determine what is allowed and what is prohibited, hence diluting the impact of these laws in protecting PII and other sensitive data.

International Comparisons

- **European Union's General Data Protection Regulation (GDPR)**

The European Union's General Data Protection Regulation (GDPR) has one of the highest standards of data protection with a clear and elaborate framework. It is important to note that the GDPR gives a detailed definition of data processing, consent, and rights of individuals, whereby data protection is enhanced. Its scope and terms are general and specific when it comes to data protection matters and it offers robust protection measures that are not currently available in the laws of Pakistan. In addition, GDPR has very clear and specific rules and regulations, which if violated, come with heavy penalties that have put data protection at a high standard among the

member countries.¹²⁴ This level of enforcement is missing in Pakistan's current legal framework where weak penalties and weak regulation hinder the efficiency of data protection laws.

- **Singapore's Personal Data Protection Act (PDPA)**

Similarly, the legal framework of data protection in the Singapore is supported by the Personal Data Protection Act (PDPA). The PDPA has identified specific duties that are expected of organizations when it comes to the collection, use, and sharing of personal data. This has the effect of stressing the importance of compliance and coming down heavily on anyone who fails to adhere to the standards set.¹²⁵ This approach that Singapore has taken into consideration shows that in order to protect data, there must be well-defined rules and regulations and rigorously implemented measures.

Recommendations for Pakistan

A Comprehensive Data Protection Law: To overcome these challenges, Pakistan should consider enacting a robust and comprehensive data protection law in line with the GDPR and the PDPA of Singapore. We should have a new law that defines the rules on data processing and consent, as well as individual rights, in detail to guarantee efficient protection of personal data.

Strengthen Regulatory Authority: Similarly, it is important to enhance the measures that are in place for the enforcement of the laws. The establishment of a powerful regulatory authority like the National Cyber Crime Investigation Agency (NCCIA) with a clear mandate separate from the

¹²⁴ Peter Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, 1st ed. (Cham: Springer International Publishing, 2017), <https://doi.org/10.1007/978-3-319-57959-7>.

¹²⁵ D. Setiawati, H. A. Hakim, and F. A. H. Yoga, "Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore," *Indonesian Comparative Law Review* 2, no. 2 (2020): 95-109.

Federal Investigation Agency (FIA) is needed. But, it must have sufficient resources and the necessary legal mechanisms to compel compliance can help to promote the protection of data. This authority should have the capacity to impose stiff consequences for any violations of the data protection regulation so as to discourage non-adherence.

Introduction of Clear and Precise Language: There are some issues that need to be addressed in Pakistan's data protection laws, one of which is the language used should be easier to understand. PECA 2016 has been critiqued for its broad and ambiguous language, which has been associated with unpredictable implementation. The use of clear terminology in the new data protection law can, therefore, lead to the same application and comprehension of the law and would, therefore, be useful in the protection of data. It is also important to note that laws and regulations should also be reviewed periodically in order to address the current and emerging threats, as well as the new technologies that exist in cyberspace.

5.6.3 Policy Components

To effectively address all the elements of cybersecurity, it is crucial to have a well-rounded cybersecurity policy with several components, including:

Incident Response and Crisis Management: This includes coming up with a national incident response plan, conducting routine exercises and scenarios, and formation of a national cyber incident response team. For instance, the US National Cyber Incident Response Plan (NCIRP)

outlines the framework of coordinated response between the public and private sectors in the face of cyber threats.¹²⁶

Public-Private Partnerships: Such cooperation is crucial for the fight against cyber threats and includes legal and institutional frameworks as well as information exchange tools on the federal and non-federal levels between the public and private sectors. The UK's Cyber Security Information Sharing Partnership (CiSP) is another example of how sharing cyber threats can be done in real time between sectors.¹²⁷

Capacity Building and Awareness Programs: Measures that need to be adopted for the development of proper cybersecurity policies include training, integration of cybersecurity courses in educational institutions, and public awareness. The Israel Cyber Education Center provides a good example of this model, with a wide range of training courses and educational programs that help develop the capacity in the field of cybersecurity from the early years of school.¹²⁸

Protection of Critical Information Infrastructure (CII): This component has to be secured with a high level of security and should be regularly audited for compliance with national security standards. The European Programme for Critical Infrastructure Protection (EPCIP) also focuses

¹²⁶ Quentin E. Hodgson, A. A. R. O. N. Clark-Ginsberg, Zachary Haldeman, Andrew Lauand, and Ian Mitch, "Managing Response to Significant Cyber Incidents," (2022), https://www.rand.org/content/dam/rand/pubs/research_reports/RAA1200/RAA1265-4/RAND_RRA1265-4.pdf.

¹²⁷ I. Burak Tolga and Gunnar Faith-Ell, "Information Sharing Framework for Penetration Testing," *NATO Cooperative Cyber Defence Centre of Excellence* (2020), https://www.ccdcoe.org/uploads/2020/04/Paper_version_Final3.pdf.

¹²⁸ Lior Tabansky, Isaac Ben Israel, "The National Cyber-Strategy of Israel and the INCB," in *Cybersecurity in Israel* (2015), 49-54, https://link.springer.com/chapter/10.1007/978-3-319-18986-4_7.

on safeguarding CII in each EU member state to ensure that the systems that are in place are effective and secure.¹²⁹

Risk Management Framework: It is crucial to carry out the risk assessments on a continuous basis, put in place measures to address the identified risks, and ensure that there are appropriate changes to the security framework. The Australian Cyber Security Centre’s Essential Eight has recommended guidelines that can be applied in different organizations to prevent cyber threats and risks.¹³⁰

International Cooperation: In this regard, it is vital to participate in the international cyberspace initiatives, build partnerships and implement the best practices of the international partners in the cybersecurity policy. South Korea’s active engagement in the international cybersecurity forums and relations with the international organizations for cybersecurity strengthens the overall cybersecurity of South Korea.¹³¹

With the incorporation of these elements, Pakistan can come up with a complete and well-coordinated cybersecurity policy. In this regard, the best practices from around the world and their adaption to Pakistan will help in developing a strong cybersecurity system that would be able to manage and respond to the cyber threats of today and tomorrow.

¹²⁹ Marzio Di Feo and Luigi Martino, “Public–private partnership (PPP) in the context of European Union policy initiatives on critical infrastructure protection (CIP) from cyber attacks,” in *Governing Complexity in Times of Turbulence* (2022), 54-79, <https://www.elgaronline.com/edcollchap/edcoll/9781800889644/9781800889644.00014.xml>.

¹³⁰ Australian Cyber Security Centre, “Essential Eight Explained,” (2019), <https://www.cyber.gov.au/sites/default/files/2023-05/PROTECT%20-%20Essential%20Eight%20Explained%20%28May%202023%29.pdf>.

¹³¹ National Cybersecurity Organisation: Republic of Korea, Sungbaek Cho, NATO CCDCOE Strategy Researcher, <https://ccdcoe.org/uploads/2022/12/ROK-Country-report.pdf>.

5.7 Implementation Strategies

5.7.1 Resource Allocation

The resource management in the implementation of a cybersecurity policy must be done in an appropriate manner. Pakistan should focus on adequate funding for cybersecurity efforts; the government should ensure that proper resources are allocated to people and technologies.

The government should release funds to purchase new cybersecurity technologies and tools and upgrade the current structures. Creating a fund for cybersecurity can provide for continuing and future endeavors. For instance, expenditure on the procurement and maintenance of continuous monitoring systems and intrusion detection technologies can greatly improve the cybersecurity of the country.

5.7.2 Capacity Building and Training

The cybersecurity workforce is a necessity, and it has to be trained. Pakistan needs to develop a better training regime for its IT workforce, law enforcement agencies, and government employees. In addition, the creation of cybersecurity training academies and certification programs can go a long way in addressing the shortage. Possible cooperation with international counterparts for training and certifications can also help develop local capacity. There is a need for frequent training in the form of workshops and seminars to update stakeholders on current trends and threats in cybersecurity. To address this issue, amplifying the cybersecurity courses offered in universities and technical institutions is a way of ensuring that future employees are ready.

5.7.3 Public Awareness and Education

It is crucial to educate the public on potential cybersecurity threats and how to prevent them. There should be mass awareness campaigns across the country through all media channels regarding online safety and strategies to avoid phishing scams and protect our data. It is recommended that elementary schools include basic cybersecurity lessons in the curriculum so that students are reminded of the proper way to act. To get tips and resources on how to protect personal information online, one can visit government websites and their social media pages. In addition, the beginning of a national cybersecurity awareness month may lead to an increase in attention to cybersecurity matters and enhance the involvement of the public.

5.7.4 Technology and Innovation

To prevent cyber threats, it is crucial to invest in the most advanced cybersecurity tools and promote the development of new solutions. The government of Pakistan should encourage research and development in the field of cybersecurity in the form of grants and incentives for private and public sector proponents. Cooperating with IT companies and start-ups may help to enhance the level of security and develop modern and efficient solutions in the sphere of cybersecurity that suit the specific region. Some of the recent technologies that can enhance the capabilities of threat detection and response to risks include the use of artificial intelligence and machine learning. Using blockchain technology for transaction and data protection can also enhance cyber security measures to further safeguard information.¹³²

¹³² Vinden Wylde, Nisha Rawindaran, John Lawrence, Rushil Balasubramanian, Edmond Prakash, Ambikesh Jayal, Imtiaz Khan, Chaminda Hewage, and Jon Platts, "Cybersecurity, Data Privacy and Blockchain: A Review," *SN Computer Science* 3, no. 2 (2022): 127, <https://link.springer.com/article/10.1007/s42979-022-01020-4>.

Thus, through proper resource management, the establishment of training programs, the enhancement of public awareness, and the promotion of technology, it is possible for Pakistan to successfully realize its cybersecurity policy. This enhanced strategy will build a strong cybersecurity strategy that will address the threats that affect our nation and respond to new and challenging cyber threats.

5.8 Monitoring and Evaluation

In order to assess the efficiency of the cybersecurity policies, it is necessary to define the KPIs to track the results and progress. Some of the possible KPIs should be the number of detected and prevented cyber threats, the time taken to address a particular incident, the compliance with the set cybersecurity standards, and the level of users' awareness and the training completed. Periodic inspections and assessments should be done so as to determine the organization's level of compliance and compliance gaps. For instance, a KPI could be the decrease in the number of successful phishing incidents after the organization's awareness campaigns.

KPI Name	Location	Agencies Involved
Incident Detection and Response Time	United States	Department of Homeland Security (DHS)
Patch Management	Japan	National Center of Incident Readiness and Strategy for Cybersecurity (NISC)
User Awareness and Training Completion	Israel	Israeli National Cyber Directorate (INCD)
Vulnerability Management	Australia	Australian Cyber Security Centre (ACSC)

Mean Time to Recover (MTTR)	Germany	German Federal Office for Information Security (BSI)
-----------------------------	---------	--

Table 1: Key Performance Indicators (KPIs) Used Worldwide

(Source: GDPR, NIST, NCSA)

5.8.1 Continuous Improvement Mechanisms

Mechanisms of continuous improvement are important in order to guarantee that cybersecurity is efficient in facing new challenges. This entails the identification and management of cybersecurity audits, threats, and incidents by revising the policies and procedures periodically. Thus, it is critical to implement a closed-loop process in which the lessons learned from the incidents could be applied to improve the effectiveness of the security measures. For instance, after a major cyber event, it is important to perform a root cause analysis to identify the weaknesses that were exploited and use the information to make changes in security measures and employee awareness programs. Also, it is crucial to be aware of the worldwide cybersecurity issues and implement the existing recommendations to support the ongoing improvement process.¹³³

The training and awareness programs should also be conducted and revised on a routine basis for new threats and to include new information on cybersecurity. Engaging with international cybersecurity organizations can be useful in order to gain knowledge and tools for the further enhancement of the national cybersecurity framework. Automated tools, which are used to generate data and analytics in real-time, can help in the improvement process as they are able to show possible risks and address them in a timely manner.

¹³³ Peter Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, 1st ed. (Cham: Springer International Publishing, 2017), <https://doi.org/10.1007/978-3-319-57959-7>.

Conclusion

To have an all-encompassing and successful cybersecurity strategy in Pakistan, the following domains need to be considered. First of all, the general legislation concerning cybersecurity should be extended and solidified by adopting the Cybersecurity Act. This law should articulate what it precisely encapsulates, the ambit of the law, and the measures that have been put in place to enforce compliance, which was well demonstrated in Singapore when they enacted the Cybersecurity Act 2018. The strengthening of the regulatory authority can be done by creating a strong body that is capable of carrying out all the mandates and has enough resources to enable it to carry out the necessary actions.

In order to extend the public's understanding, promote the message through campaigns, and integrate the topic of cybersecurity in schools and colleges, much can be done to build a culture of cybersecurity. Also, the improvement of the public-private partnerships and technological advancement through the provision of grants as well as collaboration with the technology firms to develop the best and most modern security technologies for use. As mentioned, the assessment of risks on a frequent basis and modifications in security measures and frameworks are vital to combat cybercrimes.

For this reason, the current situation may be considered a turning point in Pakistan's digital transformation process. To achieve this, the following guidelines are recommended to ensure that the country has good and sustainable cybersecurity to protect the nation's interests and foster economic growth. Everyone has to join hands and ensure that the government, private firms, learning institutions, and civil society organizations step up their efforts in the fight against

cybercrime to address the current threat posed by cybercriminals. Thus, Pakistan can ensure the security of the digital future of the country and make cyberspace safer from the possible threats that can occur. It is high time that something is done before it is too late and the harm is done.

BIBLIOGRAPHY:

Aamna Rafiq. "Challenges of Securitising Cyberspace in Pakistan." *Strategic Studies* 39, no. 1 (April 24, 2019): 90–101.

Abbas, Haider, Hiroki Suguri, Zheng Yan, William Allen, and Xiali Sharon Zhang. "IEEE Access Special Section: Security Analytics and Intelligence for Cyber Physical Systems." *IEEE Access* 8 (2020): 208195–98.

Adler, Patricia A., Peter Adler, and Robert S. Weiss. "Learning from Strangers: The Art and Method of Qualitative Interview Studies." *Contemporary Sociology* 24, no. 3 (May 1995): 420.

Ahmad, Sara. "Cyber Security Threat and Pakistan's Preparedness: An Analysis of National Cyber Security Policy 2021." *Pakistan Journal of Humanities & Social Sciences Research* 5, no. 1 (2022): 33.

Ahmed, Sara. "Cyber Security Threat and Pakistan's Preparedness: An Analysis of National Cyber Security Policy 2021." *Pakistan Journal of Humanities and Social Sciences Research* 5, no. 1 (June 30, 2022): 25–40.

Ahmed, Sara. "Cyber Security Threat and Pakistan's Preparedness: An Analysis of National Cyber Security Policy 2021." *Pakistan Journal of Humanities and Social Sciences Research* 5, no. 1 (June 30, 2022): 25–40.

Ahmed, Syed Bilal, and M. Sheryar Khan. "Cyber Threat to Pakistan National Security: National Security and Threat Perception." *Pakistan Review of Social Sciences* 3, no. 1 (2022).

Akram, Muhammad Shehzad, Moneeb Jaffar Mir, and Abdul Rehman. "Dimension of Cyber-Warfare in Pakistan's Context." *Journal of Positive School Psychology* 7, no. 6 (2023): 82–94.

Algarni, Sumaiah. "Cybersecurity Attacks: Analysis of 'Wannacry' Attack and Proposing Methods for Reducing or Preventing Such Attacks in Future." In *ICT Systems and Sustainability: Proceedings of ICT4SD 2020, Volume 1*, 776. Singapore: Springer, 2021. https://link.springer.com/chapter/10.1007/978-981-15-8289-9_73.

Anderson, Chad, Richard L. Baskerville, and Mala Kaul. "Information Security Control Theory: Achieving a Sustainable Reconciliation between Sharing and Protecting the Privacy of Information." *Journal of Management Information Systems* 34, no. 4 (October 2, 2017): 1082–1112.

Anwar, Syeda Sundus, and Tughral Yamin. "Civil Military Cooperation (CIMIC) in Cyber Security Domain: Analyzing Pakistan's Prospects." *Global Strategic & Securities Studies Review* VI, no. I (March 30, 2021): 68–81.

Aslam, Laraib, Rabbia Khalid, Sibtain Ali Bukhari, Manisha Shabbir, Sundus Tehreem Bilal, and Sobia Aqil. "Click, Hack, Vanish: The Growing Threat of Cyberattacks on Pakistan's Financial Sectors." *Harf-o-Sukhan* 8, no. 2 (2024): 309-325. <https://www.harf-o-sukhan.com/index.php/Harf-o-sukhan/article/view/1323>.

Australian Cyber Security Centre. "Essential Eight Explained." 2019. <https://www.cyber.gov.au/sites/default/files/2023-05/PROTECT%20-%20Essential%20Eight%20Explained%20%28May%202023%29.pdf>.

Australian Cyber Security Centre. “Essential Eight Explained.” 2019. <https://www.cyber.gov.au/sites/default/files/2023-05/PROTECT%20-%20Essential%20Eight%20Explained%20%28May%202023%29.pdf>.

Awan, Jawad Hussain, Shahzad Memon, Mahmood Hussain Shah, and Fawad Hussain Awan. “Security of eGovernment Services and Challenges in Pakistan.” *2016 SAI Computing Conference (SAI)*, July 13, 2016, 1082–85.

Awan, Jawad Hussain, Shahzad Memon, Mahmood Hussain Shah, and Fawad Hussain Awan. “Security of EGovernment Services and Challenges in Pakistan.” *2016 SAI Computing Conference (SAI)*, July 13, 2016.

Aziz, Basharat, Faisal Yameen, and Shaukat Hussain Bhatti. “Development of Digital Markets and Protection of E-Consumers.” *Annals of Social Sciences and Perspective* 5, no. 1 (2024): 104. <https://assap.wum.edu.pk/index.php/ojs/article/view/308>.

Backman, Sarah. "Risk vs. Threat-Based Cybersecurity: The Case of the EU." *European Security* 32, no. 1 (2023): 85-103.

Baloch, Rafay. *Ethical Hacking and Penetration Testing Guide*. Auerbach Publications, 2017.

Banerji, Geetali, Yogesh Kumar, Yash Mittal, and Mayank Chaubey. “A Study on Internet of Military Things.” *IITM Journal of Information Technology*, 31. <https://iitmjp.ac.in/wp-content/uploads/2024/03/BOOKLET-2024.pdf#page=31>.

Batool, Sarfraz, Shahzad Ali Gill, Saba Javaid, and Ali Junaid Khan. “Good Governance via E-Governance: Moving Towards Digitalization for a Digital Economy.” *Review of*

Applied Management and Social Sciences 4, no. 4 (2021): 823-836.
<https://ramss.spcrd.org/index.php/ramss/article/view/186>.

Bokhari, Syed Asad Abbas. "A Quantitative Study on the Factors Influencing Implementation of Cybersecurity Laws and Regulations in Pakistan." *Social Science* 2023 12, no. 11 (2023): 629.

Brenner, Susan W. "Cybercrime: Criminal Threats from Cyberspace." *Choice Reviews Online* 48, no. 02 (October 1, 2010).

Buzan, Barry, and Ole Waever. *Regions and Powers: The Structure of International Security*. Cambridge: Cambridge University Press, 2003.

Buzan, Barry, Ole Waever, and Jaap de Wilde. "Security: A New Framework for Analysis." *International Journal* 53, no. 4 (1998).

Buzan, Barry. *People, States & Fear: An Agenda for International Security Studies in the Post-Cold War Era*. Colchester: Ecpr Press, 1983.

Cavelty, Myriam Dunn, and Andreas Wenger. "Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science." *Contemporary Security Policy* 41, no. 1 (October 14, 2019): 5–32.

Chyzhmar, Kateryna, Oleksii Dnipro, Oksana Korotiuk, Roman Volodymyrovych Shapoval, and Olga Sydorenko. "State Information Security as a Challenge of Information and Computer Technology Development." *Journal of Security and Sustainability Issues* 9, no. 3 (March 25, 2020): 819–28.

Crosston, Matthew. "Virtual Patriots and a New American Cyber Strategy: Changing the Zero-Sum Game." *Strategic Studies Quarterly* 6, no. 4 (2012): 100–118.

Curtis, Sarah, Wil Gesler, Glenn Smith, and Sarah Washburn. "Approaches to Sampling and Case Selection in Qualitative Research: Examples in the Geography of Health." *Social Science & Medicine* 50, no. 7-8 (April 2000): 1001–14.

Dalal, Reeshad S., David J. Howard, Rebecca J. Bennett, Clay Posey, Stephen J. Zaccaro, and Bradley J. Brummel. "Organizational Science and Cybersecurity: Abundant Opportunities for Research at the Interface." *Journal of Business and Psychology* 37, no. 1 (February 4, 2021).

Di Feo, Marzio, and Luigi Martino. "Public–private partnership (PPP) in the context of European Union policy initiatives on critical infrastructure protection (CIP) from cyber attacks." In *Governing Complexity in Times of Turbulence*, 54-79. 2022. <https://www.elgaronline.com/edcollchap/edcoll/9781800889644/9781800889644.00014.xml>.

Esentire. "2023 Official Cybercrime Report." *Esentire*, 2023.

<https://www.esentire.com/resources/library/2023-official-cybercrime-report>.

EU - Information Commissioner's Office. "Essential Guide to the General Data Protection Regulation (GDPR)." *Guide to the General Data Protection Regulation (GDPR)*, March 22, 2018.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711097/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf.

Fadziso, Takudzwa, Upendar Rao Thaduri, Sreekanth Dekkati, and Venkata Koteswara Rao Ballamudi. "Evolution of the Cyber Security Threat: An Overview of the Scale of Cyber Threat." *Digitization and Sustainability Review* 3, no. 1 (September 2023): 1–12.

Faleesi, N., R. Gavrilă, M. R. Klejnstrup, and K. Moulinos. "National Cyber Security Strategies: An Implementation Guide." Heraklion, 2012.

<https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide>.

Fang, Binxing. *Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace*. Singapore: Springer; Beijing, China, 2018.

Fatima, Irtā. "Pakistan's Cyber Threat Landscape and Prospects of Regional Cooperation on Cyber Security." *Spotlight on Regional Studies* 40, no. 11 (November 2022).

Federal Financial Institutions Examination Council. "Federal Financial Institutions Examination Council." 2016.

Fonseca-Herrera, Omar A., Alix E. Rojas, and Hector Florez. "A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard." *IAENG International Journal of Computer Science* 48, no. 2 (2021): 213-222.

Fuster, G. G., and Lina Jasmontaite. "Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights." In *The Ethics of Cybersecurity*, edited by M. Christen, B. Gordjin, and M. Loi. Springer Cham, 2020.

Futter, Andrew. "Is Trident Safe from Cyber Attack?," 2016. <https://www.europeanleadershipnetwork.org/wp-content/uploads/2017/10/Is-Trident-safe-from-cyber-attack-1.pdf>.

Gjelten, Terry. "Estonia, the Digital Republic." *The New Yorker*, December 18, 2017. <https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic>.

Gourisetti, Sri Nikhil, et al. *Facility Cybersecurity Framework Best Practices*. No. PNNL-30291. Richland, WA: Pacific Northwest National Lab. (PNNL), 2020.

Government of Pakistan. *The Electronic Transaction Ordinance 2002*. Accessed July 2023. <https://pkcert.gov.pk/wp-content/uploads/2023/07/Electronic-Transaction-Ordinance-2002.pdf>.

Hamdani, Syed Wasif Abbas, Haider Abbas, Abdul Rehman Janjua, Waleed Bin Shahid, Muhammad Faisal Amjad, Jahanzaib Malik, Malik Hamza Murtaza, Mohammed Atiquzzaman, and Abdul Waheed Khan. "Cybersecurity Standards in the Context of Operating System." *ACM Computing Surveys* 54, no. 3 (June 2021): 1–36.

Hathaway, Melissa, and Francesca Spidalieri. "Cyber Readiness at a Glance." 2017.

Hodgson, Quentin E., Aaron Clark-Ginsberg, Zachary Haldeman, Andrew Lauland, and Ian Mitch. "Managing Response to Significant Cyber Incidents." 2022. https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1200/RRA1265-4/RAND_RRA1265-4.pdf.

Hong, Kwo- Shing, Yen- Ping Chi, Louis R. Chao, and Jih- Hsing Tang. "An Integrated System Theory of Information Security Management." *Information Management & Computer Security* 11, no. 5 (December 2003): 243–48.

Hoofnagle, Chris Jay, Bart Van Der Sloot, and Frederik Zuiderveen Borgesius. "The European Union General Data Protection Regulation: What It Is and What It Means." *Information & Communications Technology Law* 28, no. 1 (2019): 65-98.

Ilbiz, Ethem, and Christian Kaunert. "Cybercrime, Public-Private Partnership and Europol." In *The Sharing Economy for Tackling Cybercrime*, 13-28. Cham: Springer International Publishing, 2023.

International Telecommunication Union. "Global Cybersecurity Index 2020." Geneva: ITU Publications, 2020.

Jackson, Eric Blake, Richard Dreyling, and Ingrid Pappel. "A Historical Analysis on Interoperability in Estonian Data Exchange Architecture: Perspectives from the Past and for the Future." In *Proceedings of the 14th International Conference on Theory and Practice of Electronic Governance*, 111-116. 2021.

Japan Ministry of Internal Affairs and Communications. "Cybersecurity Strategy." 2015. http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/cybersecurity/index.html.

Jawad Hussain Awan, Shahzad Memon, Mahmood Hussain Shah, and Fawad Hussain Awan. "Security of eGovernment Services and Challenges in Pakistan." *Institute of Information and Communication Technology*, July 13, 2016.

Kaminska, Monica. "To Retaliate or Not: A Matter of Cyber Risk Perception." PhD diss., University of Oxford, 2021.

Khan, Haiqa. "Navigating Pakistan's Digital Revolution: Cybercrimes, Reporting, and Safeguarding." *The Friday Times*, August 19, 2023. <https://thefridaytimes.com/19-Aug-2023/navigating-pakistan-s-digital-revolution-cybercrimes-reporting-and-safeguarding>.

Khan, Muhammad Imad Ayub. "Cyber-Warfare: Implications for the National Security of Pakistan." *NDU Journal* 33 (2019): 117–32.

Khan, Muhammed Fahim, and Aamer Raza. "Cybersecurity and Challenges Faced by Pakistan." *Pak. Journal of International Affairs* 4, no. 1 (2021).

Khan, Umair Pervez, and Muhammed Waqar Khan. "Cybersecurity in Pakistan: Regulations, Gaps and a Way Forward." *Cyberpolitik Journal* 5, no. 10 (2020).

Kim, Yu-Kyung, Myong-Hyun Go, Sonyong Kim, Jaeyeon Lee, and Kyungho Lee. "Evaluating Cybersecurity Capacity Building of ASEAN Plus Three through Social Network Analysis." *Journal of Internet Technology* 24, no. 2 (2023): 495-505.

Knake, Robert K, and Richard A Clark. *Cyber War : The next Threat to National Security and What to Do about It*. Abu Dhabi, Uae: The Ecscr, 2012.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz. *Cyberpower and National Security*. University of Nebraska Press: Potomac Books, 2009.

Kumar, Ranjit. *Research Methodology: A Step-By-Step Guide for Beginners*. 5th ed. London: Sage, 2019.

Lelonek, Jaimie. "Analyzing Russia's Conventional and Cyber Operations in Ukraine." PhD diss., Utica University, 2022.

Lewis, James A., Erica D. Lonergan, Julia Voo, Melanie Garson, and Amy Ertan. *Evolving Cyber Operations and Capabilities*. Center for Strategic and International Studies, 2023.

Lin, Herbert. "Russian Cyber Operations in the Invasion of Ukraine." *The Cyber Defense Review* 7, no. 4 (2022): 31-46.

Lostri, Eugenia, James Andrew Lewis, and Georgia Wood. "A Shared Responsibility: Public-Private Cooperation for Cybersecurity." CSIS, March 2, 2022.

Matania, Eviatar, Lior Yoffe, and Tal Goldstein. "Structuring the National Cyber Defence: In Evolution Towards a Central Cyber Authority." *Journal of Cyber Policy* 2, no. 1 (2017): 16-25.

Mifsud, Francesco. "Internal and External Challenges to an Effective Organisation-Wide Cyber Security Set of Policies." Cybergate - Your Cyber Security Partner, October 10, 2022. <https://cybergateinternational.com/blog/internal-and-external-challenges-to-an-effective-organisation-wide-cyber-security-set-of-policies/>.

Ministry of IT & Telecom. *National Cyber Security Policy 2021*. Government of Pakistan, 2021.

<https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf>.

Mohamed, Nachaat. "Current Trends in AI and ML for Cybersecurity: A State-of-The-Art Survey." *Cogent Engineering* 10, no. 2 (October 25, 2023).

Mpshane-Nkosi, Mmakoena. "4IR and the Emergence of Digital Foreign Policy: A Global Comparative Study." PhD diss., University of Johannesburg, 2023.

National Cybersecurity Organisation: Republic of Korea, Sungbaek Cho, NATO CCDCOE Strategy Researcher. <https://ccdcoe.org/uploads/2022/12/ROK-Country-report.pdf>.

National Research Council (U.S, and National Research Council (U.S.). Computer Science And Telecommunications Board. *At the Nexus of Cybersecurity and Public Policy : Some Basic Concepts and Issues*. Washington, Dc: National Academies Press, 2014.

NCSC. "Vulnerability Assessment." 2020. <https://www.ncsc.gov.uk/>.

NIST. *Framework for Improving Critical Infrastructure Cybersecurity*. 2018. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

NIST. "Cybersecurity Framework." National Institute of Standards and Technology, 2023. <https://www.nist.gov/cyberframework>.

Nurse, Jason RC, Maria Bada, Betsy Uchendu, and Steven Furnell. "Developing a Cyber Security Culture: Current Practices and Future Needs." *Computers & Security* 109 (2021): 102387.

Pakistan Telecommunication Authority. "Cybersecurity Strategy for Telecom Sector 2023-2028." PTA, 2023.

https://pta.gov.pk/assets/media/cyber_security_strategy_telecom_sector_2023_2028_11-12-2023.pdf.

Pakistan Telecommunication Authority. "Telecom Indicators | PTA." Pta.gov.pk, 2023.
<https://www.pta.gov.pk/en/telecom-indicators>.

Peltier, Thomas R. *Information Security Policies, Procedures, and Standards : Guidelines for Effective Information Security Management*. Boca Raton, Fla.: Auerbach, 2002.

Polkinghorne, Donald. *Methodology for the Human Sciences: Systems of Inquiry*. Albany: State University Of New York Press, 1983.

Pomerleau, P. L., and D. L. Lowery. "The Evolution of Cybersecurity within the American Financial Sector." In *Countering Cyber Threats to Financial Institutions: A Private and Public Partnership Approach to Critical Infrastructure Protection*, 29-45. 2020.
https://link.springer.com/chapter/10.1007/978-3-030-54054-8_3.

Prins, Corien, Erik Schrijvers, and Reijer Passchier. *Preparing for Digital Disruption*. Springer Nature, 2021.

Radanliev, Petar. "Cyber Diplomacy: Defining the Opportunities for Cybersecurity and Risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing." *Journal of Cyber Security Technology* (2024): 1-51.

Rafiq, Aamna. "Challenges of Securitising Cyberspace in Pakistan." *Strategic Studies* 39, no. 1 (April 24, 2019): 90–101. <https://doi.org/10.53532/ss.039.01.00126>.

Rasool, Sadia. "Cyber Security Threat in Pakistan: Causes Challenges and Way Forward." *International Scientific Online Journal*, no. 12 (July 2015).

Raza, Syed Irfan. "Leaks Reveal Massive Breach in Security at PM Office." *Dawn*, September 26, 2022. <https://www.dawn.com/news/1712044>.

Riggs, Hugo, Shahid Tufail, Imtiaz Parvez, Mohd Tariq, Mohammed Aquib Khan, Asham Amir, Kedari Vineetha Vuda, and Arif I. Sarwat. "Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure." *Sensors* 23, no. 8 (January 1, 2023): 4060. <https://www.mdpi.com/1424-8220/23/8/4060>.

Romaniuk, Scott N., and Michael Claus. "Germany's Cybersecurity Strategy: Confronting Future Challenges." In *Routledge Companion to Global Cyber-Security Strategy*, 73-88. London: Routledge, 2021.

Roscini, Marco. *Cyber Operations and the Use of Force in International Law*. Oxford University Press, 2014.

Safitra, Muhammad Fakhrul , Muharman Lubis, and Hanif Fakhurroja.

"Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity." *Sustainability* 2023 15, no. 18 (September 6, 2023).

Salma, Dita Aulia, and Fahlesa Munabari. "Blockchain Technology: Cyber Security Strategy in Post-2007 Cyber-Attacks Estonia." *Deviance Jurnal Kriminologi* 7, no. 1 (2023): 32-45.

Schmitt, Michael N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, United Kingdom ; New York, Ny, Usa: Cambridge University Press, 2017.

Senor, Dan, and Saul Singer. *Start-up Nation: The Story of Israel's Economic Miracle*. Toronto: McClelland & Stewart, 2011.

Setiawati, D., H. A. Hakim, and F. A. H. Yoga. "Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore." *Indonesian Comparative Law Review* 2, no. 2 (2020): 95-109.

Shackelford, Scott J., Anne Boustead, and Christos Makridis. "Defining 'Reasonable' Cybersecurity: Lessons from the States." *Yale JL & Tech.* 25 (2023): 86.

Shad, Muhammad Riaz. "Cyber Threat Landscape and Readiness Challenge of Pakistan." *Strategic Studies* 39, no. 1 (April 24, 2019): 1–19.

Shively, Jacob. "Cybersecurity Policy and the Trump Administration." *Policy Studies* 42 (June 28, 2021): 1–17.

Singapore Government. "Smart Nation: A Digital Government." 2018. <https://www.smartnation.gov.sg>.

Singh, Bhupinder. "Unleashing Alternative Dispute Resolution (ADR) in Resolving Complex Legal-Technical Issues Arising in Cyberspace Lending E-Commerce and Intellectual Property: Proliferation of E-Commerce Digital Economy." *Revista Brasileira de Alternative Dispute Resolution-Brazilian Journal of Alternative Dispute Resolution-RBADR* 5, no. 10 (2023): 81-105.

St. John, Mariah, and Brenna Swanston. "Cybersecurity Stats: Facts and Figures You Should Know – Forbes Advisor." www.forbes.com, February 24, 2024. <https://www.forbes.com/advisor/education/it-and-tech/cybersecurity->

statistics/#:~:text=Cybersecurity%20Fast%20Facts&text=As%20the%20globe%20becomes%20more.

Staszczyk, Artur. “European Parliament Position on EU Cyber Security and Defense Policy.” *Reality of Politics* 1, no. 10 (March 31, 2019): 122–33.

Tabansky, Lior, and Isaac Ben Israel. “The National Cyber-Strategy of Israel and the INCB.” In *Cybersecurity in Israel*, 49-54. 2015.
https://link.springer.com/chapter/10.1007/978-3-319-18986-4_7.

The Newspaper's Staff Reporter. “Cyberattack Disrupts National Bank of Pakistan Services; Recovery by Monday Likely.” *Dawn*. October 31, 2021.
<https://www.dawn.com/news/1655059>.

Tolga, I. Burak, and Gunnar Faith-Ell. “Information Sharing Framework for Penetration Testing.” NATO Cooperative Cyber Defence Centre of Excellence, 2020.
https://www.ccdcoe.org/uploads/2020/04/Paper_version_Final3.pdf.

Trautman, Lawrence J. “Cybersecurity: What about U.S. Policy?” *Journal of Law, Technology and Policy* 1 (2015).

United Nations. “Cybersecurity: A Global Issue Demanding a Global Approach.” Un.org, December 12, 2011.

<https://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html>.

Verizon. “DBIR Report 2023.” Verizon Business, 2023.

<https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/>.

Voigt, Peter, and Axel von dem Bussche. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. 1st ed. Cham: Springer International Publishing, 2017.

<https://doi.org/10.1007/978-3-319-57959-7>.

Vu, Cung, and S. Rajaratnam. *Cyber Security in Singapore*. Singapore: S. Rajaratnam School of International Studies, 2022.

Wamala, F. "ITU National Cybersecurity Strategy Guide," 2011.

<http://www.itu.int/ITUUD/%20cyb/cybersecurity/docs/itu-nationalcybersecurity-%20guide.pdf>.

Warriach, Saqib Khan, Imran Alam, M. Mumtaz Ali Khan, Abeera Haider, and Samee Ozair Khan. "Cyber Terrorism: Pakistan's Security Perspective." *JRSP* 97, no. 3 (June 2020).

White, Gregory B., and Natalie Sjin. "The NIST Cybersecurity Framework." In *Research Anthology on Business Aspects of Cybersecurity*, 39-55. Hershey, PA: IGI Global, 2022.

Willett, Marcus. "Lessons of the SolarWinds Hack." In *Survival April–May 2021: Facing Russia*, 7-25. Routledge, 2023.

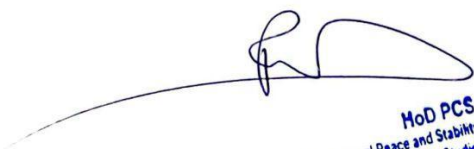
World Economic Forum, and Accenture. "Global Cybersecurity Outlook 2024 ." World Economic Forum, January 2024.

Wylde, Vinden, Nisha Rawindaran, John Lawrence, Rushil Balasubramanian, Edmond Prakash, Ambikesh Jayal, Imtiaz Khan, Chaminda Hewage, and Jon Platts. "Cybersecurity, Data Privacy and Blockchain: A Review." *SN Computer Science* 3, no. 2 (2022): 127.

<https://link.springer.com/article/10.1007/s42979-022-01020-4>.

Yamin, Tughral. "Cyberspace Management in Pakistan." *Governance and Management Review* 3, no. 1 (2018): 46–61.

Zhang, Yin, Haider Abbas, and Yi Sun. "Smart E-Commerce Integration with Recommender Systems." *Electronic Markets*, May 17, 2019.



MoD PCS
Centre for International Peace and Stability
NUS Institute of Peace and Conflict Studies
Islamabad

Zahra Michelle Khan - Challenges to Cyber Security Policy in Pakistan, A Critical Discourse - Supervis.docx

by Sheraz Khaliq

Submission date: 15-Aug-2024 03:18AM (UTC-0700)

Submission ID: 2432381889

File name: Zahra_Michelle_Khan_-_Challenges_to_Cyber_Security_Policy_in_Pakistan_A_Critical_Discourse_-_Supervis.docx (273.1K)

Word count: 20133

Character count: 121254



Zahra Michelle Khan - Challenges To Cybersecurity Policy in Pak A Critical Discourse.docx

ORIGINALITY REPORT

18%	14%	12%	9%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

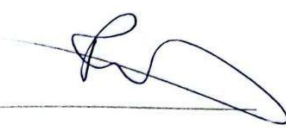
1	pure.southwales.ac.uk Internet Source	1%
2	www.itu.int Internet Source	1%
3	Submitted to Higher Education Commission Pakistan Student Paper	1%
4	ouci.dntb.gov.ua Internet Source	<1%
5	issi.org.pk Internet Source	<1%
6	dokumen.pub Internet Source	<1%
7	Submitted to University of New South Wales Student Paper	<1%
8	Submitted to American Public University System Student Paper	<1%



9	www.grafiati.com Internet Source	<1 %
10	Submitted to Webster University Student Paper	<1 %
11	www.mdpi.com Internet Source	<1 %
12	web.archive.org Internet Source	<1 %
13	Submitted to Manipal University Student Paper	<1 %
14	ndujournal.ndu.edu.pk Internet Source	<1 %
15	aurora.dawn.com Internet Source	<1 %
16	norr.numl.edu.pk Internet Source	<1 %
17	Submitted to University of Bradford Student Paper	<1 %
18	fastercapital.com Internet Source	<1 %
19	repository.iuk.ac.ke:8080 Internet Source	<1 %
20	www.coursehero.com Internet Source	<1 %



210	Le, Ngoc Thuy. "A Novel Capability Maturity Model with Quantitative Metrics for Securing Cloud Computing", University of Technology Sydney (Australia), 2024 Publication	<1 %
211	Paul Voigt, Axel von dem Bussche. "The EU General Data Protection Regulation (GDPR)", Springer Science and Business Media LLC, 2017 Publication	<1 %
212	Submitted to RMIT University Student Paper	<1 %
213	Rommel Banlaoi. "Philippine Security in the Age of Terror - National, Regional, and Global Challenges in the Post-9/11 World", Auerbach Publications, 2019 Publication	<1 %
214	Scott N. Romaniuk, Mary Manjikian. "Routledge Companion to Global Cyber-Security Strategy", Routledge, 2021 Publication	<1 %
215	acikbilim.yok.gov.tr Internet Source	<1 %
216	journalppw.com Internet Source	<1 %
217	www.efsas.org Internet Source	<1 %



218	press.armywarcollege.edu Internet Source	<1 %
219	Submitted to BPP College of Professional Studies Limited Student Paper	<1 %
220	Mattia Caldarulo, Eric W. Welch, Mary K. Feeney. "Determinants of cyber-incident among small and medium US cities", Government Information Quarterly, 2022 Publication	<1 %
221	journals.sagepub.com Internet Source	<1 %
222	lawreview.uchicago.edu Internet Source	<1 %

Exclude quotes On
Exclude bibliography On

Exclude matches Off