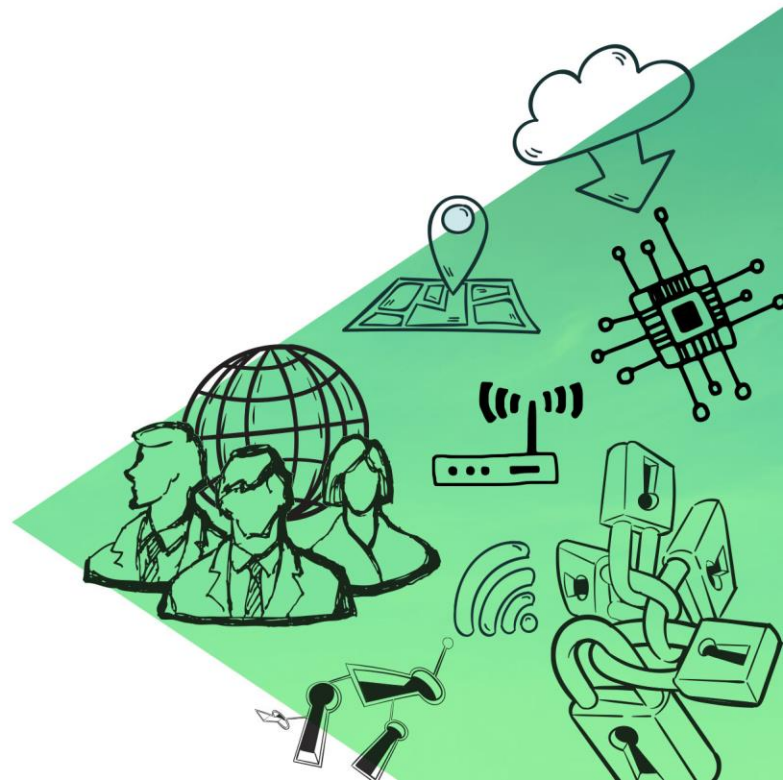


Cyber Security Risk Governance: *Threat Vectors and Solutions* for Pakistan

Ajwa Hijazi

Research Assistant

Working Paper



© Centre for Aerospace & Security Studies

2024

All rights reserved. No part of this Publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior permission of the Editor/Publisher.

Opinions expressed are those of the author/s and do not necessarily reflect the views of the Centre. Complete responsibility for factual accuracy of the data presented and bibliographic citations lie entirely with the author/s. CASS has a strict zero tolerance plagiarism policy.

President

Air Marshal Javaid Ahmed (Retd)

Editor

Sarah Siddiq Aneel

Layout

Hira Mumtaz

All correspondence pertaining to this publication should be addressed to CASS, Islamabad, through post or email at the following address:

Centre for Aerospace & Security Studies

☎ +92 051 5405011

✉ cass.thinkers@casstt.com

f [cass.thinkers](https://www.facebook.com/cass.thinkers)

@ [cassthinkers](https://www.instagram.com/cassthinkers)

✕ [@CassThinkers](https://twitter.com/CassThinkers)

in [Centre for Aerospace & Security Studies](https://www.linkedin.com/company/centre-for-aerospace-and-security-studies)



CENTRE for AEROSPACE & SECURITY STUDIES

**Cyber Security Risk Governance:
*Threat Vectors and Solutions for Pakistan***

Working Paper

Ajwa Hijazi

Research Assistant

TABLE OF CONTENTS

Abstract	1
Introduction	2
Cyber Security Threats Impacting Pakistan	3
Rapid Increase in Data Theft	5
Phishing	6
Ransomware	7
Distributed Denial-of-Service (DDoS) Attack	8
Cyber Threats to Critical Infrastructure	9
Pakistan’s Cyber Security Architecture	10
Initial Organisational Developments	11
Pakistan Electronic Crimes Prevention Act (PECA), 2016	11
National Centre for Cyber Security	13
National Cyber Security Policy (NCSP), 2021	14
Cyber Security Strategy for the Telecom Sector	16
Computer Emergency Response Teams (CERTs) Rules, 2023	17
National Cyber Crimes Investigation Agency (NCCIA), 2024	17
Cyber Security Risk Governance: Looking Ahead	18
Reduce Fragmentation and Bureaucratic Overlap in Cyber Security Governance	19
Apply Structured Cyber Risk Governance Protocols	19
Increase Digital Literacy and Cyber Security Awareness	20
Expand Infrastructure, Connectivity and Access	20
Regulate Inclusive Policy on Data Protection	21
Adopt Advanced Cyber Security Technologies	22
Move towards Indigenisation and Data Localisation	23
Information Sharing and Global Collaboration	23
Conclusion	24

Abstract

Swift progress in technology has accelerated digitalisation globally, with Pakistan following suit. However, with these advancements come escalating cyber risks. This Working Paper critically examines Pakistan's cyber security landscape, focusing on prevalent threat vectors such as phishing, hacking, ransomware, and Distributed Denial of Service (DDoS) attacks. Through an analysis of the country's existing cyber security framework, the study identifies key strengths and areas of vulnerability. By leveraging secondary data, the research underscores the urgent need for improved Cyber Security Risk Governance and addresses the obstacles hindering effective cyber security practices. The paper concludes that to strengthen its cyber security posture, Pakistan must address both structural and contextual challenges to ensure that reforms are impactful and sustainable.

Keywords: Cyber Security, Cyber Governance, Cyber Threats, Information Communication Technology (ICT), Pakistan.

1. Introduction

Advent of Information and Communication Technologies (ICT) has transformed the global landscape, bringing significant advancements to various facets of human life, including personal interactions, business operations, organisational functioning, and social infrastructure such as finance, electricity, water, and health. However, alongside these opportunities, ICT has also introduced new security threats. Increasing reliance on ICT in a country's infrastructure creates vulnerabilities that can be exploited by individuals, organisations, nation-states, or non-state actors, leading to cyber threats.

The United States' National Institute of Standards and Technology (NIST) defines a cyber threat as *'any circumstance or event with the potential to adversely impact organizational operations, assets, or individuals through an information system, via unauthorized destruction, disclosure, modification of information, or denial of services.'*¹

The increasing sophistication and disruptive potential of cyber threats² highlight the critical need to protect computer systems, networks, mobile devices, and servers. Cyber security focuses on defending information systems from these digital attacks, while cyber security governance encompasses the strategies designed to prevent such disruptions.

While Pakistan's upward movement in the ITU 2024 'Global Cybersecurity Index'³ is a positive development, there remains a significant journey ahead in fully securing the nation's digital landscape. Pakistan's rise from 79th place in 2021 to being among the 46 leading countries highlights progress, particularly in areas such as legal frameworks, capacity-building, and incident response capabilities. However, this improved ranking should not overshadow the ongoing challenges the country faces and critical gaps in preparedness, resilience and governance.

As global reliance on ICT grows, the potential for cyber disruptions increases. Pakistan's multifaceted cyber security challenges, reflected in rising cyberattacks

¹ National Institute of Standards and Technology, "Cyber Threat," Accessed November 20,2023, https://csrc.nist.gov/glossary/term/cyber_threat.

² United Nations, *Cybersecurity in the United Nations System Organizations*, report (Geneva: UN, 2021), https://www.unjuu.org/sites/www.unjuu.org/files/jiu_rep_2021_3_english.pdf.

³ International Telecommunication Union, *Global Cybersecurity Index 2024*, 5th Edition (Geneva: ITU, 2024), https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf.

escalating by a staggering 300% compared to the same period in 2023,⁴ include malicious actors attempting to exploit networks, as well as the need to secure citizens' data and information systems. Compounding these issues is the widespread lack of awareness among Pakistani internet users, who often possess limited knowledge of information technology, leaving them vulnerable to a wide array of cyber threats. This knowledge gap, combined with the country's shortage of technological expertise and resources, hampers effective regulation and the development of robust cyber security measures,⁵ underscoring the pressing need for enhanced governance in this domain. The country must focus on further strengthening its cyber security infrastructure to mitigate risks and ensure long-term sustainability.

This *Working Paper* seeks to analyse Pakistan's domestic cyber security threat landscape, assess the current cyber security architecture, and highlight the necessity of strengthening cyber security risk governance. The study utilises secondary data sources, including journal papers, opinion articles, reports, and scholarly research, to draw its conclusions.

2. Cyber Security Threats Impacting Pakistan

In this era of rapid digital advancement, cyberspace has emerged as the hub of human interactions. The world's dependence on ICT is increasing each day. As of October 2023, there are around 5.3 billion internet users worldwide, comprising 65.7 percent of the global population.⁶ In the case of Pakistan, internet penetration is 36.7 percent of the population,⁷ and as of January 2023, Pakistan had a digital population of approximately 87.35 million people, positioning it among the top 20 countries with the

⁴ Express Tribune, "Spyware Attacks Increased by 300% in Pakistan. Backdoor Attacks Witness Moderate Increase in 2024," May 10, 2024, <https://tribune.com.pk/story/2466023/spyware-attacks-increased-by-300-in-pakistan>.

⁵ Umair Pervez Khan and Muhammad Waqar Khan, "Cybersecurity in Pakistan: Regulations, Gaps and Way Forward," *Cyberpolitik Journal* 5, no.10 (2020): 205-218.

⁶ Statista, "Number of Internet and Social Media Users Worldwide as of October 2023," Accessed November 23, 2023, <https://www.statista.com/statistics/617136/digital-population-worldwide/>.

⁷ DataReportal, "Digital 2023: Pakistan," Accessed November 23, 2023, [https://datareportal.com/reports/digital-2023pakistan#:~:text=There%20were%2087.35%20million%20internet,percent%20of%20the%20total%20population](https://datareportal.com/reports/digital-2023pakistan#:~:text=There%20were%2087.35%20million%20internet,percent%20of%20the%20total%20population.).

largest online presence globally.⁸ This significant digital base presents both opportunities for growth in the digital economy and challenges in terms of ensuring robust cyber security measures to protect its expanding online community.

Pakistan's cyber threat landscape is shaped by three critical dimensions: inherent risks stemming from inadequate cyber security preparedness; compounding effects of domestic and regional sociopolitical tensions;⁹ and fragmentation and bureaucratic overlap in cyber security governance.

The country's vulnerabilities in its digital governance infrastructure especially leave it exposed to a wide range of cyber threats. These risks are further exacerbated by sociopolitical hostilities, both within Pakistan and in its surrounding region, which heighten the likelihood of politically motivated cyberattacks and other forms of digital aggression.

In its 2015 report, Symantec highlighted that millions of new malware had been identified in Pakistani cyberspace.¹⁰ The report also identified Pakistan's susceptibility to espionage and data theft. In 2021, it was reported by the Federal Investigation Agency (FIA) that over three years, there had been a 38 percent increase in cybercrimes;¹¹ and a Pakistan Telecommunications (PTA) report indicated that 10,000 cyberattacks occurred in 2022. The subjects of these attacks were the banking sector, telecom industry, educational sector, and critical infrastructure, with the military and government sectors being the main targets of the attackers.¹² In the first quarter of 2024, spyware attacks in Pakistan surged by an alarming 300% compared to the same period in 2023, indicating a sharp rise in espionage and data infiltration threats. Findings from the Kaspersky Managed Detection and Response (MDR) team revealed that high-severity incidents, particularly those requiring direct human intervention,

⁸ Statista, "Countries with the Largest Digital Populations in the World as of January 2023 (in millions)," Accessed November 23, 2023, <https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/>.

⁹ Muhammad Riaz Shad, "Cyber Threat Landscape and Readiness Challenge of Pakistan," *Journal of Strategic Studies* 39, no.1 (2019): 1-19.

¹⁰ Irta Fatima, "Pakistan's Cyber Threat Landscape and Prospects of Regional Cooperation on Cyber Security," *Spotlight on Regional Affairs* 40, no.11 (2022): 1-4.

¹¹ Muhammad Nadeem Mirza and Muhammad Shahzad Akram, "3-Cs of Cyberspace and Pakistan: Cyber Crime, Cyber Terrorism and Cyber Warfare," *Journal of Strategic Studies* 42, no.1 (2022): 62-80.

¹² Jawed Aziz Masudi and Nasir Mustafa, "Cyber Security and Data Privacy Law in Pakistan: Protecting Information and Privacy in the Digital Age," *Pakistan Journal of International Affairs* 6, no.3 (2023): 356-366.

occurred more than twice daily in 2023. This escalation highlights the growing scale and intensity of cyber threats facing Pakistan.¹³ Following are some of the key threat vectors impacting the country's cyber landscape:

2.1. Rapid Increase in Data Theft

Data theft, involving the illegal transfer of personal, financial, and technical information, has become increasingly prevalent in Pakistan, particularly with the rapid expansion of digital banking. Key government entities and the telecom sector have also been significantly impacted. In 2018, the Director of FIA's cybercrime wing revealed that data from almost all Pakistani banks had been compromised due to a major security breach,¹⁴ exposing the card details of nearly 19,000 individuals from 22 banks on the dark web.¹⁵

Over the past few years, Pakistan has faced numerous cyberattacks, primarily in the form of phishing and hacking of critical government sites, with the primary objective of data theft. In 2018, reports from TechJuice and local news agencies indicated that citizens' personal information, including data from the Punjab Information Technology Board (PITB), had been breached. Allegedly, this included sensitive details such as Computerised National Identity Card information and mobile phone user databases. While the PITB denied these claims, TechJuice reported that the stolen data was being sold on platforms like Facebook and WhatsApp.¹⁶

In 2021, the FIA informed the National Assembly's Standing Committee on Information Technology that biometric data from the National Database and Registration Authority (NADRA) had been compromised. A year later, the federal IT Minister disclosed that around 200,000 hacking incidents occurred daily across Pakistan.¹⁷

In a more recent 2023 incident, hackers gained access to the database of a private company used by various restaurants, compromising the data of approximately 2.2

¹³ Express Tribune, "Spyware Attacks Increased by 300% in Pakistan."

¹⁴ Shakeel Qarar, "Almost All Pakistani Banks Hacked in Security Breach, says FIA Cybercrime Head," *Dawn*, November 6, 2018, <https://www.dawn.com/news/1443970>.

¹⁵ Ayaz Hussain Abbasi, "The Growing Threat of Cyber Fraud," *T-Magazine*, May 8, 2022, <https://tribune.com.pk/story/2355657/the-growing-threat-of-cyber-fraud>.

¹⁶ Shad, "Cyber Threat Landscape and Readiness Challenge of Pakistan."

¹⁷ Faran Mahmood, "The Long Road to Becoming Cyber Power," *Express Tribune*, July 10, 2023, <https://tribune.com.pk/story/2425486/the-long-road-to-becoming-cyber-power>.

million Pakistanis. The stolen information, including customers' contact numbers and credit card details, was subsequently put up for sale online.¹⁸

2.2. Phishing

Phishing is a highly effective type of cybercrime that allows criminals to trick users into giving away sensitive information. Since its first documented occurrence in the 1990s, phishing has evolved into a more advanced and complex attack method. Today, it is one of the most common forms of online fraud. Victims of phishing attacks can suffer significant consequences, such as the theft of personal information, identity fraud, and the compromise of confidential business or government data.¹⁹

In Pakistan, there are increasing incidents of phishing emails and text-based messages pretending to be from legitimate governmental organisations.²⁰ In response to rising cyber threats, several government entities have issued advisories to warn the public. The Federal Board of Revenue (FBR) has cautioned taxpayers to be vigilant against fraudulent emails requesting sensitive information such as Taxpayer PINs and bank account details.²¹ Similarly, the National Telecommunication and Information Security Board (NTISB) released a notice addressing the increase in financial fraud and banking scams involving phishing techniques. The board highlighted that scammers use various attack methods, including anonymity, social engineering (e.g., compromised phone numbers or WhatsApp accounts), and malicious applications, to exploit individuals' account details.²²

¹⁸ "Hacked Data of Over 2m Pakistanis Up for Sale," *Pakistan Today*, September 21, 2023, <https://www.pakistantoday.com.pk/2023/09/21/hacked-data-of-over-2m-pakistanis-up-for-sale/>.

¹⁹ Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf and Imtiaz Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," Review Article, *Frontiers of Computer Science* 3 (2021), <https://doi.org/10.3389/fcomp.2021.563060>.

²⁰ Karandaaz and Bill and Melinda Gates Foundation, *SMS Fraud Detection and Prevention in Pakistan*, report (Lahore: Karandaaz, 2019), <https://karandaazmain.wpenginepowered.com/wp-content/uploads/2019/05/SMS-Fraud-Detection-and-Prevention-in-Pakistan-1.pdf>; HackRead, "Chinese 'Smishing Triad' Group Targets Pakistanis with SMS Phishing," June 13, 2024, <https://hackread.com/chinese-smishing-triad-group-pakistan-sms-phishing/>; Sindhu Abbasi, "Pakistan's Web of Cyber Scammers," *Dawn*, July 16, 2023, <https://www.dawn.com/news/1764628>.

²¹ Federal Board of Revenue, "Beware of Fraudulent Emails - Phishing Scams," Accessed December 2, 2023, <https://www.fbr.gov.pk/beware-fraudulent-emails/21095>.

²² Tahir Amin, "NTISB Issues Advisory Amid Surging Financial, Banking Scams," *Business Recorder*, September 4, 2023, <https://www.brecorder.com/news/40261358>.

2.3. Ransomware

Ransomware is a type of cyberattack where hackers restrict or block users' access to their data, demanding a ransom in exchange for restoring access. In today's digital age, data has become one of the most valuable assets, making it a prime target for cybercriminals. High-profile attacks on large corporations underscore the challenges of safeguarding sensitive information. Ransomware incidents, such as those targeting companies like Sony and the MGM Resort hotel and casino chain, highlight the growing sophistication of these attacks.

Recent global data indicates that ransomware incidents have surged dramatically. According to Microsoft, human-operated ransomware attacks increased by over 200% between September 2022 and June 2023, with attackers increasingly targeting critical industries like education, healthcare, and manufacturing.²³ The financial impact of these attacks is staggering, with global ransomware costs projected to reach USD 265 billion annually by 2031, up from USD 20 billion in 2021.²⁴

Pakistan's digital audience is equally and increasingly vulnerable to ransomware threats, particularly in the realm of the digital economy. Consumers who shop online and input their personal information into inadequately secured e-commerce platforms are at significant risk of data breaches.²⁵ In 2020, K-Electric, the country's largest energy provider, fell victim to a major ransomware attack. The Netwalker ransomware group targeted the company, demanding a ransom of USD 3.85 million and giving K-Electric a seven-day deadline to comply.²⁶ More recently in 2023, the Election Commission of Pakistan (ECP) fell victim to a ransomware attack in which an unidentified hacker attempted to access data stored on its employees' computers. In response, the ECP issued an advisory, urging its employees to exercise caution when handling digital information to prevent further breaches. This incident highlights the

²³ Jonathan Greig, "Microsoft: Human-Operated Ransomware Attacks Tripled Over Past Year," *Record*, October 6, 2023, <https://therecord.media/human-operated-ransomware-attacks-report-microsoft>; Jacob Fox, "Top Cybersecurity Statistics for 2024," *Cobalt*, December 8, 2023, <https://www.cobalt.io/blog/cybersecurity-statistics-2024>.

²⁴ Fox, "Top Cybersecurity Statistics for 2024."

²⁵ Rafia Zakaria, "Growing Ransomware Attacks," *Dawn*, September 27, 2023, <https://www.dawn.com/news/1778117>.

²⁶ Daryna Anotniuk, "Hackers Target Pakistani Government, Bank and Telecom Provider with China-Made Malware," *Record*, July 14, 2023, <https://therecord.media/hackers-target-pakistani-government-with-malware>.

growing vulnerability of governmental institutions to cyberattacks and the pressing need for stronger cyber security protocols to safeguard sensitive data.²⁷

2.4. Distributed Denial-of-Service (DDoS) Attack

A Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt the normal operations of a target network or server by overwhelming it with excessive internet traffic, rendering the service or infrastructure temporarily unavailable. In 2023, the Government of Pakistan (GoP) revealed in an advisory that the Russian hacker group 'Kill Net' had launched attacks against Pakistan's military and civilian infrastructures, using multiple attack vectors, including DDoS. 'Kill Net' is notorious for deploying DDoS as a mass service disruptor, targeting not only Pakistan but also entities such as NATO, Ukraine, and the United States.²⁸ This highlights the group's broader strategy of using DDoS to cripple critical infrastructure, underscoring the need for stronger network defence mechanisms in Pakistan and globally, as these attacks can cause widespread disruption and financial losses across affected sectors.

Indian hackers have consistently posed a significant threat to Pakistan's cyberspace, particularly targeting government and military websites through cyberattacks, including DDoS attacks. Since 1998, these attacks have periodically intensified, most notably after the establishment of the Indian Cyber Army (ICA) in 2010. The ICA's formation marked a turning point, leading to more organised and visible cyber intrusions against Pakistan. This escalation not only underscores the persistent cyber warfare between the two nations but also highlights the vulnerabilities in Pakistan's cyber security infrastructure.²⁹ In retaliation, Pakistani hackers mount counterattacks. A notable example occurred more than a decade ago when, in response to India hacking approximately 40 Pakistani websites, Pakistani hackers retaliated by breaching around 270 Indian websites, including high-profile targets like the Central Bureau of Intelligence (CBI).³⁰

²⁷ Iftikhar A. Khan, "ECP Issues Advisory after Suspected Ransomware Attack," *Dawn*, July 8, 2023, <https://www.dawn.com/news/1763614>.

²⁸ Shahzad Paracha, "Russian Hacker Involved in Targeting Pakistan's Military and Civil Setups," *Pakistan Today*, July 5, 2023, <https://www.pakistantoday.com.pk/2023/07/05/russian-hacker-involved-in-targeting-pakistans-military-and-civil-setups/>.

²⁹ Muhammad Riaz Shad, "Cyber Threat Landscape and Readiness Challenge of Pakistan," *Journal of Strategic Studies* 39, no.1 (2019): 1-19.

³⁰ Ibid.

This back-and-forth demonstrates the deeply rooted cyber tensions between the two countries, where attacks are not limited to military or governmental targets but extend to critical infrastructure, public databases, and sensitive information repositories

In April 2023, Pakistan International Airlines (PIA) suffered a DDoS attack orchestrated by the hacking group United Cyber Caliphate (UCC). During the incident, the airline's website displayed 'Error Code 1020',³¹ indicating that specific users had been intentionally blocked from accessing the site.³² Similarly, in October 2023, the Federal Cabinet issued an advisory warning users about vulnerabilities in certain versions of Google Chrome, which could expose users to cyberattacks. The advisory highlighted that if these vulnerabilities were exploited, they could also lead to DDoS attacks,³³ underlining the need for users to update their browsers to more secure versions.

Ransomware attacks indicate the increasing sophistication of cyber threats and the necessity for domestic organisations and individuals alike to remain vigilant and proactive in their cyber security practices.

2.5. Cyber Threats to Critical Infrastructure

In Pakistan, the growing digitalisation of essential systems such as national power grids, stock exchanges, and command and control systems has heightened their exposure to potential cyberattacks. The disruption of these infrastructures can have severe consequences, as it directly affects the provision of essential services. For instance, a cyberattack on the national power grid could lead to widespread physical outages, interrupting the country's energy supply and impacting daily operations.³⁴ This underscores the urgent need for robust cyber security measures to protect such critical systems from digital threats.

In January 2023, Pakistan experienced a nationwide power outage that plunged parts of the country into darkness, halting its energy supply. Although the 1,112 grid

³¹ Ashish Kaithan, "Pakistan Cyber Attack, Team UCC Claims to Take Down Pakistan International Airlines," *Cyber Express*, April 4, 2023, <https://thecyberexpress.com/pakistan-cyber-attack-international-airlines/>.

³² Nimbus, "How to Fix Error 1020 on a Website," Accessed January 15, 2023, <https://nimbushosting.co.uk/blog/how-to-fix-error-1020-on-a-website#>.

³³ Wajid Ali, "High-Risk Alert Issued for Google Chrome Users by Pakistan Government," *Samaa Tv*, October 17, 2023, <https://www.samaa.tv/208732840-high-risk-alert-issued-for-google-chrome-users-by-pakistan-government>.

³⁴ Hammaad Salik, Rao Ibrahim Zahid and Babar Khan Akhunzada, "Cyber Threats to Pakistan's National Power Grid," *Geopolitics*, February 13, 2023, <https://thegeopolitics.com/cyber-threats-to-pakistans-national-power-grid/>.

stations were restored within 24 hours, the blackout brought the country's operations to a standstill, affecting major cities like Islamabad and Karachi. The power failure disrupted critical functions across sectors, from government operations to business activities. At the time, the Energy Minister acknowledged the possibility of a 'remote chance' that the incident may have been caused by a cyberattack,³⁵ highlighting concerns over the vulnerability of Pakistan's national grid to digital threats.³⁶

3. Pakistan's Cyber Security Architecture

With the rapid expansion of Pakistan's IT sector and its increasing penetration across the economy, the government has made notable strides toward developing a cyber security regulatory architecture. In 2021, the Federal Cabinet approved the 'National Cyber Security Policy', marking a significant step in formalising a national strategy for securing digital infrastructure.³⁷

Building on this policy, the government has introduced several enforcement mechanisms. In 2024, the National Cyber Crimes Investigation Agency (NCCIA) was notified.³⁸ Prior to the NCCIA, the Federal Investigation Agency's (FIA) Cybercrime Wing had been the primary body responsible for addressing cyber threats. It launched Cyber Patrolling Units (CPUs) to monitor social media activity, including the trends and discussions emerging on various platforms.³⁹ In addition to these enforcement efforts, the Prevention of Electronic Crimes Act (PECA) of 2016 provides a legal framework to prosecute a wide range of cyber offenses. This legislation is key to addressing the growing risks posed by cyber threats in Pakistan, aiming to enhance data security and provide legal recourse for cyber-related crimes.⁴⁰

³⁵ Stuti Mishra, "Pakistan Says Country-Wide Power Outage could have been Caused by Cyberattack," *Independent*, January 24, 2023, <https://www.independent.co.uk/asia/south-asia/pakistan-power-outage-cause-cyber-attack-b2268053>.

³⁶ Centre for Aerospace & Security Studies, *Cyberspace as a Global Common: Formulation and Applicability of International Law*, report (Islamabad: CASS), <https://casstt.com/cyberspace-as-a-global-common-formulation-and-applicability-of-international-law-2/>.

³⁷ Ibid.

³⁸ Abdullah Momand, "Govt Notifies New Cybercrime Investigation Agency to Tackle PECA Offences," *Dawn*, May 3, 2024, <https://www.dawn.com/news/1831222>.

³⁹ International Trade Administration, "Pakistan - Country Commercial Guide, Cybersecurity," U.S. Department of Commerce, 2024, <https://www.trade.gov/country-commercial-guides/pakistan-cybersecurity#:~:text=Like%20other%20markets%2C%20the%20cybersecurity,terrorism%2C%20vandalism%2C%20and%20pornography>.

⁴⁰ Ibid.

Despite these developments, Pakistan's cyber security governance remains in its formative stages. The country's technological advancements have created both opportunities and vulnerabilities. This section further explores the governance framework that has evolved to counter the proliferation of cyber threats:

3.1. Initial Organisational Developments

In 1996, through the enactment of the Pakistan Telecommunication Act, the Pakistan Telecommunication Authority (PTA) was established. It was formed to issue licenses and regulate the telecommunication sector. With the gap of a few years, two more were added: the 'Electronic Transaction Ordinance' (ETO) and the 'Pakistan Electronic Media Regulatory Authority' (PEMRA). The former was the first legislation on the IT sector and focused on legally facilitating electronic transactions in the country, whereas the latter was established as a regulatory authority for the media industry in Pakistan, which was mushrooming at that time.⁴¹ Moreover, due to the absence of any direct legislation on data protection, data privacy was being regulated through the provisions of ETO as it criminalised illegal access to information.⁴²

3.2. Pakistan Electronic Crimes Prevention Act (PECA), 2016

The current cyber security landscape in Pakistan is primarily governed by the 'Prevention of Electronic Crimes Act' (PECA), enacted in 2016⁴³ to address crimes within the digital and information systems domain. PECA serves as the central legal framework for criminalising a wide array of cyber-related offences in Pakistan's digital space. The law specifically defines 23 different cyber offences, of which three - cyber terrorism, offences related to dignity, and offences against modesty - are categorised as cognizable, meaning they warrant immediate legal action without the need for a warrant.

Beyond its criminal provisions, PECA also encompasses procedural and regulatory elements, outlining the structure for the investigation and prosecution of cybercrimes. It designates specific authorities to handle these investigations, ensuring that only

⁴¹ Research Society of International Law, *Strengthening the Legal Framework for Cybersecurity in Pakistan: The Computer Emergency Response Team Rules, 2023*, report (Islamabad: RSIL, 2023), <https://rsilpak.org/2023/strengthening-the-legal-framework-for-cybersecurity-in-pakistan-the-computer-emergency-response-team-rules-2023/>.

⁴² Ibid.

⁴³ Government of Pakistan, *The Prevention of Electronic Crimes Act, 2016*, https://na.gov.pk/uploads/documents/1470910659_707.pdf.

authorised agencies are empowered to act. According to the PEC Rules of 2018, issued under Section 51 of PECA, the FIA is the sole entity authorised to investigate cybercriminal activities, reinforcing its central role in Pakistan's cyber governance.⁴⁴

PECA also calls for establishing Computer Emergency Response Teams (CERT) to enhance cyber security readiness and respond effectively to cyber incidents. In alignment with this requirement, the Federal Government introduced rules for the formation and operation of CERTs on 23 September 2023. These rules outline key aspects such as the creation, functioning, and essential components of CERT teams, which are tasked with managing cyber security threats and coordinating responses to incidents across critical sectors.⁴⁵ The establishment of CERTs represents a vital step toward strengthening Pakistan's overall cyber security architecture, providing a more structured approach to monitoring, responding to, and mitigating cyber threats in real time.⁴⁶

However, PECA has been the subject of criticism by various analysts and academics since its enactment. The Act defines terms, such as 'acts,' in vague and subjective ways. Public outcry has focused on PECA's infringement on fundamental rights, particularly freedom of speech. The delegation of both legislative and judicial powers to the Pakistan Telecommunication Authority (PTA), which can remove and block online content, is seen as a violation of Article 19 of the Constitution, which protects free speech.⁴⁷ The Act is also seen as ineffective in many cases, particularly due to the non-cognizable, bailable, and compoundable nature of most of its provisions. This limits its deterrent effect against cyber offences. PECA also lacks clear guidelines for investigating officers, leading to potential misuse; and struggles with jurisdiction over international entities.⁴⁸ Another study highlighted that PECA's penalties are insufficient

⁴⁴ Research Society of International Law, *Legal Framework for Policing Cyberspace in Pakistan: An Overview*, (Islamabad: RSIL, 2023), <https://rsilpak.org/2023/legal-framework-for-policing-cyberspace-in-pakistan-an-overview/>.

⁴⁵ Ibid.

⁴⁶ Centre for Aerospace & Security Studies, *Cyberspace as a Global Common*.

⁴⁷ Esha Arshad Khan, "The Prevention of Electronic Crimes Act 2016: An Analysis," *Legislative Reviews*, *LUMS Law Journal* 5 (2020), https://sahsol.lums.edu.pk/sites/default/files/2022-09/11._the_prevention_of_electronic_crimes_act_2016-_an_analysis.pdf.

⁴⁸ Waseem Haider, Ashraf Ali, and Muhammad Zubair, "Prevention of Electronic Crime Act, 2016: An Analysis of the Act's Effectiveness in Controlling Misuse of Social Media in Pakistan," *Journal of Educational Research & Social Sciences Review (JERSSR)* 3, no. 2 (April-June 2023): 48-53.

for serious cybercrimes or too harsh for minor offenses, creating a legal imbalance that hinders its overall effectiveness.⁴⁹

In 2022, PECA was amended with provisions regarding criminalising the online defamation of state institutions and authorities. This amendment made defamation non-bailable and increased the prison time from three to five years for the convicts. The Asia Associate Director of Human Rights Watch in 2022, stated, 'PECA neither protects the public from the cybercrime concerns nor respects the fundamental rights.'⁵⁰

Recently, Pakistan acquired a national firewall⁵¹ valued at USD 300 million.⁵² While government reports highlight its potential to enhance internet security, it is equally important to allocate comparable resources toward strengthening the country's indigenous cyber security capabilities. This balanced approach will ensure long-term resilience and self-sufficiency in addressing emerging cyber threats.

3.3. National Centre for Cyber Security

The government established the National Centre for Cyber Security (NCCS) in 2018 as a collaborative effort between the Higher Education Commission (HEC) and the Planning Commission 'to build national capabilities and capacities in Cyber Security and produce indigenous professionals and solutions in the field of Cyber Security.'⁵³ Following an open call for proposals, ten universities were selected after a rigorous evaluation process to establish specialised R&D labs under NCCS.⁵⁴ Air University was chosen as the NCCS Secretariat and houses two affiliated labs 'National Cyber Crime and Forensics Lab' and 'Devices & Network Security Lab.'⁵⁵

⁴⁹ Muhammad Iqbal, S.R. Talpur, A. Manzoor et al., "The Prevention of Electronic Crimes Act (PECA) 2016: Understanding the Challenges in Pakistan," *Siazga Research Journal* 2, no. 4: 273-282, <https://doi.org/10.58341/srj.v2i4.35engr>.

⁵⁰ Human Rights Watch, "Pakistan: Repeal Amendment to Draconian Cyber Law," February 28, 2023, <https://www.hrw.org/news/2022/02/28/pakistan-repeal-amendment-draconian-cyber-law>.

⁵¹ Sindhu Abbasi, "Pakistan's Firewall: Explained," *T-Magazine*, September 8, 2024, <https://tribune.com.pk/story/2494442/pakistans-firewall-explained>.

⁵² Ariba Shahid, "Pakistan's Internet Firewall could Cost Economy 300 Million, Association-Says," *Reuters*, August 12, 2024, https://www.reuters.com/technology/pakistans-internet-firewall-could-cost-economy-300-million-association-says-2024-08-15/?utm_source=pocket_saves.

⁵³ National Centre for Cyber Security, "What We Do," Accessed September 18, 2023, <<https://www.nccs.pk/nccs/what-we-do>>.

⁵⁴ National Centre for Cyber Security, "Collaborations and Academic Partners," Accessed September 18, 2023, <https://www.nccs.pk/collaborations/academic-patners>.

⁵⁵ National Centre for Cyber Security, "About NCCS," Accessed September 18, 2023, <https://www.nccs.pk/>; "The Role of National Centre for Cyber Security in Pakistan," *Nation*, July

Since its inception in 2018, the NCCS has facilitated the launch of multiple startups by supporting the development of products and prototypes through its affiliated labs. Key startups include ThingzEye Pvt Ltd; and Lynx Information Security Pvt Ltd. Other notable startups include Cyber Droid Pvt Ltd and TRIC Tech Pvt Ltd, demonstrating NCCS's impact in fostering innovation and entrepreneurship in Pakistan's cyber security landscape.⁵⁶ Furthermore, since its establishment, the NCCS labs have trained more than 4,000 individuals through more than 112 workshops, tech trainings, and relevant seminars.

The importance of skilled human resources is central to strengthening the cyber security ecosystem, with the National Cyber Security Academy (NCSA) playing a vital role in this effort. Established in November 2021 at Air University, Islamabad, the NCSA aims to bolster cyber capacity building by equipping professionals with the knowledge and skills necessary to support the government in addressing cyber threats across both the public and private sectors.⁵⁷

3.4. National Cyber Security Policy (NCSP), 2021

In 2021, the Ministry of Information Technology & Telecommunication (MoITT) formalised Pakistan's first National Cyber Security Policy (NCSP). Its scope includes *'to secure the entire cyberspace of Pakistan including all digital assets of Pakistan, data processed, managed, stored, transmitted or any other activity carried out in public and private sectors, and the information and communication systems used by the citizens of Pakistan.'*

Under the NCSP, the state should have a 'Cyber Governance Policy Committee' (CGPC) responsible for national oversight of cyber security issues, focusing on policy formulation, legal frameworks, and structural requirements. It is meant to play a key role in coordinating among departments and ensuring alignment with global cyber security standards. The CGPC also assigns roles for international representation and consultations on cyber governance. Its recommendations are subject to approval by

7, 2022, <https://www.nation.com.pk/07-Jul-2022/the-role-of-national-center-for-cyber-security-in-pakistan>.

⁵⁶ National Centre for Cyber Security, "NCCS Startups," Accessed September 18, 2023, <https://www.nccs.pk/collaborations/NCCS-Startups>.

⁵⁷ Sana Jamal, "Pakistan's First National Cyber Academy Launched," *Gulf News*, November 24, 2021, <https://gulfnews.com/world/asia/pakistan/pakistans-first-national-cyber-academy-launched-1.83925731>.

the Federal Cabinet, ensuring national-level ownership and alignment with emerging cyberspace challenges.⁵⁸

Two key guiding principles of the NCSP focus on safeguarding online data privacy and ensuring the security of citizens, thereby enhancing national prosperity in the digital sphere. The policy also underscores the gravity of a cyberattack on the country's Critical Infrastructure (CI) and Critical Information Infrastructure (CII), viewing it as 'an act of aggression against national sovereignty.'⁵⁹ Hence, under the NCSP, Pakistan asserts its right to defend itself with appropriate response measures to protect its digital assets and national interests.

Scholars argue that while the NCSP is a positive step, its effectiveness hinges on proper and timely implementation. This requires strong cooperation and coordination among relevant organisations, alongside public awareness campaigns to educate citizens about cyber threats.⁶⁰

It has also been pointed out that other key areas that still lack clarity include the CGPC's operating framework, reporting structure, powers, and membership. Without clear definitions, these bodies risk becoming inactive and ineffective. To ensure successful implementation, policymakers must establish a comprehensive cyber security framework applicable to all organisations and implement a robust audit mechanism to maintain compliance. Clarifying CGPC's structure and responsibilities will be critical for achieving effective cyber security governance across all sectors.⁶¹

⁵⁸ Ministry of Information Technologies and Communication, *National Cyber Security Policy, 2021* (Government of Pakistan, 2021), <https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf>.

⁵⁹ Ibid., p.8.

⁶⁰ Sara Ahmed, "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): 26-40, https://web.archive.org/web/20220809150211id_/https://journals.wumardan.edu.pk/view_paper.php?paper_id=296.

⁶¹ Muneeb Imran Shaikh, "Pakistan's Cybersecurity Policy in 2021: A Review," *ISACA*, November 8, 2021, <https://www.isaca.org/resources/news-and-trends/industry-news/2021/pakistans-cybersecurity-policy-in-2021-a-review>.

3.5. Cyber Security Strategy for the Telecom Sector

In line with the NCSP, the Pakistan Telecom Authority (PTA) launched the 'Cyber Security Strategy 2023-2028 for Telecom Sector'⁶² in December 2023. It is an ambitious five-year plan that focuses on enhancing the digital resilience of the country's existing telecom infrastructure against cyber threats.⁶³ The roadmap of this strategy underlines six foundational pillars, each pertaining to one aspect of cyber security such as 'legal framework, cyber resilience, proactive monitoring and incident response, capacity building, cooperation and collaboration and public awareness.'⁶⁴

Moreover, the PTA has outlined a set of expectations from the telecom companies to ensure the strategy's implementation. Some of the significant ones outline that telecom companies should:

- Protect customer data by implementing robust security measures.
- Provide customers with information about cyber security threats and how to protect themselves from such threats.
- Develop short-term (yearly), medium-term (2-3 years), and long-term (3-5 years) plans to meet cyber security objectives.
- Ensure compliance with PTA directives and adhere to the cyber security framework.
- Train all personnel in cyber security practices to safeguard against internal threats and ensure organisational readiness.⁶⁵

While this telecom cyber security strategy presents a solid framework to enhance the security and resilience of telecom companies against evolving cyber risks, it remains too early to assess its success since it is still in its initial stages.

⁶² Pakistan Telecom Authority, *Cyber Security Strategy for Telecom Sector 2023-2028* (Government of Pakistan, 2023), https://pta.gov.pk/assets/media/cyber_security_strategy_telecom_sector_2023_2028_11-12-2023.pdf.

⁶³ "PTA 'Cyber Security Strategy' to Enhance Telecom Sector's Digital Resilience," *News International*, December 12, 2023, <https://www.thenews.com.pk/latest/1137625-pta-cyber-security-strategy-to-enhance-telecom-sectors-digital-resilience>.

⁶⁴ Pakistan Telecom Authority, *Cyber Security Strategy for Telecom Sector 2023-2028*.

⁶⁵ Ahmad Haamdani, "Fortifying Telecom Sector": PTA Unveils Cyber Security Strategy 2023-2028," *Pakistan Today*, December 22, 2023, <https://www.pakistantoday.com.pk/2023/12/22/fortifying-telecom-sector-pta-unveils-cyber-security-strategy-2023-2028/>.

3.6. Computer Emergency Response Teams (CERTs) Rules, 2023

Over the past decade, the communication industry has expanded rapidly, driven by modern communication devices that facilitate global connectivity. This growth has exposed organisations operating in a digital, computer-based environment to heightened risks of cyberattacks. Historically, Pakistan lacked a strong institutional framework to manage and secure its cyberspace. However, a significant development occurred in September 2023 with the introduction of 'Computer Emergency Response Teams (CERTs) Rules, 2023'.⁶⁶ These rules are designed to provide legislative protection against cyber threats at national, sectoral, and organisational levels. Their practical implementation is being supported by the announcement of National Security Operations.⁶⁷ However, only with a comprehensive evaluation after a period of operation will the success of these initiatives in managing cyber risks be fully understood.

3.7. National Cyber Crimes Investigation Agency (NCCIA), 2024

The creation of the National Cyber Crimes Investigation Agency (NCCIA), officially notified by the Federal Government in May 2024, marks a significant restructuring in Pakistan's approach to combatting electronic crimes. Ironically though, its establishment effectively renders the FIA's Cybercrime Wing 'defunct', transferring its personnel, assets, liabilities, and ongoing investigations to the new agency. This move, enacted under Sections 51 and 29 of the Prevention of Electronic Crimes Act, 2016, represents a strategic shift to centralise and improve Pakistan's cybercrime enforcement capabilities. According to government directives, this transition is also aimed to plug the gap between both domestic and international cybercrime cooperation.⁶⁸

While the NCCIA promises to strengthen Pakistan's cyber security architecture, the interim period during which former FIA personnel continue their duties until NCCIA's staffing is complete introduces potential challenges in maintaining seamless

⁶⁶ Ministry of Information Technology and Telecommunications, *Computer Emergency Response Teams (CERTs) Rules, 2023* (Government of Pakistan, September 26, 2023), https://moitt.gov.pk/SiteImage/Misc/files/CERT_Rules_2023.pdf.

⁶⁷ Tahir Amin, "CERT Rules, 2023 Notified To Bolster Cyber Security Defences," *Business Recorder*, October 13, 2023, <https://www.brecorder.com/news/40267846>.

⁶⁸ "National Cyber Crimes Investigation Agency Notified to Deal with Offences under PECA Act," *Nation*, May 4, 2024, <https://www.nation.com.pk/04-May-2024/national-cyber-crimes-investigation-agency-notified-to-deal-with-offences-under-peca-act>.

operational continuity. Nevertheless, the NCCIA's formation signals a proactive approach to mitigating rising cyber threats through improved governance and international collaboration.

4. Cyber Security Risk Governance: Looking Ahead

Research indicates that in many developing countries, there is often a significant disconnect between policy formulation and effective implementation. This gap is typically driven by structural inefficiencies, lack of resources, and inadequate coordination among key agencies.⁶⁹ In particular, policies are frequently well-drafted, but they fall short in execution due to insufficient institutional capacity and the absence of clear, enforceable frameworks. In the context of cyber security, the complexity of inter-agency collaboration and the rapid evolution of cyber threats exacerbate these challenges. For example, while PECA laid a legal foundation, subsequent policies, like the NCSP, continue to struggle with practical implementation, mirroring the global trend in developing countries where policy reforms often face barriers at the execution stage.⁷⁰ Plus, ideally, 'policy' guides the development of strategies and corresponding 'legislation', but this reversal in countries like Pakistan (where PECA came before the NCSP) reflects broader governance issues.⁷¹

Over the past years, the Federal Government has taken various steps focusing on the curation of Pakistan's cyber security framework. But with each passing day, the nature and lethality of cyber threats have been increasing. To address the complex and evolving cyber threat landscape, there is a pressing need for enhanced cyber security risk governance in the country. 'Cyber Security Risk Governance' involves methodologies, tools, and frameworks employed to manage and mitigate cyber risks.⁷²

⁶⁹ D.D. Kipo-Sunyezi, "Implementation Research in Developed and Developing Countries: An Analysis of the Trends and Directions," *Public Organiz Rev* 23: 1259-1273 (2023), <https://doi.org/10.1007/s11115-022-00659-0>.

⁷⁰ Ibid.

⁷¹ Amna Rafiq, "National Cyber Security Policy of Pakistan 2021," *Institute of Strategic Studies*, October 15, 2021, https://issi.org.pk/wp-content/uploads/2021/10/IB_Aamna_Oct_15_2021.pdf.

⁷² International Risk Governance Council, *Cyber Security Risk Governance*, report (Zurich: Swiss Centre for Global Dialogue, October 29-30, 2015), <https://irgc.org/wp-content/uploads/2018/09/Cyber-Security-Risk-Governance-29-30-October-2015-Workshop-Report.pdf>; Centraleyes, "Cyber Security Governance", Accessed December 27, 2023, <https://www.centraleyes.com/glossary/cyber-governance/>.

To ensure a secure digital environment, Pakistan must prioritise synchronised implementation of cyber security measures outlined in its various policies discussed earlier, including effective documentation and reporting of cyber security practices to ensure compliance with digital security laws and demonstrate the country's commitment to *cyber security risk governance*. However, for this framework to be effectively operationalised, the country must tackle several structural and indigenous challenges and focus on inclusive solutions as discussed below:

4.1. Reduce Fragmentation and Bureaucratic Overlap in Cyber Security Governance

Transitioning cybercrime investigations from one agency (FIA Cyber Wing) to another (NCCIA)⁷³ is likely to create an immediate gap in institutional continuity, which can disrupt ongoing investigations and weaken cyber security enforcement during the handover period. Furthermore, the sudden change raises concerns about resource allocation, expertise transfer, and operational clarity. While the NCCIA aims to safeguard digital rights, the overlap in responsibilities and the interim arrangement of having FIA personnel continue their roles for another year may lead to confusion, inefficiencies, and delayed response to cyber threats. This structural shift also risks undermining public trust in cyber security efforts, as the shift from an established entity to a new one could be seen as a destabilisation of existing protections. Such abrupt changes in governance, particularly without clear delineation of roles and accountability, need to be avoided.

4.2. Apply Structured Cyber Risk Governance Protocols

Effective documentation and reporting of cyber security practices are essential to ensure compliance with digital security laws and demonstrate the country's commitment to cyber security risk governance. Responsibility extends across all departments, requiring collaboration to proactively address security risks. This inter-departmental coordination is critical in a government structure where multiple ministries and agencies must align to protect sensitive national data.

Cyber risk governance in Pakistan must establish clear internal controls. These controls should be tailored to high-risk areas like national databases and financial systems, where breaches could have severe consequences. Proper documentation of these

⁷³ Momand, "Govt Notifies New Cybercrime Investigation Agency to Tackle PECA Offences."

controls is not just a procedural necessity but a means of building trust with international partners and internal auditors, showcasing the government's seriousness about cyber security.

Moreover, a well-defined approach to internal controls, with specific responsibilities assigned to each ministry or department, will strengthen the country's readiness for external audits, whether by international bodies or third-party organisations.⁷⁴ Such preparedness will help Pakistan's legal compliance and mitigate the risk of cyber incidents, ultimately adding value by ensuring that cyber security efforts are integrated across all governmental operations. A controls-focused strategy will allow Pakistan to streamline its cyber risk governance, reducing the overall time and resources spent managing these risks while allowing departments to focus on their core functions.⁷⁵

By applying structured cyber governance protocols, Pakistan can achieve a stronger understanding of its internal processes, increase compliance, and create a resilient framework to address the ever-evolving nature of cyber security threats.

4.3. Increase Digital Literacy and Cyber Security Awareness

Pakistan must take proactive steps to improve digital literacy, as the current lack of awareness leaves much of the population vulnerable to cyber threats. With only 34 percent of adults possessing adequate digital skills, according to a 2020 World Bank study, there is an urgent need to educate the public on surfing the digital space safely. As the digital economy grows, with a 48 percent rise in freelancers (with earnings of around USD 400 million) from 2021-22,⁷⁶ the sustainability of these ventures depends on cyber security awareness. Raising digital literacy should not only focus on basic skills but also put emphasis on online safety and threat mitigation, creating a more resilient digital landscape.

4.4. Expand Infrastructure, Connectivity and Access

Pakistan must prioritise expanding internet infrastructure to bridge the stark digital divide. In areas like Balochistan, inadequate connectivity limits social and economic mobility, contributing to the country's low ranking of 79th globally in the Inclusive

⁷⁴ Peter Trim and Yang-Im Lee, *Cyber Security Management-A Governance, Risk and Compliance Framework*, First Edition (London: Routledge), 2016.

⁷⁵ Ibid.

⁷⁶ Aun Haider, "The Rise of Freelancing in Pakistan," *Medium*, June 28, 2023, <https://medium.com/@aunhaider/the-rise-of-freelancing-in-pakistan-b9020dd8af7c>.

Internet Index (2022).⁷⁷ Approximately 40% of non-mobile internet users struggle with basic device operation, highlighting the need for targeted digital inclusion initiatives.⁷⁸

To fully capitalise on digital transformation, the government must invest in upgrading infrastructure and ensuring equal access, while simultaneously educating citizens on how to effectively engage with the digital world. By addressing 'Access and Awareness' together, Pakistan can drive inclusive growth and better integrate underserved regions into the digital and innovation economy.

4.5. Regulate Inclusive Policy on Data Protection

In today's digital age, data is often regarded as the new currency, making the protection of personal information critically important. Personal data, which includes details such as names, phone numbers, CNIC numbers, and financial information, is highly valuable and susceptible to breaches. A data breach can lead to serious consequences such as identity theft or the creation of fraudulent, *benami* accounts. Therefore, ensuring data privacy and understanding the risks associated with data breaches are essential to safeguarding both personal and financial security.⁷⁹ Moreover, businesses increasingly rely on personal data and advanced analytical technologies to gain insights into consumer behaviours and preferences. This data-driven approach allows companies to tailor their products, services, and marketing strategies to meet consumer demands more effectively. However, personal data should not be treated as a mere commodity, as it is closely tied to an individual's autonomy and privacy rights.⁸⁰ Recognising this, many countries have implemented laws to ensure the protection of their citizens' data, requiring organisations to obtain explicit consent before collecting or sharing personal information. One prominent example is the European Union's General Data Protection Regulation (GDPR), which empowers individuals to control their data and holds organisations accountable for its proper handling. Similarly, Pakistan urgently needs a clear and comprehensive data

⁷⁷ Economist Impact, "Inclusive Internet Index 2022," Accessed December 27, 2023, <https://impact.economist.com/projects/inclusive-internet-index/2022/country/Pakistan>.

⁷⁸ "Digital Literacy at Centre of Economic Growth," *Pakistan Observer*, February 13, 2020, <https://pakobserver.net/digital-literacy-at-center-of-economic-growth/>.

⁷⁹ Hikmat Turabi, "Protecting Personal Info," *Dawn*, April 17, 2023, <https://www.dawn.com/news/1747903/protecting-personal-info>.

⁸⁰ Ibid.

protection law that prioritises the autonomy and rights of personal data, ensuring it is protected and handled with the utmost responsibility.

Pakistan has shown a relatively slow response in establishing robust data protection and privacy regulations. While several regulations aim at protecting data, the country lacks a comprehensive legal framework to govern the storage, processing, and transfer of personal data. The 'Personal Data Protection Bill', introduced in 2021,⁸¹ remains in its consultation phase as of mid-2024, yet to be enacted into law.⁸²

However, the process surrounding the bill has raised significant concerns. Reports indicate that the Federal Cabinet approved the bill and moved it to the National Assembly without sufficient prior consultation or debate. Organisations like Privacy International (PI) have scrutinised multiple versions of the bill, warning that its current form would fail to offer meaningful protection for citizens' data and privacy rights.⁸³ In an era where Pakistan is pushing for greater digitalisation, an effective and unambiguous data protection law is critical to safeguard personal information, ensure accountability, and instill public confidence in the digital economy. Without such a law, the country risks lagging behind in both protecting individual privacy and advancing its digital agenda.

4.6. Adopt Advanced Cyber Security Technologies

From a technological perspective, Pakistan must urgently prioritise securing its critical institutions by deploying advanced cyber security systems. In this effort, leveraging state-of-the-art tools like 'Zero Trust Architecture',⁸⁴ which enforces strict access control, and AI-driven threat detection systems that utilise Machine Learning to predict and mitigate emerging threats, will be essential. Furthermore, Pakistan can adopt

⁸¹ Sahar Iqbal, "Data Privacy and Protection in Pakistan," *International Bar Association*, July 24, 2023, <https://www.ibanet.org/data-privacy-and-protection-in-Pakistan>.

⁸² Tahir Amin, 'IT Ministry Finalising Personal Data Protection Bill', *Business Recorder*, May 22, 2024, <https://www.brecorder.com/news/40304612>.

⁸³ "Privacy International Raises Concerns regarding Pakistan's Personal Data Protection Bill," *Privacy International*, August 8, 2023, <https://privacyinternational.org/news-analysis/5090/privacy-international-raises-concerns-regarding-pakistans-personal-data>.

⁸⁴ National Institute of Standards and Technology, *Zero Trust Architecture*, Special Publication 800-207, report (U.S. Department of Commerce), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>.

advanced encryption protocols, such as Post-Quantum Cryptography (PQC),⁸⁵ which are designed to protect data even against future quantum computing threats.

To enhance cyber security resilience, the government should invest in tools such as Identity and Access Management (IAM) solutions⁸⁶ to secure user authentication and data access across sectors. Additionally, deploying Operational Technology (OT)⁸⁷ security tools to safeguard infrastructure, especially in industries like energy and transport, is vital given the increasing sophistication of cyberattacks on critical infrastructure worldwide. These technologies, paired with continuous monitoring solutions, will help Pakistan proactively secure its critical systems.⁸⁸

4.7. Move towards Indigenisation and Data Localisation

To effectively enhance Pakistan's cyber security infrastructure, prioritising the development of indigenous software and hardware is essential. By focusing on indigenising end-to-end encryption capabilities, Pakistan can secure local data flows more robustly. Moreover, aligning this strategy with a data localisation policy,⁸⁹ the country should invest in the creation of homegrown data centres, which are pivotal for building secure digital ecosystems. This comprehensive approach will not only safeguard the integrity of local data but also position Pakistan to capitalise on emerging opportunities in cloud computing and AI, fostering long-term growth and competitiveness in these high-tech fields.

4.8. Information Sharing and Global Collaboration

Given the global nature of cyber threats and related crimes, establishing international cooperation is essential. In this era of rapid digital growth, effective information sharing between government agencies and international actors can greatly enhance collaboration in detecting and addressing cyber threats, provided it is handled with

⁸⁵ National Institute of Standards and Technology, "Post-Quantum Cryptography," *Information Technology Laboratory, Computer Security Resource Center*, August 13, 2024, <https://csrc.nist.gov/projects/post-quantum-cryptography>.

⁸⁶ CyberArk, "What is Identity and Access Management (IAM)?", Accessed December 1, 2023, <https://www.cyberark.com/what-is/iam/>.

⁸⁷ CISCO, "What is OT Security?", Accessed December 1, 2023, <https://www.cisco.com/site/us/en/learn/topics/security/what-is-ot-security.html>.

⁸⁸ Ehtisham Ul Haque et al., "Cyber Forensic Investigation Infrastructure of Pakistan: An Analysis of the Cyber Threat Landscape and Readiness," *IEEE Access* 11 (2023): 40049-63.

⁸⁹ Data localisation policy refers to regulations that require data, especially sensitive or personal information, to be stored and processed within a country's borders to ensure security, privacy, and sovereignty over local data.

diligence and care. However, Pakistan has yet to ratify the Budapest Convention, the world's first and most comprehensive international treaty on cybercrime.⁹⁰ Pakistan has refrained from signing the Budapest Convention due to concerns that sharing data with international law enforcement could compromise the country's sovereignty.⁹¹ That such cooperation may lead to foreign entities accessing sensitive information, which could be seen as an intrusion. However, cyber threats are inherently transnational, making international cooperation essential. Pakistan must consider establishing a secure information-sharing infrastructure that balances privacy concerns with the need for collaboration in tracking, investigating, and prosecuting cybercriminals. By participating in a multilateral arrangement, Pakistan can address its sovereignty concerns while strengthening its ability to combat cybercrime on a global scale.

5. Conclusion

In conclusion, Pakistan's journey through the evolving digital landscape brings both opportunities and challenges, particularly in the realm of cyber security. While the country has made strides in developing legislation and policies to address the rising cyber threats, its current framework remains insufficient. The primary challenges include inadequate digital literacy, ambiguous laws, limited international cooperation, and a weak institutional framework, all of which hinder effective cyber risk governance. To ensure comprehensive protection against cyber threats, Pakistan must modernise its *Cyber Security Risk Governance* framework and prioritise implementation of robust, transparent mechanisms that respect constitutional rights, such as fair judicial process and freedom of expression. By addressing these key gaps and enhancing collaboration on a global scale, Pakistan can strengthen its defences against the growing threat of cybercrime and ensure a secure digital environment for its citizens.

⁹⁰ Faran Mahmood, "Should Pakistan Sign the Budapest Convention?," *Express Tribune*, November 21, 2022, <https://tribune.com.pk/story/2387309/should-pakistan-sign-the-budapest-convention>.

⁹¹ Faran Mahmood, "The Long Road to Becoming Cyber Power," *Express Tribune*, July 10, 2023, <https://tribune.com.pk/story/2425486/the-long-road-to-becoming-cyber-power>.



ABOUT THE AUTHOR

Ajwa Hijazi is a Research Assistant at the Centre for Aerospace & Security Studies (CASS), Islamabad. She has done her MPhil in Peace and Conflict Studies from the National Defence University (NDU), Islamabad. Earlier, she completed her undergraduate degree in Defence and Diplomatic Studies from the Fatima Jinnah Women University (FJWU), Rawalpindi, Pakistan. Her research interests include traditional and non-traditional security with a focus on internal security, human security, and electoral politics.

ABOUT CASS

The Centre for Aerospace & Security Studies (CASS), Islamabad, was established in 2018 to engage with policymakers and inform the public on issues related to aerospace and security from an independent, non-partisan and future-centric analytical lens. The Centre produces information through evidence-based research to exert national, regional and global impact on issues of airpower, emerging technologies and security.

VISION

To serve as a thought leader in the aerospace and security domains globally, providing thinkers and policymakers with independent, comprehensive and multifaceted insight on aerospace and security issues.

MISSION

To provide independent insight and analysis on aerospace and international security issues, of both an immediate and long-term concern; and to inform the discourse of policymakers, academics, and practitioners through a diverse range of detailed research outputs disseminated through both direct and indirect engagement on a regular basis.

CORE AREAS OF RESEARCH

Aerospace

Emerging Technologies

Security



Strategic Foresight



**CENTRE FOR
AEROSPACE & SECURITY
STUDIES, ISLAMABAD**
Independence. Analytical Rigour. Foresight

 Old Airport Road, Islamabad, Pakistan
 cass.thinkers@casstt.com
 Centre for Aerospace & Security Studies

 +92 051 5405011
 www.casstt.com
 [cassthinkers](https://www.instagram.com/cassthinkers)

 [@CassThinkers](https://twitter.com/CassThinkers)
 [cass.thinkers](https://www.facebook.com/cass.thinkers)