Print ISSN: 0215-0411 - Online ISSN : 0215-0419
Volume: 2 , Issue: 4, Winter 2023

Special Issue
Winter 2023

Khyber Journal of Public Policy

KJPP

National Institute of Public Administration

National School of Public Policy

Report of Policy Lab on Bridging Gaps in National Security Policies and their Implementation in Pakistan

پاکستان میں قومی سلامتی کی پالیسیوں کے اطلاق میں حائل رکاوٹوں کا خاتمہ

Policy Analysis & Recommendations- Part-6 of 11

Pakistan's Cyber Security

Assessing cyber security threats, digital infrastructure protection, and cyber policy frameworks.

Team Lead
Dr. Muqeem Islam Soharwardy
Phd (Public Policy & Governance) NDU
MPhil (Economic Development)
Chief Instructor,
National Institute of Public Administration (NIPA)
National school of Public Policy (NSPP),
Editor, Khyber Journal of Public Policy (KJPP)
Former Director General (NAVTTC), GoP
muqeemz@gmail.com, +92-343-5090648

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

إِنَّ اللّٰه لَا يُغَيِّرُ مَا بِقَوْمٍ حَتَّىٰ يُغَيِّرُوا مَا بِأَنفُسِهِمْ

(سورة الرعد 13:11)

بے شک، اللہ کسی قوم کی حالت نہیں بدلتا جب تک وہ خود اپنی حالت کو نہ بدلے۔

Indeed, Allah does not change the condition of a people
until they change what is in themselves.
(Surah Ar-Ra'd 13:11)

ظَهَرَ الْفَسَادُ فِي الْبَرِّ وَالْبَحْرِ بِمَا كَسَبَتْ أَيْدِي النَّاسِ لِيُذِيقَهُمْ بَعْضَ الَّذِي عَمِلُوا لَعَلَّهُمْ يَرْجِعُونَ

(سورة الروم 30:41)

خشکی اور تری میں فساد ظاہر ہو گیا ہے، لوگوں کے اپنے ہاتھوں کے کیے ہوئے اعمال کی وجہ سے، تاکہ اللہ انہیں ان کے کچھ اعمال کا مزہ چکھائے، شاید کہ وہ باز آ جائیں۔

Corruption has appeared on land and sea because of
what the hands of people have earned, so that
He may let them taste part of what they have done,
that perhaps they will return (to righteousness).
(Surah Ar-Rum 30:41)

Pakistan's Cyber Security

Assessing cybersecurity threats, digital infrastructure protection, and cyber policy frameworks.

Research Group

- **Dr. Muqeem Islam Soharwardy (Team Lead)**
- Abul Hassan Kashan
- Azhar Mehmood
- Sami Ur Rehman Khan
- Tariq Aziz
- Jehanzeb Khan Orakzai

Preface

Public policy formulation and implementation are dynamic processes that require a comprehensive understanding of national security in all its dimensions. To equip policymakers, practitioners, and scholars with the necessary analytical tools to assess and refine policy strategies, a **Policy Simulation Lab on Analyzing & Evaluating Implementation Strategies for Pakistan's National Security Dimensions** was conceptualized, designed, and mentored by **Dr. Muqeem Islam Soharwardy** in **November 2023**.

This **Policy simulation Lab** was a unique initiative aimed at critically assessing the effectiveness of policy implementation strategies across multiple domains of national security. It provided a structured environment where participants engaged in high-level problem-solving, scenario planning, and decision-making to address contemporary security challenges. The exercise was framed around a holistic approach to national security, moving beyond traditional defense mechanisms to include economic, environmental, cyber, and cultural security considerations.

The report of **Policy simulation Lab** presents the findings and recommendations of **nine Task Forces**, each dedicated to evaluating implementation strategies for a specific security dimension. These include:

1. **Energy Security** – Examining sustainable and resilient energy policies to ensure national energy independence and efficiency.
2. **Economic Security** – Identifying strategies to strengthen Pakistan's economic resilience, trade policies, and financial stability.
3. **Social Security** – Addressing social protection mechanisms, inequality, and welfare policies to promote social cohesion.
4. **Environmental Security** – Evaluating environmental policies to mitigate climate risks, resource depletion, and ecological threats.
5. **Military Security** – Reviewing the strategic defense framework, modernization efforts, and geopolitical considerations.
6. **Cybersecurity** – Assessing cybersecurity threats, digital infrastructure protection, and cyber policy frameworks.
7. **Health Security** – Developing robust public health policies to counter emerging health crises and pandemics.
8. **Food Security** – Ensuring sustainable agricultural policies, food distribution, and supply chain resilience.
9. **Cultural Security** – Analyzing policies to protect national identity, cultural heritage, and counter ideological extremism.

Each task force conducted an in-depth examination of current policy frameworks, identified key challenges, and proposed actionable strategies to enhance national security implementation. The insights gained from this simulation exercise offer valuable contributions to policy discourse and serve as a strategic guide for decision-makers.

This report is a testament to the collaborative efforts of participants, researchers, and policymakers who engaged in this exercise with commitment and intellectual rigor. It is our hope that the findings herein will serve as a valuable resource for shaping Pakistan's future national security policies in an increasingly complex global landscape.

It is hoped that this document will serve as a significant milestone in the design, implementation, and facilitation of policies, paving the way for broader economic and industrial transformation in Pakistan, انشاءالله .

Dr. Muqeem Islam Soharwardy,
PhD (Public Policy & Governance) NDU
MPhil (Economic Development)
Chief Instructor,
National Institute of Public Policy (NIPA)
National School of Public Policy (NSPP)
Editor, Khyber Journal of Public Policy (KJPP)
Former Director General, NAVTTC, GoP
muqeemz@gmail.com , +92 3435090648

December 15, 2023

Executive Summary

Cybersecurity has become an indispensable component of the digital infrastructure in Pakistan and around the world. With the exponential growth in the use of the internet and digital technologies, the country faces a wide array of cybersecurity threats that threaten its critical infrastructure, economy, and citizens' privacy. These threats include malicious hacking, data breaches, and a growing range of cybercrimes that increasingly target individuals and organizations. This document explores the state of cybersecurity in Pakistan, examining its policies, challenges, existing implementations, and key recommendations for improvements.

Cybersecurity Threats and Challenges

Pakistan is encountering a range of cybersecurity threats that continue to evolve rapidly. These include phishing attacks, ransomware, distributed denial-of-service (DDoS) attacks, malware, SQL injection, and social engineering scams. With the expansion of the Internet of Things (IoT), the country's vulnerability to cybercriminals is further heightened as these devices often lack adequate security measures. Moreover, insider threats—where employees or trusted individuals within organizations misuse their access—pose significant risks.

The evolving nature of these cyber threats requires continuous adaptation of cybersecurity measures. The increasing sophistication of state-sponsored cyber-espionage activities and ransomware campaigns underlines the urgency for improved cybersecurity resilience. In addition to these technological threats, Pakistan’s legal framework still grapples with addressing complex cybercrimes, balancing national security with privacy concerns, and ensuring compliance with international standards.

Cybersecurity Policies and Legislation

The Government of Pakistan has made considerable strides in developing a legal and regulatory framework to address cybersecurity issues. Key initiatives include the establishment of the Pakistan Computer Emergency Response Team (PakCERT) and the National Response Center for Cyber Crimes (NR3C), which play critical roles in responding to cyber incidents. The enactment of the Prevention of Electronic Crimes Act (PECA) 2016 laid a solid foundation for combating cybercrimes and protecting digital rights. Additionally, the National Cybersecurity Policy 2021 outlines a comprehensive framework for cyber governance, infrastructure protection, and international collaboration.

The National Cybersecurity Policy 2021 envisions a robust cybersecurity framework, focusing on governance, crime response, capacity-building, and global cooperation. It emphasizes the need for a coordinated approach among governmental agencies, private

sector organizations, and civil society. However, its success depends on effective implementation strategies, which remain insufficiently defined in the policy document.

Critical Analysis of Policy Implementation

Despite the establishment of comprehensive legal frameworks like PECA and the National Cybersecurity Policy 2021, there are significant gaps in policy implementation. A major challenge lies in the absence of concrete strategies for translating policy objectives into actionable steps. Although the National Cybersecurity Policy 2021 outlines broad goals such as creating a "Central Entity" for oversight and fostering public-private partnerships, it lacks clear guidelines on how these measures will be executed. Furthermore, there is limited emphasis on financial resources or institutional coordination, leaving the policy's successful implementation uncertain.

The policy also overlooks crucial aspects like stakeholder involvement in the policy design process and the need for continuous feedback loops between different cybersecurity entities. While the establishment of the Cyber Governance Policy Committee (CGPC) provides a central body for oversight, progress has been slow, and stakeholder engagement remains limited. The lack of clarity on institutional roles and funding mechanisms has hindered progress in implementing the policy, particularly in sectors such as finance, telecom, and public services.

Stakeholder Involvement and Engagement

Stakeholder engagement is essential to the success of any cybersecurity policy, yet it has been insufficient in Pakistan’s approach. While the National Cybersecurity Policy 2021 acknowledges the role of stakeholders, including the private sector and academia, there is little transparency about how these groups will be involved in the policy’s design, implementation, and execution. The document does mention the need for public-private partnerships but fails to elaborate on concrete strategies for collaboration, including timelines, specific roles, and the level of engagement from each stakeholder.

Moreover, the lack of meaningful engagement with the private sector, particularly in areas such as cybersecurity training, funding, and research, has limited the scope of cybersecurity awareness and resilience in Pakistan. This is compounded by a shortage of skilled professionals and an inadequate cybersecurity workforce. Many organizations are still reluctant to adopt best practices, relying heavily on outsourced solutions rather than building local expertise.

Institutional Frameworks for Implementation

For the National Cybersecurity Policy 2021 to succeed, institutional frameworks must be established and strengthened. The policy outlines the creation of a Cyber Governance Policy Committee (CGPC), which will oversee the implementation of the policy at the national level. However, the document lacks clarity on how this committee will interact with other key institutions, including sectoral regulators and CERTs (Computer Emergency Response Teams), to ensure coordination across different areas of government and industry.

The financial sector, in particular, has made some progress through the State Bank of Pakistan's directives for cybersecurity outsourcing, but this is a reflection of the sector's limited internal capacity to manage cybersecurity risks effectively. Similarly, the telecommunications sector has also been slow to implement robust cybersecurity frameworks, indicating a lack of urgency in addressing systemic vulnerabilities.

Recommendations for Improvement

To strengthen Pakistan's cybersecurity posture, several key measures must be taken. First, it is essential to develop clear and actionable implementation strategies for the National Cybersecurity Policy 2021. These should include specific roles for stakeholders, timelines for implementation, and mechanisms for monitoring progress. A critical component of this is increasing financial investment in cybersecurity infrastructure, research, and capacity-building programs.

Furthermore, a concerted effort should be made to engage stakeholders meaningfully in both policy design and implementation. This would help ensure that the policy reflects the diverse needs of different sectors and incorporates feedback from all relevant actors. Public-private partnerships should be fostered to build a resilient cybersecurity ecosystem that can respond to evolving threats.

Finally, the establishment of institutional frameworks such as CERTs for key sectors, including finance and telecommunications, is vital. These frameworks must operate with clear roles and responsibilities and be equipped with the necessary resources and personnel to manage cyber risks effectively. Monitoring and evaluation mechanisms should also be implemented to track progress and address any shortcomings in real-time.

The National Cybersecurity Policy of 2021 emphasizes the importance of a structured, coordinated, and adaptive approach to cybersecurity as essential for Pakistan's national security. The policy recognizes that safeguarding digital infrastructure and the privacy of citizens against evolving cyber threats requires a comprehensive, multi-stakeholder framework. The government's efforts, along with active cooperation between public and private sectors, aim to establish a secure digital ecosystem.

The following recommendations are critical to strengthen the national cybersecurity posture, aligning with Pakistan's strategic goals:

1. National Cybersecurity Strategy

- **Objective:** Develop and implement a comprehensive strategy to safeguard critical national infrastructure and protect sensitive data.
- **Action:** Establish a unified approach involving government agencies, private sectors, and international collaborations to mitigate cyber threats and ensure a coordinated incident response.

2. Critical Infrastructure Protection

- **Objective:** Protect vital infrastructure, including energy, healthcare, and transportation systems, from both physical and cyber threats.

- **Action:** Implement risk assessments, security protocols, and resilience plans while fostering cooperation across government, private, and critical infrastructure sectors.

3. Strengthening Legal and Regulatory Framework

- **Objective:** Build a robust legal structure to address cybersecurity challenges and privacy concerns effectively.
- **Action:** Regular updates to laws and regulations, ensuring compliance while promoting innovation and safeguarding citizens' rights.

4. Data Privacy and Protection

- **Objective:** Safeguard personal data from unauthorized access and breaches, maintaining citizens' trust in digital systems.
- **Action:** Introduce robust data privacy regulations in line with global standards like GDPR to protect individuals' privacy and ensure transparent data handling practices.

5. Investment in Cybersecurity Education and Workforce Development

- **Objective:** Build a highly skilled cybersecurity workforce to protect against and respond to evolving cyber threats.
- **Action:** Develop targeted educational programs, training centers, and public awareness campaigns to cultivate a knowledgeable cybersecurity workforce.

6. Facilitating International Cooperation

- **Objective:** Enhance global cybersecurity efforts through cooperation and information-sharing with international partners.
- **Action:** Work with global counterparts to develop common standards, share threat intelligence, and strengthen collective cyber defense mechanisms.

7. Public Awareness Campaign

- **Objective:** Empower citizens with the knowledge to protect their digital lives through better cybersecurity practices.
- **Action:** Launch nationwide campaigns educating the public on common threats, safe practices, and the importance of securing personal data.

8. Addressing Emerging Technologies in Cybersecurity

- **Objective:** Stay ahead of new cybersecurity threats arising from emerging technologies like AI, IoT, and quantum computing.
- **Action:** Research and adopt cybersecurity measures tailored to emerging technologies, ensuring they do not become vulnerabilities.

9. Effective Incident Response Plan

- **Objective:** Ensure prompt and efficient responses to cybersecurity incidents to minimize damage and restore systems.
- **Action:** Develop clear procedures and designated teams to handle cybersecurity breaches, including communication strategies and recovery protocols.

10. Securing the Supply Chain

- **Objective:** Safeguard digital supply chains from cyber threats that can compromise hardware, software, or services.
- **Action:** Establish strict security measures to assess and monitor third-party suppliers, ensuring their security practices meet national standards.

Strategic Recommendations

1. Secure Communication Infrastructure

1.1 Develop a Secure, Encrypted Government Communication Platform

- Establish a Pakistan-exclusive encrypted communication system (e.g., China's WeLink, Russia's Era Messenger) for government and military personnel.
- Restrict the use of WhatsApp, Zoom, and foreign communication apps for sensitive discussions.
- Implement end-to-end encryption and self-destructing messages for classified communications.

1.2 Secure Zoom, Video Conferencing & Online Meetings

- Develop government-controlled video conferencing software with Pakistan-based servers.
- Enforce multi-factor authentication (MFA) and AI-powered intrusion detection to prevent hacking.
- Mandate VPN usage and private network access for remote meetings.

1.3 Regulate & Monitor Satellite Internet Usage

- Restrict Starlink and other foreign satellite internet services in military, foreign, and intelligence offices.
- Develop Pakistan's own encrypted satellite communication system for military and diplomatic use.
- Implement real-time monitoring & AI-based tracking of satellite communication devices used by government officials.

2. Telecom & Digital Infrastructure Security

2.1 Restrict Foreign SIM Cards & Enforce Local Telecom Security

- Ban or strictly regulate foreign SIM cards in government offices to prevent unauthorized data leaks and espionage.
- Mandate that all official communications occur through Pakistani telecom networks with government-approved encryption protocols.
- Implement geo-fencing technology to block unauthorized devices in sensitive locations (e.g., military bases, foreign embassies).

2.2 Implement AI-Driven Call & Internet Traffic Surveillance

- Establish an AI-powered cybersecurity center to monitor suspicious call activity, deepfake voice cloning, and internet traffic within government networks.
- Use blockchain-based call encryption to prevent foreign intelligence agencies from intercepting official calls.
- Deploy honeypot techniques to detect and track cyber espionage attempts.

3. Policy, Governance & Legal Framework

3.1 Strengthen Cybersecurity Laws & Training for Government Officials

- Mandate cybersecurity training for all government, military, and foreign office employees to prevent phishing attacks and social engineering scams.
- Pass strict laws banning unauthorized usage of personal email, social media, and foreign apps for official communications.
- Establish a National Cyber Security Council to audit and enforce strict security policies in all government ministries.

3.2 National Cybersecurity Framework & Policy Update

- Develop a National Cybersecurity Strategy 2025 with AI-driven security measures, integrating policies for Starlink internet, e-commerce, and digital finance.
- Strengthen the Prevention of Electronic Crimes Act (PECA) to cover AI-based cybercrimes, deepfake regulations, and crypto-related frauds.

3.3 Strengthening National CERT (Computer Emergency Response Team)

- Expand Pakistan's CERT capacity with AI-driven cybersecurity incident response and global cooperation for cyber threat mitigation.
- Conduct cyber drills and simulations with private and government institutions to enhance cyber resilience.

4. AI & Emerging Technology Security

4.1 AI-Powered Threat Intelligence & Early Warning System

- Deploy AI-based Cyber Threat Intelligence (CTI) systems to detect phishing, hacking attempts, and financial frauds in real-time.
- Establish a Cybersecurity Operations Center (CSOC) for real-time national monitoring of cyber threats.

4.2 Protection Against Deepfake & AI-Generated Cyber Threats

- Introduce deepfake detection systems in media platforms, government websites, and financial institutions to prevent misinformation and fraud.
- Criminalize AI-generated identity theft, impersonation fraud, and social engineering scams.

5. Financial & Digital Economy Security

5.1 Secure E-Commerce & Digital Payment Systems

- Implement AI-based fraud detection systems in e-commerce platforms and payment gateways.
- Enforce Two-Factor Authentication (2FA) and biometric verification for all online payments and banking transactions.

5.2 Blockchain Regulation & Secure Crypto Transactions

- Develop legal and regulatory frameworks for cryptocurrency transactions, ensuring compliance with FATF guidelines.
- Introduce Pakistan Digital Currency (PDC) based on blockchain for secure and traceable digital transactions.

5.3 Advanced Cybersecurity for Banking & Financial Sector

- Strengthen the State Bank of Pakistan's (SBP) cybersecurity regulations to combat AI-driven frauds and digital heists.
- Implement Centralized AI-based Transaction Monitoring Systems (TMS) to detect suspicious banking transactions and prevent fraud.

6. Public Awareness, Training & International Cooperation

6.1 Digital ID Protection & Call Center Fraud Prevention

- Mandate AI-based voice authentication and biometric verification for financial transactions to prevent call center fraud.
- Introduce the National Digital Identity Protection Act to secure user data from misuse in fraudulent activities.

6.2 Cybersecurity Education & Workforce Development

- Introduce AI and Cybersecurity courses at university and vocational levels to develop a skilled cybersecurity workforce.
- Establish Cybersecurity Research & Innovation Centers to develop indigenous AI-driven security solutions.

6.3 Cross-Border Cybercrime & Global Cooperation

- Strengthen cybercrime cooperation agreements with Interpol, China, Turkey, and GCC countries for tracking cross-border financial frauds.
- Establish an AI-driven global cybercrime monitoring system with real-time intelligence sharing.

6.4 Public Awareness & Digital Hygiene Initiatives

- Launch a National Cybersecurity Awareness Program focusing on AI frauds, e-commerce security, and online financial literacy.
- Introduce Cyber Hygiene Certification for businesses and individuals to promote secure digital practices.

7. Strengthening National & Military Cyber Defense

7.1 Strengthening Government & Military Cyber Defense

- Develop AI-based cyber defense systems to counter cyber espionage, state-sponsored hacking, and Starlink-related vulnerabilities.
- Establish a Cyber Defense Unit within Pakistan Army & ISI for cyber warfare preparedness.

7.2 AI-Driven Website Security & Hacking Prevention

- Enforce mandatory website security standards for government and private sector websites to prevent cyberattacks.
- Develop AI-based website security firewalls and auto-detection of hacking attempts to prevent data leaks.

Conclusion

A multi-faceted cybersecurity strategy is essential for safeguarding Pakistan's government, military, and foreign offices from cyber threats. By implementing these recommendations, Pakistan can enhance its national cybersecurity posture, protect sensitive communications, and mitigate risks associated with emerging cyber threats. Continued collaboration, AI integration, and legal enforcement will be key to ensuring long-term cyber resilience. The success of Pakistan’s National Cybersecurity Policy hinges on implementing these recommendations with a coordinated effort from all stakeholders. Strengthening legal frameworks, protecting critical infrastructure, and empowering the workforce are key to ensuring national resilience in the digital era. Effective international cooperation and public awareness will further bolster Pakistan's security posture, making it a global player in cybersecurity governance.

Introduction to Cybersecurity

Cybersecurity, in todays interconnected and digitized world, has become an indispensable pillar of our digital infrastructure. It encompasses a vast array of practices, technologies, and measures designed to protect computer systems, networks, and data from a multitude of threats and vulnerabilities. These threats range from malicious hackers seeking to breach sensitive information to malware and viruses that can disrupt operations and compromise data integrity. As our reliance on technology continues to grow, so does the importance of cybersecurity. It is not only a matter of safeguarding sensitive information but also ensuring the resilience and functionality of critical systems that underpin modern society. This introduction sets the stage for a deeper exploration of the multifaceted world of cybersecurity, where the constant battle between defenders and attackers shapes the digital landscape.

Types of Cybersecurity Attacks

1. **Phishing Attacks** Phishing attacks involve the use of deceptive emails or messages to trick individuals into revealing sensitive information, such as login credentials or financial data. These messages often appear legitimate and may contain links to fraudulent websites or attachments with malware.
2. **Ransomware** is a type of malware that encrypts a victim's data, rendering it inaccessible. Attackers then demand a ransom for the decryption key. Paying the ransom is risky, and prevention and data backups are essential defenses.
3. **DDoS Attacks (Distributed Denial of Service)** DDoS attacks overload a target server or network with an overwhelming volume of traffic, rendering it inaccessible to legitimate users. Attackers use botnets or compromised devices to orchestrate these attacks, causing disruption and financial loss.
4. **Man-in-the-Middle (MitM) Attacks** in MitM attacks, a cybercriminal intercepts communication between two parties, often without their knowledge. This allows the attacker to eavesdrop on sensitive information or modify data being transmitted, compromising confidentiality and integrity.
5. **SQL Injection** SQL injection is a method used to exploit vulnerabilities in poorly-coded web applications. Attackers inject malicious SQL queries into input fields, enabling them to access, modify, or delete data in a database. This can lead to data breaches and other security issues.
6. **Malware** short for malicious software, encompasses a variety of software designed to harm or gain unauthorized access to a computer or network. Types of malware include viruses, Trojans, worms, and spyware, each with distinct methods and purposes.
7. **Zero-Day Exploits** exploits target vulnerabilities in software that are unknown to the software developer or vendor. Cybercriminals can exploit these vulnerabilities before a patch or fix is available, making them particularly dangerous.
8. **Social Engineering Attacks** on psychological manipulation to deceive individuals into divulging confidential information or performing actions that compromise security. Examples include pretexting, baiting, and tailgating.
9. **Insider Threats** involve individuals within an organization who misuse their access and privileges to compromise security. This may be accidental, such as negligence, or intentional, where an employee acts maliciously.
10. **IoT (Internet of Things) Vulnerabilities** As IoT devices become more prevalent, they

introduce new attack surfaces. Cybercriminals can exploit insecure IoT devices to gain access to networks or use them in botnets for other malicious activities.

Situational Analysis

The background of cybersecurity policy and rules in Pakistan is marked by a growing recognition of the importance of addressing cyber threats and ensuring digital security. Pakistan began developing its cybersecurity framework in the early 2000s, with the establishment of organizations like the Pakistan Computer Emergency Response Team (PakCERT) and the National Response Center for Cyber Crimes (NR3C) to handle cyber incidents and build capacity in this field. A significant milestone came with the enactment of the Prevention of Electronic Crimes Ordinance 2007, which later evolved into the Prevention of Electronic Crimes Act (PECA) 2016. This legislation provided a legal basis for addressing cybercrimes, protecting digital rights, and regulating online behavior. Subsequently, the government initiated efforts to improve the legal and regulatory framework to meet the evolving challenges of the digital age. While these initiatives have laid the foundation for cybersecurity in Pakistan, the country faces ongoing challenges in terms of protecting critical infrastructure, promoting international cooperation, and balancing security with individual rights and privacy, underscoring the need for continuous development in this crucial field.

One of the notable strengths in Pakistan's cybersecurity landscape is the existence of a comprehensive legal framework, which includes the Prevention of Electronic Crimes Act (PECA) 2016. This legal foundation provides a framework for addressing various cybercrimes and protecting digital rights. The government has also proactively established organizations such as the Pakistan Computer Emergency Response Team (PakCERT) and the National Response Center for Cyber Crimes (NR3C) to effectively address and respond to cyber threats. Moreover, there is a growing awareness of cybersecurity issues among the general public and organizations in Pakistan, with ongoing efforts to educate individuals and institutions about the risks and best practices in the digital realm. These strengths provide a solid basis for Pakistan to continue improving its cybersecurity capabilities and resilience in the face of evolving cyber threats.

One of the notable weaknesses in Pakistan's cybersecurity landscape is the evolving and dynamic nature of cyber threats. Pakistan faces a diverse range of cybersecurity challenges, including ransomware attacks, data breaches, and state-sponsored cyber-espionage. The fast-paced evolution of these threats necessitates continuous adaptation of cybersecurity strategies and capabilities to effectively mitigate these risks. Additionally, there is a shortage of adequately trained cybersecurity experts and state-of-the-art technology, which hinders the country's ability to respond comprehensively to cyber threats. Regulatory concerns also pose challenges, with fears of potential misuse of the legal framework, particularly with regards to stifling freedom of expression and dissent. Achieving a balance between strengthening cybersecurity measures and protecting individual rights and privacy remains a challenge. Addressing these weaknesses is crucial for Pakistan to enhance its overall cybersecurity posture and effectively safeguard its digital infrastructure and data.

Research Methodology

Qualitative data is used for analysis. The data collection was mainly done through secondary sources news articles, reports, research papers and policy paper available on internet. SWOT, GAP & Stakeholders Analysis are applied

Perform a critical analysis and evaluation of existing policies and policy documents

The National Cyber Security Policy 2021 of Pakistan appears to be a comprehensive and

forward-looking framework aimed at addressing the growing cybersecurity challenges faced by the country. The document covers a wide range of areas from cyber governance, cyber infrastructure protection, cybercrime response mechanisms, capacity-building, awareness, regulations, global cooperation, and more, addressing various stakeholders and relevant government and non-government institutions.

The document outlines a clear vision, scope, and objectives for the implementation of a comprehensive cybersecurity policy, recognizing cybersecurity as a critical national asset that needs synchronized management and regulation. The policy objectives and principles appear to be both pragmatic and ambitious, aiming to establish a secure and robust cyberspace ensuring accountable confidentiality, integrity, and availability of digital assets leading to socio-economic development and national security.

However, the real challenge for the National Cyber Security Policy 2021 will be its implementation, as it requires significant investments in resources, technology, and capacity building. It is also unclear how it will be enforced and how compliance will be monitored and evaluated, particularly for non-government actors. Also, the document lacks specifics in some areas, requiring further elaboration or supplemental policies.

Nevertheless, the National Cyber Security Policy 2021 is a step in the right direction, reflecting the current state of cybersecurity in the country, and outlining a compelling vision of a secure and resilient cyberspace. It will be interesting to monitor the implementation of the policy and its effectiveness over the coming years.

Critical analysis of existing implementation strategies

The National Cybersecurity Policy 2021 document provides a framework for cyber governance, outlines the vision, scope, objectives, principles, and deliverables to achieve the desired outcomes of the policy.

However, the document is lacking in clear and concrete implementation strategies. While it describes the need for a "Central Entity" at the federal level and various sectorial and organizational entities at the national level, there is no clear guidance on how these entities will work together to implement the policy.

Additionally, the document outlines the need for "capacity building," "awareness," and "cooperation and collaborations," but does not provide specific strategies for achieving these goals. The document also does not address financial resources or funding mechanisms for implementation.

Moreover, the interim measures outlined in the document consist of utilizing existing state organizations and institutions to support the implementation of the policy. While this may be necessary in the short term, it does not provide a clear or comprehensive implementation strategy.

In summary, while the National Cybersecurity Policy 2021 document outlines important goals, objectives, and principles, it is vague and lacks clear implementation strategies for achieving these goals. (CyberSecurityPolicy, 2021, p. 15)

Stakeholders' involvement, impact, and engagement in policy design, implementation planning and on-ground execution

The National Cybersecurity Policy 2021 is largely focused on the government's role and responsibility in Cybersecurity. The document recognizes the need for collaboration between stakeholders, including private sector organizations, academic institutions, and civil society. However, there is limited information on the extent of stakeholder involvement in policy design, implementation planning, and on-ground execution.

In terms of policy design, the document does not provide any information on whether stakeholders were consulted during the development process. Such stakeholders may have had played a critical role in informing the policy's vision, scope, and objectives based on their unique Cybersecurity challenges and priorities. (CyberSecurityPolicy, 2021, p. 5)

Regarding implementation planning, the document acknowledges the need for public-private partnerships (PPP) to promote Cybersecurity. It also highlights the need to nurture an environment for entrepreneurship based on cooperation among government, industry, academia, and research institutions in various areas to support PPPs. (CyberSecurityPolicy, 2021, p. 13) The National Centre for Cybersecurity; which has been charged with the responsibility of research to fill the gaps, was established long before the formulation of cybersecurity policy however, little progress has been made. However, the document does not provide concrete strategies for engaging stakeholders, including the extent of their participation in implementation planning, phases, and timelines.

On-ground execution is not well elaborated. The Policy suggests that central authority will be established which will be an umbrella institution for regulating, enhancing, coordinating and implementing key policy measures. Moreover, institutional structures for implementation are to be established by the Cyber Governance Policy Committee (CGPC). The Cyber Governance Policy Committee (CGPC) is responsible for guiding and recommending the National Cybersecurity Policy and Cybersecurity Act, addressing organizational, technical, and legal requirements, harmonizing departmental reporting mechanisms, conducting regular consultations on cyber governance, assigning international collaboration roles, and ensuring policy alignment with evolving cyberspace needs. The Policy recommendations from CGPC are approved by the Federal Cabinet. (CyberSecurityPolicy, 2021, p. 5) However, the progress on the Cybersecurity Policy is at snail's pace. Additionally, there is no mention of the extent to which stakeholders will participate in these structures or have access to the information required to implement the policy effectively.

In summary, while the National Cybersecurity Policy 2021 recognizes the need for stakeholder engagement, involvement, and impact, it lacks clear guidelines on integrating stakeholders' concerns into the policy's design, implementation planning, and on-ground execution.

Institutional frameworks for implementation

The National Cybersecurity Policy 2021 acknowledges the need for institutional structures for effective implementation of the policy. These structures include the Cyber Governance Policy Committee (CGPC), a designated organization / division of the federal government and sectoral regulators/CERTs (including but not limited to Defense, Telecom, Banking and finance, Power, Federal and Provincial public & Private sectors) working together to ensure the overall national Cybersecurity coordination. The establishment of National CERT after lapse of two years of the policy substantiates the lack of will / lack of sensitivity and slow progress on part of the Govt. The Financial sector through State Bank of Pakistan as well as PTA have somewhat proceeded towards the establishment of respective CERTs however, the idea has still not been implemented. The State Bank of Pakistan has issued clear directions to the Financial Institutions for outsourcing Cybersecurity which clearly shows the lack of capacity on part of the Financial Institutions.

Moreover, the effectiveness of these institutional frameworks in achieving the policy's objectives. Here are some factors that may contribute to effective institutional frameworks

a) Transparency

Institutional frameworks need to be transparent. Relevant stakeholders should be informed of the institutional frameworks, their composition, roles, and responsibilities. This will help establish trust and accountability between stakeholders and institutions.

b) Capacity

The designated organizations of the federal government must have sufficient capacity, capability and resources to handle its responsibilities related to the policy's implementation. This includes recruiting qualified personnel and acquiring appropriate technology and infrastructure.

c) Coordination

Institutions need to work in coordination to ensure effective implementation of the policy. Coordination is especially critical among sectoral regulators/CERTs, which are responsible for ensuring Cybersecurity in their respective areas.

d) Monitoring and Evaluation

Institutional frameworks need to be monitored and evaluated regularly to assess their effectiveness. The results of monitoring and evaluation will help identify strengths and weaknesses of the frameworks and design appropriate measures for improvement.

Overall, it is not clear how these institutional frameworks will be implemented. Thus, it is difficult to critically evaluate the performance of these institutional frameworks in achieving the policy's objectives.

SWOT Analysis of each institution and stakeholder

a) NADRA (National Database and Registration Authority)

Strengths	**Weaknesses**
• Massive Database NADRA has a comprehensive database of citizens, making it a valuable resource for various government departments. • Identification Expertise It's well-versed in identity verification and biometrics including fingerprint searching. • Technological Infrastructure NADRA has invested in modern technology for efficient data management which is state of the art.	• Privacy Concerns handling vast personal data raises concerns about privacy and data security. • Operational Challenges Serving a large population can lead to logistical challenges and delays. • Dependence on Government Funding Reliance on government funding may impact its autonomy.
Opportunities	**Threats**
• Digital Services Can expand into providing digital identity verification services. • International Collaboration Collaborate with other countries on secure identity management.	1. Data Breaches Constant threat of cyberattacks and data breaches. 2. Policy Changes Changing government policies can impact its operations

b) FBR (Federal Board of Revenue)

Strengths	Weaknesses
• Revenue Collection FBR plays a vital role in collecting government revenue. • Authority It has legal authority for tax collection and enforcement. • Skilled Workforce Employs professionals with financial expertise.	• Tax Evasion Struggles with tax evasion and non-compliance issues. • Complex Tax Laws Pakistan's tax laws can be intricate, making it challenging for both taxpayers and FBR.
Opportunities	**Threats**
• Digital Transformation Can improve tax collection through digital tools and automation. • Streamlined Processes Simplify tax filing and payment processes for taxpayers.	• Economic Downturn Economic instability can affect revenue collection. • Corruption Internal corruption can undermine its effectiveness.

c) FIA (Federal Investigation Agency)

Strengths	Weaknesses
• Law Enforcement FIA has legal authority for investigating cybercrime, human trafficking, and other federal offenses. • Specialized Units It has specialized units for dealing with cybercrime and immigration	• Resource Constraints May face resource constraints for handling complex investigations. • Bureaucratic Hurdles Bureaucratic obstacles can slow down investigations
Opportunities	**Threats**
• Enhanced Cybercrime Capabilities Can further develop capabilities to combat cybercrime. • International Collaboration Collaborate with other law enforcement agencies globally.	• Evolving Cyber Threats Rapidly evolving cyber threats pose a constant challenge. • Corruption Internal corruption can undermine its integrity and effectiveness.

d) Military and Defense (SWOT analysis of Pakistan Army's Cyber Command in regard to Cybersecurity)

Strengths	Weaknesses
• Establishment of Cyber Division and Army Centre of Emerging Technologies • Leadership attention – COAS General Qamar Javed Bajwa has visited Cyber Division and Army Centre of Emerging Technologies • Pakistan Air Force and Navy have also established cyber commands • Establishment of Pakistan's first ever National Cybersecurity Academy	• Lesser focus as a result of war on terror engagements across the country. • Defense assets of the armed forces are prone to Cyber-attacks due to non-enforcement of Cyber Policies in civilian and financial institutions. • The circuits / chips (procured from abroad) used in weapons / targeting / radar systems make the defense apparatus prone to Cyber-attacks.

• Evolving technology has revolutionized war strategies and opened a new domain for militaries called Cyber Warfare • As Pakistan Air force is already leading electronic warfare in South Asia • Pakistan Armed forces have always insured balance of power in the region.	
Opportunities • The newly raised Cyber Command shall progressively be linked to Tri-Services level and will also form part of national cyber initiatives to have synergy at national level • Need to enhance capability and capacity in cyber domains	**Threats** • Every government or non-government institution faces cyber threats today including Pakistan Armed Forces as we have a technological superior enemy at our borders. • Threats from state actors as well as non-state actors • New ways of committing cyber-attacks are emerging with each passing year • Cyber Warfare is usually defined as a cyber-attack or series of attacks that target a country's governmental/nongovernmental institutions, cause widespread destruction on civilian and government infrastructure and can even paralyze a whole state. (Hassan, p. 2023)

e) Financial Sector as a stakeholder

Strengths	**Weaknesses**
• The State Bank of Pakistan has established a comprehensive regulatory and supervisory framework to mitigate cybersecurity risks faced by financial institutions. • SBP's regulatory regime is based on the US National Institute of Standards and Technology's (NIST) Cybersecurity Framework and the Bank for International Settlements' (BIS) Guidance on cyber resilience for financial market infrastructure. • SBP's regulatory framework includes a set of control requirements in its internal IT Security Policies and Risk Management Framework and performs major risk assessments of IT business and support systems.	• The increasing perceived cybersecurity risks by participants in Pakistan. - Risks associated with outsourcing arrangements increase financial institutions' dependence on third-party service providers and their risk profile.
Opportunities	**Threats**
• Financial institutions can put strong internal controls in place to effectively identify, assess, and manage cybersecurity risks. • There is a need for continuous enhancement of regulatory and supervisory frameworks to counter the emerging and evolving risks from digital finance arrangements	• Cyber-attacks such as ransomware, phishing, data leakage, denial of service, malware propagation, or cyber extortion. • Large scale cyber-attacks on state institutions and banks in Pakistan. - Cyber risks have surpassed health risks as the top ranked threat to growth for financial institutions' CEOs. • The increasing use of outsourcing arrangements for non-core functions and business support functions by financial institutions increases their dependence on third-party service providers and consequently their risk profile.

f) Federal Government as a stakeholder

Strengths	Weaknesses
• The federal government has the authority to design, develop, approve, and implement Cybersecurity policies across government sectors and public databases. It also has the ability to establish institutional frameworks and coordinate among stakeholders to facilitate implementation of the policy.	• The federal government may lack the technical expertise and capacity in some areas of Cybersecurity
Opportunities	**Threats**
• The policy provides an opportunity for the federal government to strengthen its institutional frameworks, collaborate with sectoral regulators and other stakeholders for effective policy implementation and invest in capacity building programs for its officials to improve their skills and knowledge in Cybersecurity.	• The threats faced by the federal government as a stakeholder include the vulnerability of the government's digital assets, the increasing sophistication of cyber-attacks, and the rapidly evolving nature of cyber threats.

g) Sectoral Regulators / CERTs as stakeholders

Strengths	Weaknesses
• The sectoral Regulators/CERTs have the technical expertise and specialization to monitor and ensure Cybersecurity in their respective areas of control. • The sectoral CERTs also provide its stakeholders with a coordinated emergency response mechanism in the event of a cyberattacks.	• The lack of central coordination and collaboration among the sectoral CERTs with the designated organization of the Federal Government may hinder effective implementation of the policy. • They may also face resource constraints which may affect their ability to perform their duties effectively
Opportunities	**Threats**
• The sectoral CERTs can collaborate with the designated organization of the federal government to improve their institutional frameworks, develop Cybersecurity standards, and guidelines for their respective industries. • They can also invest in capacity building and training programs to enhance their skillset and develop Cybersecurity solutions tailored to their specific sectors.	• The threats faced by sectoral regulators/CERTs include the evolving nature of Cyber threats, the dynamic nature of their industries, and the lack of resources required to tightly secure the nation's assets.

h) Cyber Governance Policy Committee (CGPC)

Strengths	Weaknesses
• The CGPC can provide effective coordination among different institutions and stakeholders for policy implementation. It also has the mandate to establish regulations, guidelines, and a framework for Cybersecurity monitoring and assessment to ensure compliance with the policy.	• The CGPC may face resource constraints and lack of technical expertise in some areas of Cybersecurity. It may also face external pressure from various industry stakeholders to water-down the policy or weaken its regulation on Cybersecurity.
Opportunities	**Threats**

• The CGPC has an opportunity to collaborate with stakeholders and sectoral regulators / CERTs to develop robust institutional frameworks to ensure effective policy implementation. It can work with industry stakeholders to secure funding and technical expertise to enhance its capacity and capability to monitor and assess Cybersecurity.	• Threats faced by CGPC include resource constraints, conflicting stakeholder interests, and external pressure that may weaken its authority and ability to enforce Cybersecurity regulations and frameworks.

i) Private sector stakeholders

Strengths	Weaknesses
• Private sector stakeholders in Pakistan have a large role to play in Cybersecurity as they control a large segment of the country's ICT infrastructure. They can leverage their resources and expertise to contribute to Cybersecurity policy implementation.	• Private sector stakeholders may not view Cybersecurity as a priority, which may lead to weak policies, inadequate resources, and unwillingness to invest in Cybersecurity adequately.
Opportunities	**Threats**
• Private sector stakeholders can collaborate with the Federal Government and the sectoral regulators/CERTs to ensure effective Cybersecurity policy implementation. They can allocate adequate resources, including personnel, tools, and technologies to enhance Cybersecurity. They can also invest in capacity building programs for their employees to develop their skillsets and knowledge of Cybersecurity.	• The threats faced by the private sector stakeholders include the increasing sophistication of cyberattacks, the lack of incentives to invest in Cybersecurity, and reputational damage in case of a cyberattack stock price slumps or loss of customer trust.

j) Individual stakeholders

Strengths	Weaknesses
• In the absence of individual Cybersecurity ensuring cybersecurity through their use of technology. experts, individual stakeholders play a critical role in	• Lack of awareness (especially in rural areas) may lead them to unknowingly engage in insecure online behavior, which poses a risk to national Cybersecurity.
Opportunities	**Threats**
• National Cybersecurity Policy 2021 provides an opportunity for individuals to engage in a culture of Cybersecurity and become aware of threats and the best practices to safeguard themselves online from cyber threats.	• The threats faced by individual stakeholders include the lack of awareness, lack of stringent implementing regulations infringements on the right to privacy, and weak infrastructure may serve as easy targets for cyber criminals.

k) Academia and Research Institutions

Strengths	Weaknesses

• Academia and research institutions possess a wealth of knowledge, and research in Cybersecurity and can provide the necessary expertise for the successful implementation of Cybersecurity Policy 2021.	• Constraints in funding and resources may hinder research and development in Cybersecurity.
Opportunities • Cybersecurity Policy 2021 provides an opportunity for academia and institutions to collaborate with stakeholders to develop Cybersecurity solutions and systems, conduct research in critical areas of Cybersecurity, and produce a pool of qualified professionals equipped with the necessary skills to combat cyber threats.	**Threats** • The threats faced by academia and research institutions include resource constraints and the potential for cybercriminals to target them due to the importance of their research for policy makers to make informed policy decisions concerning Cybersecurity.

Legal framework in Pakistan

a) The Pakistan Telecommunication Reorganization Act 1996

This Act was the first initiative to recognize and regulate the digital services in Pakistan. It provides for the reorganization of the telecommunication system in Pakistan by establishing the Pakistan Telecommunication Authority. The act also covers various aspects of licensing, regulation, oversight, and enforcement of telecommunication services in Pakistan. The section 31of this act defines various offences and penalties related to telecommunication services, such as Unauthorized operation or use of telecommunication systems or services, damage or interference with telecommunication systems or services, theft or dishonest use of telecommunication systems or services.

b) Pakistan Telecommunication Reorganization Act 1996

The Pakistan Telecommunication Reorganization Act of 1996 was a pivotal piece of legislation that transformed the telecommunications landscape in Pakistan. This act marked the beginning of a significant shift from a state-owned telecommunications monopoly to a more competitive and open market. It led to the establishment of the Pakistan Telecommunication Company Limited (PTCL) as a public limited company, paving the way for private sector participation in the telecom sector. The Act aimed to encourage investment, enhance service quality, and expand the telecommunications infrastructure throughout the country. It played a crucial role in modernizing Pakistan's telecom industry and ushered in an era of increased connectivity and access to telecommunication services for the country's growing population

c) Electronic Transaction Act 2002

The Electronic Transactions Act of 2002, enacted in Pakistan, was a groundbreaking piece of legislation that recognized the significance of electronic commerce in the modern world. This Act provided a legal framework for electronic transactions, digital signatures, and electronic data exchanges, offering legitimacy and security to online interactions. It facilitated the growth of e-commerce and digital communication by giving electronic records the same legal status as traditional paper documents. By providing legal certainty and security for electronic transactions, the Act played a pivotal role in promoting the digital economy, online business, and e-government initiatives in Pakistan. It served as a vital stepping stone in the country's journey towards digital transformation and the promotion of a more efficient and accessible electronic environment for both businesses and individuals

d) Prevention of Electronic Crimes Ordinance 2008

The Prevention of Electronic Crimes Ordinance of 2008, also known as the Cybercrime Ordinance, was a significant legal development in Pakistan aimed at addressing the challenges posed by the rapid growth of information technology and the internet. This ordinance sought to combat electronic crimes, such as cyberbullying, hacking, data breaches, and online harassment, by providing a legal framework for the investigation and prosecution of such offenses. It aimed to protect the integrity of digital data and networks and safeguard the rights and privacy of individuals in the digital sphere. The ordinance was designed to strike a balance between security and individual liberties, but it also faced criticism for its potential misuse against freedom of expression. In subsequent years, it went through amendments to address some of these concerns and adapt to the evolving landscape of electronic crimes in the digital age.

e) Prevention of Electronic Crime Act 2016

The Prevention of Electronic Crimes Act of 2016, commonly referred to as PECA, is a landmark legislation in Pakistan's legal framework designed to combat the rising threats of cybercrimes and online misconduct. This comprehensive act addresses a wide range of

electronic crimes, including cyberbullying, online harassment, hacking, and the dissemination of hate speech and offensive content. It grants law enforcement authorities the necessary tools and provisions to investigate and prosecute these offenses, while also defining punishments for those found guilty. While PECA serves as a crucial instrument to protect digital privacy and cybersecurity, it has also faced criticism for potential misuse, raising concerns about the balance between security and individual freedoms. Nevertheless, this act is instrumental in shaping the country's approach to tackling electronic crimes and ensuring a safer online environment for its citizens.

f) National Cybersecurity Policy 2021

The National Cyber Security Policy 2021 is a holistic framework designed to secure Pakistan's entire cyberspace. The policy aims to ensure a secure, robust, and continually improving nationwide digital ecosystem that guarantees accountable confidentiality, integrity, and availability of digital assets leading to socio-economic development and national security (Page 6). The policy provides a comprehensive mandate for cyber governance and security at the national level by establishing a Cyber Governance Policy Committee (CGPC) to formulate and guide the implementation of a National Cyber Security Policy and Cyber Security Act (Pages 9, 11, and 12). The policy framework also emphasizes capacity building initiatives, active defense, public-private partnerships, cybercrime response mechanisms, and regulations to achieve its objectives (Pages 9-18). The policy will be reviewed after every three years to align with emerging cyberspace requirements (Page 19). Overall, the National Cyber Security Policy 2021 provides a solid foundation for the construction of a secure digital ecosystem in Pakistan.

g) Computer Emergency Response Team (CERT) Rules 2023

CERT Rules – 2023 provides a legislative umbrella to handle ever-emerging cyber-security risks and vulnerabilities at the national, sectoral, and organizational levels by laying out a working mechanism in the form of technical support, operational facilities, and capacity-building services. (Amin, 2023)

Technological challenges related to implementation

The National Cybersecurity Policy 2021 (CyberSecurityPolicy, 2021, pp. 2-22) acknowledges the challenges that technology presents to the implementation of the policy. Here are some technological challenges that could affect the policy's implementation

a) Technology obsolescence

Technology becomes outdated quickly, making it difficult to keep up with the latest security measures. This can result in vulnerabilities that can be exploited by attackers.

b) Complexity

With technological advancements, systems are becoming more complex, and managing and securing them is becoming more challenging. This increases the likelihood of vulnerabilities that can be exploited.

c) Heterogeneity

Systems Software, and networks are becoming more heterogeneous, with different types of devices and protocols interacting with each other. This creates compatibility challenges and could increase the likelihood of system vulnerabilities.

d) Cyber threats

Cyber threats are becoming more sophisticated and diverse, making it difficult to keep security measures up-to-date. Attackers use advanced techniques such as AI, machine learning, and social engineering to breach systems.

e) Lack of skilled professionals

There's an increasing shortage of skilled Cybersecurity professionals in the field. This limits the capacity for institutions and organizations to detect and prevent Cybersecurity attacks.

To address these challenges, the policy provides a framework for Cybersecurity Governance and Strategy, which is essential in managing the risks associated with technology in order to achieve the objectives of the policy. The policy also emphasizes the need for capacity building and public-private partnerships to address critical challenges related to the technological aspect.

Overall, while the policy recognizes the challenges that technology presents to its implementation, there is a need to strengthen the policy's implementation mechanisms in light of the rapidly evolving Cyber landscape.

Administrative and human resources issues pertaining to implementation

The National Cybersecurity Policy 2021 recognizes the importance of administrative and human resources factors in implementing the policy objectives. Here are some administrative and human resource-related issues that could impact policy implementation

a) Lack of coordination among stakeholders

Cybersecurity is a cross-sectoral issue that requires the involvement of various stakeholders. Silos and a lack of coordination among stakeholders can impede implementation of the policy objectives.

b) Absence of centralized policy

The absence of a centralized policy and strategy for Cybersecurity can make securing the digital assets of the country random and uncoordinated.

c) Limited resources

Building and maintaining Cybersecurity capabilities requires expertise, technology, and financial resources. Given the competing demands for resources, there needs to be a well-planned allocation of resources to support policy implementation.

d) Training and Capacity building

Strengthening capacity and capabilities of Cybersecurity professionals can help support policy implementation. However, there is a dearth of trained professionals in this field.

e) Government Accountability

There needs to be accountability and transparency in the implementation of the policy objectives. Failure to do so could lead to bureaucratic hurdles or a lack of public trust in the policy.

Technological challenges in Implementation of Cybersecurity Policy

The implementation of Cybersecurity Policy poses challenges on the technological front as well. The National Cybersecurity Policy 2021 has identified some technological challenges, which could impede the implementation of Cybersecurity Policy. These include

a) Legacy Systems

Legacy systems pose a challenge to the implementation of Cybersecurity Policy objectives as they may be difficult to secure and maintain.

b) Low Technology Awareness

The relatively low level of technological awareness among the general public is a concern, as it may result in people falling prey to phishing or other cybercrime schemes.

c) Scarcity of Local Cybersecurity Solutions

Pakistan is mainly relying on imported hardware, software, and services. Cybersecurity Policies are not addressed even in the procurement process, and the IT supply chain of local manufacturers and service providers also exposes Pakistan's digital assets to various types of threats.

d) Cyber Attacks

Cyber Attacks from foreign countries or agents can target National Critical Information Infrastructure, IoT devices and computer systems, leading to a potential breakdown in infrastructural services.

e) Technological Obsolescence

Due to the rapid pace of technological progress and advancements in Cyber-Security attacks, new solutions will always be needed, and the obsolescence of previous ones will be almost inevitable. The speed with which these technological updates are made can either increase or decrease the threat. This gap in the techno-skills and obsolescence can impede the implementation of the policy objectives.

Economic and Financial Analysis

Unfortunately, the National Cybersecurity Policy 2021 (CyberSecurityPolicy, 2021, pp. 2-22) only briefly touches upon the financial and economic aspects of Cybersecurity. However, the policy does recognize that Cybersecurity vulnerabilities present significant financial risks to all sectors of the economy. The policy also notes that the rise in incidents related to malicious use of ICTs has impacted the integrity, transparency, and socio-economic equilibrium of the country. Cybersecurity represents one of the fundamental pillars of knowledge-based economies and the protection of our Cyber networks is vital in maintaining economic growth. Cybersecurity is especially important for the financial sector where Cybersecurity breaches can threaten the stability of the country's financial system. A successful policy will ensure the stability of businesses and individuals in the digital economy. At the same time, the policy highlights the need for coordination and public-private partnerships for the effective implementation of the policy. Therefore, while the policy recognizes the key role of the economy and finance in the discussion of Cybersecurity, it does not provide a detailed economic or financial analysis of the issue.

a) Costs of Cybersecurity

The costs of cybersecurity are multifaceted and extend beyond the financial aspects. While there are significant expenses associated with implementing and maintaining robust cybersecurity measures, such as investing in security software, hardware, and expert personnel, the consequences of neglecting cybersecurity can be far costlier. Cyberattacks can result in financial losses due to data breaches, downtime, and legal repercussions. However, the non-financial costs are equally important, including damage to a company's reputation, loss of customer trust, and potential legal liabilities. Furthermore, there are hidden costs, such as the time and resources required to recover from a cyber-incident, as well as the long-term impact on a business's competitiveness. In the realm of national cybersecurity, the costs can extend to threats against critical infrastructure, economic stability, and national security. Therefore, investing in cybersecurity is essential not only to protect against immediate financial losses but also to safeguard reputation, trust, and long-term sustainability.

b) Benefits of Cybersecurity

The benefits of cybersecurity are extensive and touch upon various aspects of individual, organizational, and national well-being. At the individual level, cybersecurity safeguards personal information and privacy, protecting people from identity theft and fraud. For organizations, it fosters trust and reliability, enhancing their reputation and ensuring the

continuity of operations. Effective cybersecurity measures reduce the risk of data breaches, financial losses, and disruption of services, resulting in cost savings and improved business resilience. In a broader context, strong cybersecurity is essential for national security and the protection of critical infrastructure, preventing potentially devastating cyberattacks. Moreover, it supports innovation and the growth of the digital economy by creating a secure environment for digital transactions and fostering trust in online interactions. Overall, cybersecurity is a vital investment that not only protects against immediate threats but also contributes to the long-term prosperity, safety, and stability of individuals, organizations, and nations.

c) Economic Impact

The economic impact of cybersecurity is significant and multifaceted. On one hand, robust cybersecurity measures are essential for safeguarding businesses and the broader economy. They protect against data breaches, financial losses, and business disruption, helping organizations maintain their stability and reputation. Effective cybersecurity promotes trust and confidence in digital transactions, fostering economic growth and innovation. However, inadequate cybersecurity can lead to substantial financial losses, legal liabilities, and reputational damage for businesses. On a larger scale, the economic consequences extend to national security and critical infrastructure protection. Cyberattacks against vital systems like energy, transportation, and healthcare can result in immense economic costs. As the digital economy continues to expand, the economic impact of cybersecurity becomes increasingly intertwined with overall economic stability and prosperity, highlighting the importance of investing in robust cybersecurity measures to mitigate risks and protect the economy.

In conclusion, conducting an economic and financial analysis of Cybersecurity in Pakistan involves weighing the costs against the benefits, considering the broader economic impact, and assessing factors such as ROI, budget allocation, and the growth of the Cybersecurity sector. It is essential for Pakistan to continually invest in and adapt its Cybersecurity strategy to protect its economy from the growing threat of cyberattacks.

Comparative analysis of 2 developed & 2 developing countries

a) Cybersecurity Infrastructure

India	**Pakistan**
• India has been investing in its Cybersecurity infrastructure. It has established organizations like the Indian Computer Emergency Response Team (CERT-In) and the National Cyber Coordination Centre (NCCC). • The growth of the IT industry and the presence of Cybersecurity firms contribute to the country's Cybersecurity capabilities.	• Pakistan has taken steps to improve its Cybersecurity infrastructure with the establishment of the Pakistan Computer Emergency Response Team (PakCERT). • While making progress, Pakistan's Cybersecurity infrastructure may not be as advanced as some other nations due to the size of its IT industry.
USA	**Germany**
• The United States boasts a robust Cybersecurity infrastructure. Key agencies like the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) are responsible for monitoring and responding to cyber threats. • The country is also home to numerous leading Cybersecurity firms and research institutions.	• Germany has a well-developed Cybersecurity infrastructure with organizations like the Federal Office for Information Security (BSI) overseeing Cybersecurity measures. • The country has a strong emphasis on data protection and privacy, which aligns with its Cybersecurity efforts.

b) Cyber Threat Landscape

India	Pakistan
• India faces a wide range of cyber threats, including state-sponsored cyber-espionage, hacktivism, and financially motivated cybercrime. • There have been notable instances of large-scale data breaches and ransomware attacks targeting government organizations and private companies.	• Pakistan experiences cyber threats, including hacktivism and financially motivated cybercrime. Reports of state-sponsored cyber-espionage activities have also emerged.
USA	**Germany**
• The USA is a prime target for cyber threats due to its global economic and political influence. • It deals with a broad spectrum of cyberattacks, including nation-state threats, advanced persistent threats (APTs), and cybercriminal activities.	• Germany faces a range of cyber threats, including state-sponsored attacks and cybercrime. • The country has a strong focus on protecting critical infrastructure, such as its energy and transportation sectors.

c) Cybersecurity Regulations and Policies

India	Pakistan
• India has implemented Cybersecurity regulations and policies, including the National Cybersecurity Policy (2013) and the draft Personal Data Protection Bill.	• Pakistan enacted the Pakistan Electronic Crimes Act (PECA) to combat cybercrimes. However, there have been concerns about potential misuse.
USA	**Germany**
• The USA has various Cybersecurity laws and regulations at the federal and state levels. It has initiatives like the National Institute of Standards and Technology (NIST) Cybersecurity Framework.	• Germany has strict data protection laws, and the European Union's General Data rotection Regulation (GDPR) plays a significant role in shaping its Cybersecurity and data protection policies.

d) International Cooperation

India	Pakistan
• India actively participates in international forums and collaborates with countries such as the United States and Israel on Cybersecurity initiatives.	• Pakistan engages in international cooperation on Cybersecurity, working with organizations like the United Nations and regional partners.
USA	**Germany**
• The USA plays a leading role in international Cybersecurity efforts, collaborating with allies and organizations like NATO.	• Germany is an active participant in international Cybersecurity cooperation, especially within the European Union.

e) Challenges

India	Pakistan
• India faces challenges related to the volume and diversity of cyber threats and the need to secure its critical infrastructure.	• Pakistan must further develop its Cybersecurity ecosystem and address the balance between Cybersecurity and freedom of expression.
USA	**Germany**
• The USA confronts ongoing threats from nation-states, the rapid evolution of cyber threats, and the need to secure critical infrastructure.	• Germany is focused on protecting critical infrastructure and maintaining data privacy in the face of evolving cyber threats.

f) Public Awareness

India	Pakistan
• India has been actively working on increasing public awareness of Cybersecurity issues, with initiatives for both businesses and individuals.	• Public awareness of Cybersecurity is growing in Pakistan, but there is room for improvement.
USA	**Germany**
• The USA has a relatively high level of public awareness regarding Cybersecurity, with numerous educational programs and campaigns.	• Germany places a strong emphasis on educating the public about data privacy and Cybersecurity.

Each of these countries has unique Cybersecurity challenges and strengths, and they continually adapt to the evolving threat landscape. Collaboration and information sharing on an international level are crucial in addressing Cybersecurity threats effectively.

GAP analysis on all dimensions of National Cybersecurity Policy 2021

Military and Defense

According to the National Cybersecurity Policy 2021, there is no specific section on the Military and Defence dimension of Cybersecurity. However, it explicitly states the intention to secure all digital assets of Pakistan and to coordinate and implement all Cybersecurity-related matters on the federal level.

Therefore, it can be inferred that the Military and Defense dimension is also included within the scope of the policy. However, in order to conduct a comprehensive GAP analysis, it might be necessary to further analyze existing laws and regulations as well as current practices and

capabilities of the military and defense organizations regarding Cybersecurity, and compare them to the objectives and principles of the policy.

Critical Infrastructure

The National Cybersecurity Policy 2021 recognizes the protection and resilience of Critical Information Infrastructure (CII) as a critical objective in ensuring national Cybersecurity. The policy framework envisages securing the entire cyberspace of Pakistan, including critical digital assets, data processed, managed, and transmitted over the networks. The policy identifies several measures to ensure the protection of CII, such as:

- Operate technical platforms to protect CII, Information and Communication Technologies (ICT), Next Generation Mobile Service and Networks, and IoT security.
- Institute processes for identification, prioritization, assessment, and protection of CII.
- Ensure a secure ICT environment, including mobile systems and cloud-based solutions through state-of-the-art security measures.
- Mandate implementation of national security standards by all critical Information Infrastructure to hire qualified Cybersecurity individuals and add an appointment of Chief Information Security Officer (CISO).
- However, the policy does not provide specific guidelines or recommendations for securing certain types of critical infrastructure, such as energy, water, or transportation systems, which are also commonly known as Critical National Infrastructure (CNI). Therefore, a comprehensive GAP analysis should be conducted by the relevant authorities to assess the existing Cybersecurity practices and capabilities of the critical infrastructure entities, identify potential risks and vulnerabilities, and devise tailored strategies to bridge the gaps between the existing situation and the objectives and principles of the National Cybersecurity Policy 2021

Government and Public Service

The National Cybersecurity Policy 2021 emphasizes the protection of the Government's information systems and infrastructure as well as the need for a robust authentication and data protection framework. The policy outlines specific measures to achieve this goal, such as:

- Encouraging the establishment of national Data Centers to co-locate servers and telecom Quality infrastructure for all government entities federal & provincial.
- Creating vulnerability management and patch management programs for all government technical systems.
- Working with relevant government entities to ensure the mandatory allocation of a certain percentage of the ICT project budget for Cybersecurity Assurance.
- Instituting a mechanism for the creation and enforcement of staff vetting and clearance schemes across the government.
- Providing access controls and authentication technology training for all government systems.

While these measures constitute a strong framework for protecting the government and public service dimension of national Cybersecurity, there may be gaps between what is outlined in the policy and the reality of the current Cybersecurity situation in government and public services within Pakistan. To conduct a comprehensive GAP analysis, it will be necessary to assess the implementation and compliance level of the policy in the public and government sectors, and identify areas that need improvement such as the gaps in protective personnel measures (screening, vetting, training and guidelines for conflict of interests of public officials etc.), as well as identifying the need for special regulations for some services such as e-voting and digital signature in some institutions. (CyberSecurityPolicy, 2021, pp. 11,12,15)

Economic Interest

- The National Cybersecurity Policy 2021 emphasizes the importance of protecting the economic interests of Pakistan and stresses the significance of establishing a secure, robust,

and continually improving digital ecosystem leading to socio-economic development and national security. The policy identifies several measures to ensure the protection of Pakistan's economic interests, as follows

- All entities involved in the development of critical infrastructure or technology will follow national standards for implementation, Cybersecurity protections, and quality control measures.
- Data collected through IoT devices and other technologies must be protected from cyber incidents and shared only through authorized users and in compliance with data protection protocols.
- All critical infrastructure must follow a single security standard, formulate and maintain a disaster recovery plan and impose necessary security clearance requirements.
- Developing and implementing a regulatory framework to enforce accountability and compliance in the financial sector for Cybersecurity threats and rewards.

However, to conduct a comprehensive GAP analysis, the actual implementation and compliance level of the policies must be thoroughly evaluated, and any gaps between the objectives set in the policy framework and current Cybersecurity practices must be identified. The GAP analysis must also address facilitating user trust in online systems, developing strategies to identify and respond appropriately to Cybersecurity threats, improving the enforcement of compliance and regulation in the financial sector, and promoting the use of secure transactional technologies. It must also ensure the best protection of intellectual property rights against cyber-attacks and build the capacity of institutes catering to the financial sector to keep abreast with emerging threats and security technologies.

National Security

1. The National Cybersecurity Policy 2021 stresses the critical importance of ensuring Pakistan's national security through robust Cybersecurity measures. The policy's objectives for this dimension include:

- Establishing a well-coordinated and essential mechanism that will enhance Pakistan's national Cybersecurity capabilities.
- Developing policies, strategies, and a regulatory framework focused on effective national Cybersecurity governance, implementation, and enforcement.
- Institutionalizing an active defense mechanism to identify, prevent, manage Cybersecurity-related incidents both in Pakistan and against it directly
- Encouraging public-private partnerships for ensuring Cybersecurity for the institutions designated for and critical for national security.
- Creating partnerships between Industry & Academia through R&D programs and establishing centers of excellence to develop and manufacture indigenous security applications and products.

GAP analysis of the National Security dimension of the National Cybersecurity Policy 2021 would include evaluating Pakistan's Cybersecurity capabilities, policies and strategies for national security, and regulatory frameworks for implementation and enforcement. The analysis would also need to address the following

- The level of collaboration and coordination of Cybersecurity governance among government institutions, local government entities, and stakeholders in the private sector, including financial, health, education, and telecommunication.
- The level of Cybersecurity cultural awareness and fostering of Cybersecurity training and education within the country to minimize potential vulnerabilities.
- The need to develop and integrate an effective incident management mechanism for dealing with any breaches and ensuring response and recovery procedures are in place.
- The need to maintain and manage the required level of Cybersecurity resources, including qualified human resources with training in Cybersecurity, physical resources, hardware, and software.

- The need to consistently research and develop effective Cybersecurity solutions and technologies to keep pace with evolving cyber threats, espionage and criminal activities. (CyberSecurityPolicy, 2021, pp. 2, 5-6, 8-17)

Twenty most crucial issues and challenges

Issues

1. Cyber Threat Landscape Understanding and addressing the evolving and diverse nature of cyber threats, including state-sponsored attacks, cybercrime, hacktivism, and more.
2. Critical Infrastructure Protection Ensuring the security and resilience of critical infrastructure, such as energy grids, transportation systems, and healthcare networks.
3. Data Privacy and Protection Developing policies to protect personal data and establish clear regulations for data handling, storage, and sharing.
4. Incident Response and Recovery Establishing robust procedures for responding to cyber incidents and facilitating swift recovery to minimize the impact of attacks.
5. International Cooperation Enhancing collaboration with other nations and international organizations to combat cross-border cyber threats and promote global Cybersecurity norms.
6. National Cyber Defense Strategy Outlining a comprehensive strategy for the defense of national cyberspace, including deterrence, detection, and response.
7. Cybersecurity Education and Workforce Development Promoting Cybersecurity awareness and training programs to address the shortage of skilled professionals in the field.
8. Regulatory Framework Developing and updating laws and regulations related to Cybersecurity, cybercrime, and data protection to keep pace with technological advancements.
9. Emerging Technologies Addressing the security challenges posed by emerging technologies like artificial intelligence, the Internet of Things, and 5G.
10. Resilience and Continuity Planning Ensuring that organizations and government agencies have plans in place to maintain critical functions and services during and after cyber incidents.

Challenges

1. Capacity Building and Workforce Development Building a skilled Cybersecurity workforce to address the shortage of experts and professionals in the field.
2. Critical Infrastructure Protection Ensuring the security and resilience of critical infrastructure such as energy, telecommunications, and healthcare systems.
3. Regulatory Framework Developing and implementing comprehensive Cybersecurity laws and regulations to establish a legal framework for cyberspace.
4. Data Privacy and Protection Balancing the need for data protection and privacy while addressing issues related to data breaches and unauthorized surveillance.
5. International Cooperation Collaborating with other nations and international organizations to combat cross-border cyber threats and promote global Cybersecurity norms.
6. Public Awareness Raising awareness among citizens and organizations about the importance of Cybersecurity and safe online practices.
7. Emerging Technologies addressing the security challenges posed by emerging technologies such as the Internet of Things, artificial intelligence, and 5G.
8. Incident Response and Recovery Developing and implementing procedures for responding to cyber incidents and facilitating rapid recovery.
9. Supply Chain Security Ensuring the security of the technology supply chain to prevent vulnerabilities in software and hardware used by organizations and the government.
10. National Defense and Deterrence Outlining a comprehensive strategy for the defense of national cyberspace, including measures to deter cyber threats and attacks.

Conclusions (From Policy document)

Based on the National Cybersecurity Policy 2021 document, the following three conclusions can be formulated

1	The government of Pakistan recognizes that an effective Cybersecurity policy is foundational for national security and therefore has prioritized the development and implementation of comprehensive Cybersecurity policies and standards.
2	A coordinated effort between government institutions, local government entities and stakeholders in the private sector, including financial, health, education and telecommunication, is essential to ensuring the success of the National Cybersecurity Policy.
3	The policy priorities capacity building, public-private partnerships, and research and development towards creating a well-coordinated framework for national Cybersecurity governance which draws from national and international best practices and appropriate legal frameworks for compliance. (CyberSecurityPolicy, 2021, pp. 1-17)

Develop a set of 10 highly important recommendations

Develop and Implement a Comprehensive National Cybersecurity Strategy

Developing and implementing a comprehensive national cybersecurity strategy is of paramount importance in today's digital age. Such a strategy serves as the cornerstone for safeguarding a nation's digital infrastructure, sensitive data, and the privacy of its citizens. It involves a multi-faceted approach that includes threat assessment, risk management, incident response planning, and the establishment of robust cybersecurity measures. A well-crafted strategy not only helps in preventing cyberattacks but also ensures a coordinated and efficient response in the event of a breach. It often requires collaboration between government agencies, private sector stakeholders, and international partners. By addressing the evolving landscape of cyber threats and promoting proactive measures, a comprehensive national cybersecurity strategy plays a vital role in maintaining the trust, security, and resilience of a nation's digital ecosystem.

Enhance Critical Infrastructure Protection

Enhancing critical infrastructure protection is an imperative task for any nation, as these vital systems and assets underpin the functioning of society and the economy. This involves developing comprehensive strategies and measures to safeguard essential infrastructure sectors such as energy, transportation, water supply, and healthcare from potential physical and cyber threats. The protection of critical infrastructure includes risk assessments, security protocols, resilience planning, and cooperation among government agencies, private sector partners, and relevant stakeholders. Cyber threats to these systems are of particular concern, given the increasing interconnectivity and reliance on digital technology. By enhancing critical infrastructure protection, a nation ensures its ability to withstand and recover from disruptions, whether they are caused by natural disasters, cyberattacks, or other unforeseen events, thereby promoting national security and the overall well-being of its citizens.

Strengthen Legal and Regulatory Framework

Strengthening the legal and regulatory framework is a fundamental component of ensuring a secure and thriving society, especially in an increasingly digital world. This involves continuously reviewing, updating, and adapting laws and regulations to address emerging challenges, such as cybersecurity threats, privacy concerns, and technological advancements. An effective legal and regulatory framework should strike a balance between protecting individual rights and fostering an environment that encourages innovation and economic growth. It also plays a crucial role in defining standards, enforcing compliance, and providing a clear legal recourse in cases of violations. A robust legal and regulatory framework is essential for safeguarding national security, preserving individual privacy, and maintaining the rule of law, which are all essential elements of a resilient and progressive society.

Data Privacy and Protection

Data privacy and protection are paramount in our digital age, where vast amounts of personal information are collected, processed, and stored. Ensuring the privacy of individuals and the security of their data is not only a matter of individual rights but also vital for building trust in the digital ecosystem. It involves implementing comprehensive measures to safeguard sensitive

information from unauthorized access, breaches, and misuse. Regulations, such as the General Data Protection Regulation (GDPR) in the European Union, have set a global standard for data privacy. These regulations grant individuals more control over their personal data and impose strict requirements on organizations regarding data collection and processing practices. Data privacy and protection are not only essential for preserving individual freedoms but also for maintaining the integrity and trust of businesses, government entities, and the broader society in the digital era.

Invest in Cybersecurity Education and Workforce Development

Investing in cybersecurity education and workforce development is a critical step in building a strong defense against the ever-evolving landscape of cyber threats. With technology playing an increasingly integral role in our daily lives, there's a growing demand for skilled cybersecurity professionals who can protect systems and data from malicious actors. These investments can take the form of educational programs, training initiatives, and research in the field of cybersecurity. By nurturing a well-trained and knowledgeable workforce, organizations and governments can better respond to cyber incidents and develop proactive strategies to prevent them. Cybersecurity education also empowers individuals to protect their own digital lives and contributes to overall digital literacy, creating a more resilient and secure digital environment for society at large.

Facilitate International Cooperation

Facilitating international cooperation is a crucial element in addressing global challenges, especially in the realms of security, trade, and diplomacy. In today's interconnected world, issues such as cybersecurity, climate change, and pandemics transcend national borders, making collaboration between nations more essential than ever. By working together, countries can share information, resources, and expertise to tackle common problems effectively. In the context of cybersecurity, for instance, international cooperation allows for the exchange of threat intelligence, the development of common standards, and the pursuit of cybercriminals across borders. Additionally, it promotes diplomacy, trade agreements, and peace by fostering mutual understanding and trust. In essence, facilitating international cooperation is not only a pragmatic approach to addressing global challenges but also a testament to the power of collective efforts in building a more stable and prosperous world.

Promote Public Awareness

Promoting public awareness in cybersecurity is a vital component of building a more secure and resilient digital society. In an era where individuals are increasingly connected online, it's imperative to educate the public about the risks and best practices for staying safe in the digital realm. This involves raising awareness about common cyber threats, such as phishing, malware, and identity theft, and teaching people how to recognize and respond to these dangers. Moreover, public awareness campaigns can emphasize the importance of strong, unique passwords, regular software updates, and the responsible use of social media and personal information online. By fostering a cybersecurity-conscious public, we not only reduce the likelihood of cyberattacks but also empower individuals to protect their digital identities and personal data, contributing to a safer and more resilient digital ecosystem for all.

Address Emerging Technologies

Addressing emerging technologies in cybersecurity is crucial in staying ahead of new and evolving threats in the digital landscape. As technology continues to advance, so do the techniques and tools that cybercriminals employ. It is imperative to stay proactive in researching and understanding these emerging technologies, such as artificial intelligence, the Internet of Things, and quantum computing, as they can both enhance and potentially undermine cybersecurity efforts. This proactive approach enables the development of robust security solutions that can adapt to new challenges, as well as the formulation of policies and regulations that ensure responsible and secure deployment of these technologies. By staying at the forefront of cybersecurity research and innovation, we can better protect digital infrastructure and data in an era of rapid technological change.

Establish an Effective Incident Response Plan

Establishing an effective incident response plan is a cornerstone of robust cybersecurity practices. In a digital environment where cyber threats are a constant reality, organizations and governments need a well-defined strategy to mitigate the impact of breaches and security incidents. Such a plan outlines the roles, responsibilities, and procedures to be followed when a cyber-incident occurs. It includes steps for identifying and containing the breach, analyzing the extent of the damage, notifying relevant stakeholders, and restoring affected systems to normal operation. An incident response plan is not only essential for limiting the damage caused by cyberattacks but also for maintaining the trust of customers, partners, and the public. In a world where data breaches and cyber incidents can have far-reaching consequences, a well-prepared incident response plan is a critical component of any cybersecurity strategy, ensuring a swift and coordinated response to safeguard digital assets and data.

Secure the Supply Chain

Securing the supply chain in cybersecurity has become an imperative as digital technologies become increasingly interconnected and reliant on third-party components and services. Supply chain security encompasses the safeguarding of all elements, from hardware and software to services and personnel that contribute to the development, delivery, and maintenance of digital systems. Ensuring the integrity of the supply chain is critical, as vulnerabilities or compromises at any point in this chain can have significant security implications. By implementing robust supply chain security measures, organizations can verify the trustworthiness of their suppliers, assess the security of components, and establish clear protocols for handling and updating software and hardware throughout their lifecycle. In a world where cyberattacks and breaches often originate from supply chain compromises, securing this critical aspect of the digital ecosystem is paramount to protecting sensitive data and maintaining a high level of trust in digital products and services.

Implementation design for the two most critical recommendations

a) Cybersecurity Education and Workforce Development

Overall Objective (Impact)	• To enhance Pakistan's national Cybersecurity resilience by developing a skilled and capable Cybersecurity workforce
Specific Objectives (Outcomes)	• To establish a sustainable and effective Cybersecurity education and workforce development program.
Activities	• Develop and update Cybersecurity curriculum for educational institutions. • Establish Cybersecurity training centers and programs. • Conduct workshops, seminars, and webinars on Cybersecurity. • Facilitate internships, apprenticeships, and practical training opportunities. • Create a public awareness campaign on the importance of Cybersecurity careers.
Indicators	• Number of educational institutions incorporating updated Cybersecurity curriculum. • Number of Cybersecurity training centers established. • Participation rates in workshops, seminars, and webinars. • Number of internships and apprenticeships provided. • Increase in the number of Cybersecurity professionals.
Means of Verification	• Records and reports from educational institutions on curriculum updates. • Documentation of established training centers. • Attendance registers and feedback from workshop participants.

	• Records of internships and apprenticeships. • Government and industry workforce data.
Assumptions	• Availability of subject matter experts and educational institutions willing to update curriculum. • Funding and resources for establishing training centers. • Interest and participation from the target audience in workshops and seminars. • Willingness of organizations to offer internships and apprenticeships.
Risks and Assumptions	• Lack of funding and resources for the project. • Limited interest in Cybersecurity careers among the target audience. • Difficulty in finding qualified instructors for training programs. • Availability of Cybersecurity experts willing to participate in education and training programs. • A supportive legal and regulatory framework for Cybersecurity education and training.
Responsible Parties	• Ministry of IT and Telecommunication. Educational institutions and technical training centers. • Industry associations and Cybersecurity professionals. • Government agencies responsible for internships and apprenticeships. • Public and private sector organizations involved in Cybersecurity awareness campaigns. • Academic institutions and industry associations.
Budget	• A detailed budget allocation for each activity, including funding sources and financial projections.
Timeline	• A timeline specifying the start and end dates for each activity and the project as a whole.

b) Promote Public Awareness

Overall Objective (Impact)	• To enhance Cybersecurity awareness and best practices among the public in Pakistan, contributing to a more secure online environment.
Specific Objectives(Outcomes)	• To implement a successful public awareness campaign on Cybersecurity
Specific Objectives(Outcomes)	• To implement a successful public awareness campaign on Cybersecurity

Activities	• Develop Cybersecurity educational materials, including brochures, videos, and infographics. • Measure and evaluate the effectiveness of the awareness campaign
Indicators	• Number of educational materials distributed. • Attendance and participation in workshops and training sessions. • Pre-and post-awareness campaign knowledge assessments
Means of Verification	• Analytics from social media and website platforms. • Workshop attendance records and participant feedback.
Assumptions	• Availability of Cybersecurity experts and content creators to develop materials. • Willingness of media outlets to collaborate in the awareness campaign.
Risks and Assumptions	• Limited engagement from the public due to information overload. • Difficulty in securing media partnerships. • Cooperation from local communities and organizations.
Responsible Parties	• Ministry of IT and Telecommunication. • Social media managers, content creators, and media partners. • Trainers and facilitators for workshops and training sessions.
Budget	• A detailed budget specifying costs for material development, media partnerships, workshop logistics.
Timeline	• A timeline specifying the start and end dates for each activity, including the campaign's duration and assessment periods.

References

1. Amin, T. (2023, October 13). CERT rules 2023 notified to bolster cyber security defence. Retrieved from https://www.brecorder.com/news/40267846/cert-rules-2023-notified-to-bolster-cyber-security-defence
2. Anwar, M. W. (2020, October). Cyber Security in Pakistan: Regulations, gaps and way forward. Retrieved from https://www.researchgate.net/publication/349097228_Cyber_Security_in_Pakistan_Regulations_Gaps_and_Way_Forward
3. CyberSecurityPolicy. (2021, January 15). National Cyber Security Policy 2021 (Consultation Draft). Retrieved from https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Consultation%20Draft(1).pdf
4. DHS's Cybersecurity Mission—An Overview. (2023, August). Cybersecurity mission overview. Retrieved from https://crsreports.congress.gov/product/pdf/IF/IF10683
5. Financial Stability Review. (2017). Cybersecurity and financial stability. Retrieved from https://www.sbp.org.pk/fsr/2017/boxes/Box-6.1.pdf
6. Hassan, A. (2021). Pakistan Army's cyber command. Retrieved from https://pakstrategic.com/pakistan-armys-cyber-command
7. Khan, M. A. (2021, March 21). NADRA database hack in context of cyber kill chain and overview of Pakistan's cybersecurity. Retrieved from https://easychair.org/publications/preprint/nJWK
8. Mohammad Yasin, A., Khaver, A. A., & Rubab. (2019, February 14). Cybersecurity: Where does Pakistan stand. Retrieved from https://sdpi.org/cyber-security-where-does-pakistan-stand-w-167/publication_detail
9. Pakistan: Experts propose recommendations to protect civilians in cyberspace. (2023, July 21). Recommendations for cybersecurity in Pakistan. Retrieved from https://www.icrc.org/en/document/pakistan-roundtable-ihl-cyber-security
10. The National Cybersecurity Strategy—Going Where No Strategy Has Gone Before. (2023, July 17). Overview of national cybersecurity strategy. Retrieved from https://crsreports.congress.gov/product/pdf/IN/IN12123