# Analyzing the Key Responsible Factors:

## Cyber Security in Pakistan

*Muhammad Ahmad Usmani*[1]

**Suggested Citation:**

Usmani, M. A. (2023). Analyzing the Key Responsible Factors: Cyber Security in Pakistan. *Journal of Pakistan Administration. 44*(2). 145–161.

Received: July 23, 2023/ Accepted: October 30, 2023/ Published: December 31, 2023.

## Abstract

This policy paper provides a comprehensive examination of Pakistan's current cybersecurity landscape, highlighting the main hurdles confronting the nation in this realm. It reviews the existing cybersecurity framework, including the Prevention of Electronic Crimes Act 2016 (PECA) and the National Cybercrime Policy 2021, while also identifying shortcomings and vulnerabilities within the system. The paper offers suggestions to address the escalating dangers and difficulties in the online environment, aiming to maintain a protected and durable online realm for individuals universally. To implement these suggestions, specific tactics are proposed. Embracing these actions and tactics can strengthen Pakistan's cybersecurity framework, protect critical infrastructure, and establish a secure and resilient cyberspace. This effort is crucial for securing the country, promoting economic stability, and improving the welfare of its inhabitants amidst continually changing cyber risks. In addition to the above, the paper discusses the importance of public-private partnerships in enhancing cybersecurity measures. It emphasies the need for collaboration between government agencies, private sector entities, and civil society organizations to effectively combat cyber threats. Furthermore, the paper explores the role of international cooperation in cybersecurity. It highlights the significance of bilateral and multilateral agreements in sharing information, conducting joint cyber exercises, and developing common cybersecurity standards. Moreover, the paper addresses the issue of capacity building in cybersecurity. It stresses the importance of training

[1] Office Management Group, Government of Pakistan
e-mail: ahmadusmani@gmail.com

programs and awareness campaigns to equip individuals and organizations with the necessary skills and knowledge to mitigate cyber risks. Overall, this policy paper provides a holistic view of Pakistan's cybersecurity challenges and proposes practical solutions to enhance its cybersecurity posture. By implementing these recommendations, Pakistan can secure its cyberspace, protect its critical infrastructure, and ensure the safety and prosperity of its citizens in the digital age.

***Keywords:*** *cyber, security, technology.*

## 1. Introduction

There is an extensive set of practices and techniques that fall under the umbrella term 'cybersecurity' in order to effectively defend computer networks; software applications and malicious hacking attempts originated by skilled individuals known as hackers; malware instances; spyware occurrences; traps set up via online scams commonly referred to as phishing attempts; additionally covering all possible forms which a breach in adequate protection could result in unauthorized access or disclosure. Concerning computer security, the term "cybersecurity" is commonly used.

Acknowledging the prominence of expansive databases and technology-driven systems that oversee essential operations and secure precious information, prioritizing their protection against unauthorized access, manipulation, or theft becomes supremely significant. From a wider perspective of society, cybersecurity involves securing public-facing facilities. For example, investigation exposed that more than 432 million individuals have experienced the impact of cybercrimes. Consequently, preserving facilities including websites, ATM machines, and computer networks from these threats is the fundamental aspect of cybersecurity.

At the global level, cybersecurity faces numerous challenges, including increasing cybercrime rates, sophisticated cyber-attacks by state and non-state actors, ransomware attacks targeting critical infrastructure, and the proliferation of Internet of Things (IoT) devices with inadequate security measures (Simon, 2017; Cristea, 2020; Rees and Rees, 2023; Munk, 2022). Additionally, the lack of international cooperation and harmonized cybersecurity standards further complicates the global cybersecurity landscape (Bechara & Schuch, 2021).

According to Khan et al. (2021) the global cybersecurity issues have significant effects on Pakistan's cybersecurity. Pakistan is vulnerable to cyber-attacks due to its reliance on digital technologies for various sectors, including banking, healthcare, and government services. The country faces challenges such as data breaches, financial fraud, and disruptions to critical infrastructure. Additionally, Pakistan's cybersecurity infrastructure and policies are still evolving, making it more susceptible to global cyber threats. Strengthening international collaborations and adopting robust cybersecurity measures are essential for Pakistan to mitigate the effects of global cybersecurity issues (Ahmad, 2022; Malik et al., 2022).

Recognizing that addressing cybersecurity requires collaboration that cannot be solely correlated to the government. Although it is crucial for governments to combat cybercrimes and implement suitable measures, depending solely on them is inadequate in completely eradicating this widespread danger.

### 1.1. Objective of Policy Paper

This policy paper is primarily focused to carry out an extensive assessment of the present cybersecurity situation in Pakistan. This study's goal is to pinpoint and evaluate the fundamental challenges that the country experiences in relation to this area. In addition, it offers strategic responses and suggestions to bolster cybersecurity measures and actively diminish the effects of cyber hazards. By implementing these measures, the aim of this document is to make policymakers, government organizations, and individuals aware of the urgent requirement to confront cybersecurity challenges.

## 1.2. Overview of Paper Structure

- In the previous section of introduction, the policy paper provides some general information regarding the terminology of "Cybersecurity" and outlines its objective. Through its establishment, it creates a background for grasping the difficulties confronted by the nation and the value of developing practical countermeasures.

- Regarding the section about cyber security challenges covers the developing threat landscape. By conducting this analysis, a thorough comprehension of the dangers and susceptibilities faced by Pakistan is established.

- Assessing Pakistan's current cyber security framework, the paper reviews existing policies, strategies, institutional arrangements, and coordination mechanisms. Examines the technological capacities and the current physical setup and spots inadequacies and shortcomings that obstruct the effectiveness of the present structure.

- Considering the findings from the analysis, the report offers customized policy proposals to solve Pakistan's particular difficulties. All recommendations are intended to enhance the cybersecurity measures in Pakistan and alleviate the identified vulnerabilities.

- To ensure successful implementation of the recommendations, the document ends by providing a segment focused on tactics for putting them into practice.

## 2. Background and Significance of Cybersecurity in Pakistan

Pakistan has undergone a major change as the years passed regarding cybersecurity. Because of the swift progress of digital infrastructure and an escalating dependence on technology, the nation has accepted the critical necessity to effectively tackle cybersecurity challenges.

- The early 2000s marked an increase in cybercrimes and threats within the nation. As a response measure, under the ***Federal Investigation Agency (FIA)***, the government formed the ***National Response Center for Cyber Crimes (NR3C)***. Within Pakistan's borders, NR3C is the main body in charge of investigating and fighting against cybercrimes. By fostering joint ventures and associations with global partners, NR3C has strengthened its capacity to efficiently tackle cyber threats spanning across borders.
- Additionally, Pakistan has been successful in advancing the cause of cybersecurity awareness and education. Multiple undertakings, like conferences, workshops, and educational programs, aim to teach individuals, businesses, and government entities about cyber risks and best practices to protect digital assets.
- The dedication of the government to maintaining cybersecurity is apparent is evident through the formulation of the ***National Cyber Security Policy*** in ***2014.*** By offering a strategic framework, this policy aims to fortify cybersecurity measures and drive the uptake of advanced security technologies. In addition to that, Pakistan has allocated funds to develop advanced infrastructure and successfully established world-class cybersecurity centers aiming to strengthen its cyber defenses.

## 3. Literature Review

Cybersecurity issues began to emerge with the rapid expansion of the internet and digital technologies. The interconnected nature of these technologies created vulnerabilities that malicious actors could exploit. Initially, cyber attacks were relatively simple, but as technology advanced, so did the sophistication of cyber threats (Lewallen, 2021; Djenna et al., 2021). Today, cyber attacks range from simple phishing scams to complex ransomware attacks, often orchestrated by well-funded and highly organized groups.

Cybersecurity issues have caused significant damages across various sectors. These damages include financial losses due to fraud and theft, disruption of critical infrastructure leading to service outages, compromise of sensitive information leading to privacy breaches, and reputational damage to organizations and individuals affected by cyber attacks (Ani et al., 2017). The costs of recovering from cyber attacks can be substantial, impacting both businesses and governments (Hasan et al., 2021).

Third World countries like Pakistan are involved in cybersecurity issues due to their increasing reliance on digital technologies (Khan et al., 2023). As these countries modernize their infrastructure and services, they become more susceptible to cyber attacks. Additionally, the lack of robust cybersecurity measures and awareness makes them attractive targets for cyber criminals. Pakistan, in particular, has faced challenges in securing its digital infrastructure and protecting its citizens' data from cyber threats (Shad, 2019).

Pakistan faces cultural challenges in addressing cybersecurity issues, including a lack of awareness about cyber threats, limited resources for cybersecurity education and training, and cultural norms that may not prioritize cybersecurity (Ibrar et al., 2023). Additionally, the rapid adoption of digital technologies in Pakistan has outpaced the development of cybersecurity policies and regulations, further exacerbating these challenges.

Haider et al. (2023) highlighted that the government of Pakistan has taken several measures to enhance cybersecurity, including the enactment of the Prevention of Electronic Crimes Act 2016 (PECA) and the formulation of the National Cybersecurity Policy 2021. These measures aim to strengthen cybersecurity infrastructure, enhance law enforcement capabilities, and increase public awareness about cyber threats. Additionally, the government has established cybersecurity centers and partnerships with international organizations to improve cybersecurity resilience.

Despite the government's efforts, there are several gaps in current cybersecurity measures in Pakistan. These include inadequate resources for cybersecurity education and training, limited coordination between government agencies and private sector entities, and challenges in enforcing cybersecurity laws and regulations (Basit et al., 2023). Additionally, the lack of public awareness about cybersecurity issues remains a significant gap that needs to be addressed.

Several factors contribute to cybersecurity issues in Pakistan, including rapid technological advancements, limited cybersecurity expertise and resources, insufficient regulatory frameworks, and the increasing connectivity of devices and systems (Awan et al., 2017). Additionally, the lack of international cooperation in addressing cyber threats and the evolving nature of cyber attacks make it challenging for Pakistan to effectively mitigate cybersecurity risks.

## 3.1. Cybersecurity Challenges in Pakistan

Pakistan currently ranks as the tenth largest population of internet users globally. With the adoption of 2G and 4G technologies, internet penetration in Pakistan reached 17.8% in 2016. However, the growth of the digital economy and increased internet usage also brings cybersecurity challenges. Pakistan ranked 94th globally in the 2018 Global Cyber Security Index Report. It encountered high malware and crypto-currency mining rates in 2018, and incidents like the hacking of senior officials' mobile phones using the 'Pegasus' malware raised concerns. The financial sector in Pakistan faces serious cyber threats, including card skimming, ATM card misuse, hacking, and online payment fraud. Thousands of bank accountholders have fallen victim to hackers, resulting in significant financial losses for Pakistani banks.

## 3.2. Major Challenges Faced by Pakistan

Cyberspace has become a potent tool for crime, terrorism, and warfare, presenting significant challenges to national security in today's age. Pakistan's increasing reliance on cyberspace raises concerns about the country's national security due to inadequate cybersecurity measures. Insufficient legislative, technological, organizational, capacity-building, and collaboration measures contribute to Pakistan's cybersecurity vulnerabilities.

Examples of Pakistan's inadequate cybersecurity measures include reports of the US National Security Agency (NSA) considering Pakistan as its second most-wanted target after Iran, as revealed by Snowden in 2013 (Khan et al., 2021). Allegations of the UK's Government Communications Headquarters (GCHQ) hacking into Pakistan's major communications infrastructure further exposed the country's vulnerabilities. Microsoft reported that Pakistan experienced the highest number of malware attacks in the second half of 2015. Additionally, Pakistan has been targeted by foreign espionage, as highlighted by the Senate Committee on Foreign Affairs (Khattak, 2017).

In following, some of the major cybersecurity challenges faced by Pakistan are discussed.

### 3.2.1. Cybercrime

As global financial and commercial transactions increasingly shift to digital platforms, organized and skilled criminals are drawn to cybercrime. Dark Market and other black-market networks, such as Silk Road, engage in various cybercrime operations, including the theft and sale of personal data from bank accounts, credit cards, social security numbers, and passwords, as well as the trafficking of botnets. This transition of organized crime from offline to online has significant detrimental effects on the global economy.

Pakistan, as e-banking and e-government gain traction, cybercrime is on the rise. The country faces various cybercrimes, ranging from account hacking to illegal cash withdrawals and money transfers. The Federal Investigation Agency's (FIA) cybercrime unit, the National Response Center for Cyber Crimes (NR3C), received a total of ***2019*** complaints in 2017. These complaints can be categorized into three primary categories: social media harassment, slander, and extortion; financial fraud; threats via telephone; and email hacking.

The financial sector appears to be particularly vulnerable to massive cybercrime incidents based on the mentioned ranking. ***Habib Bank Limited (HBL) ATMs***, for instance, fell victim to a sophisticated cyberattack involving skimming devices that compromised 579 accounts and resulted in the theft of Rs10 million. In recent years, computer hacking, and phishing/email scams have become increasingly common methods employed by cybercriminals to gain unauthorized access to computer networks and steal sensitive or personal data, enabling them to commit fraud.

### 3.2.2. Cyberwarfare

Cyberwarfare refers to state-sponsored cyberattacks conducted by well-funded and highly skilled professionals. These cyber-attacks are orchestrated by governments with political, security, and strategic objectives in mind. In the evolving landscape of warfare, cyberspace has emerged as a new battleground where governments strategically leverage digital means to support conventional military operations. This paradigm shift signifies the integration of cyber capabilities into broader military strategies, marking a new phase in warfare.

Due to their long-standing animosity, India's cyberwarfare capabilities are highly likely to be directed towards Pakistan.

Pakistan remains unaffected by any major cyberattacks. However, instances of confrontation between the Pakistan and India are becoming increasingly common. India is known to have numerous organized hacker organizations, such as **the Indian Computer Association** and the **Hindustan Hackers Organization**. The utilization of web vandalism and cyber espionage by India in its dealings with Pakistan has sparked worries, this has resulted in the FBI launching investigations. The likelihood of India aiming at Pakistan's critical infrastructure should not be dismissed.

### 3.2.3. Cyberterrorism

The cyber realm has turned into a rendezvous point for terrorists who utilize the internet. Their local and global objectives are pursued due to their ideological and political motivations. These terrorists exploit cyberspace for communication and actively promote propaganda, indoctrination, and radicalization. Besides causing harm to the websites and networks of their opponents, they also involve themselves in practices like stealing money. They manage physical activities in the unregulated domain of the internet. With its capability to offer anonymity, low cost, and worldwide access, the internet becomes a desirable and practical tool for terrorist organizations.

Pakistan has experienced significant forms of political and religious terrorism following the aftermath caused by September 11th. In terms of these acts of terrorism, it is predominantly groups like the Tehreek-e-Taliban Pakistan (TTP) and other sectarian organizations within the nation who carry them out. Violence frequently accompanies this terrorism along with ethnic separatism. Despite primarily relying on physical attacks, terrorist groups in Pakistan. They have also utilized online platforms to persuade individuals, enlist fresh recruits, and propagate their extreme viewpoints.

### 3.2.4. Hacking

Hacking poses a significant cyber risk. Unauthorized access to computer systems is involved with the intention of causing damage, disruption, or engaging in unlawful activities. Hackers can possess different motivations and varying degrees of skills. Cybercriminals include hackers who are driven by personal, political, criminal, or state-sponsored motives. While hacking may not be as grave as other major cyber threats, it is still a substantial worry. Hacking activities in Pakistan target various sectors, including government institutions, businesses, financial institutions, and individual users. Financial losses, data breaches, identity theft, and reputational damage are potential consequences of these cyberattacks.

### 3.2.5. Information Warfare - influence on public perception and stability

Information warfare is the tactical and strategic use of information to gain an advantage. "It includes multiple types of operations and has been pursued in radically different ways during different eras" (Rouse, 2017).

Pakistan has become a target of Information Warfare (IW) orchestrated by the West in collaboration with India and Israel. The areas being targeted encompass Pakistan's sovereignty, territorial integrity, cultural identity, ideological and ethnic cohesion, and its economy. Additionally, the country's nuclear program, strategic assets, armed forces, and intelligence agencies have been specifically selected as prime targets for engagement through IW.

During the operation "Rah-e-Rast" in Swat and Malakand regions in 2008/2009, a perception was deliberately created by the disinformation cells of the US and Western media that Pakistan was succumbing to the Taliban. The capabilities of the Taliban were exaggerated during this campaign.

The impact of Information Warfare on the perception and stability of the Pakistani public cannot be underestimated. By disinformation campaigns, psychological tactics, and manipulation of media narratives, IW aims to mold public opinion, sow discord, and destabilize the country.

External actors, often in collaboration with local elements, employ IW tactics to distort reality, propagate falsehoods, and portray Pakistan in a negative light. These efforts breed insecurity, mistrust, and anxiety among the public. By exploiting existing grievances, IW exacerbates social, political, sectarian, ethnic, and ideological divisions within society.

Moreover, IW specifically targets the cultural identity and core values of the Pakistani public. This deliberate strategy fosters confusion, cynicism, and a sense of disillusionment among the population.

## 4. Current Cybersecurity Framework of Pakistan

### 4.1. Prevention of Electronic Crimes Act 2016 (PECA)

The Prevention of Electronic Crimes Act 2016 (PECA) governs the existing cybersecurity legal framework in Pakistan. The objective of this act is to combat the escalating cybercrimes and offenses connected to information systems.

- If someone engages in unauthorized access, copying, or transmission of data or information systems under the PECA with any wrongful intention, they can be held liable for a punishable offense. The act also requires service providers to retain specified traffic data, including information about communication origins, destinations, routes, timing, size, duration, and service type, for a minimum of one year. data as instructed.
- In addition, the PECA creates a computer emergency response team that is accountable for addressing threats or attacks on critical infrastructure information systems or data within Pakistan.

### 4.2. National Cybercrime Policy 2021

The establishment of the National Cyber Crime Policy 2021 was a major development in the direction of developing a comprehensive framework for cybersecurity in Pakistan. The Policy, approved by Parliament on 27 July 2021, necessitates exceptional initiatives to tackle cybersecurity challenges.

The Policy provides comprehensive objectives aimed at addressing cybersecurity challenges and risk factors prevalent in Pakistan. Some of the objectives highlighted under the Policy include:

- Promoting data privacy and protection
- Upgrading information systems and infrastructure
- Raising awareness in public about cybersecurity issues

### 4.3. Recent Works

A notable recent development in Pakistan's cybersecurity landscape is the establishment of the Cyber Security Framework, implemented by the Pakistan Telecommunication Authority (PTA) through the Critical Telecom Data and Infrastructure Security Regulation (CTDISR). This framework imposes obligations on auditors and licensees to monitor, record, and report any breaches of data and other cyber-related crimes, thereby enhancing the management and mitigation of cybersecurity risks.

Another recent development is the establishment of ***National Cyber Security Authority (NCSA)*** to lead the country's cybersecurity efforts. It plays a vital role in formulating policies, devising strategies, and implementing programs aimed at bolstering cybersecurity.

## 4.4. Gaps and Weaknesses in Current Framework

The current cybersecurity framework in Pakistan has been widely criticized for its inadequacy and inefficiency in addressing the growing cyber threats faced by the country.

- One of the key issues is the lack of comprehensive and up-to-date cybersecurity legislation and regulations. The existing laws are outdated and fail to keep pace with the rapidly evolving cyber landscape.
- The coordination and cooperation among different government agencies responsible for cybersecurity remains fragmented, resulting in a lack of unified and coordinated efforts.
- The shortage of skilled cybersecurity professionals is another critical gap in the framework which further aggravates the problem.

## 4.5. Policy Recommendations

In this section, some of the recommendations will be provided to tackle current cybersecurity challenges faced by the state and enhance the current framework.

### 4.5.1. Increase Awareness

Pakistan should prioritize the augmentation of awareness concerning the perils and vulnerabilities associated with cyber assaults, while simultaneously advocating for the proliferation of cybersecurity education and training initiatives targeting both individuals and organizations. It is imperative to guarantee that individuals are well-informed about the significance of robust passwords, phishing scams, and other prevalent stratagems employed by cyber malefactors.

### 4.5.2. Enhance Legislation and Regulation

Pakistan should implement and uphold cybersecurity regulations that establish a concise legal structure to combat cyber risks and safeguard vital information infrastructure. These regulations ought to encompass measures for safeguarding data, upholding privacy rights, facilitating incident reporting, and imposing sanctions for cyber offenses. Continuously assess and enhance the legislation to align with the dynamic landscape of evolving cyber dangers.

### 4.5.3. Establish a National Cybersecurity Strategy

The state should formulate an all-encompassing cybersecurity blueprint at the national level, delineating the aims, objectives, and executable initiatives to effectively tackle cybersecurity hurdles in Pakistan as soon as possible. This strategy should encompass the active involvement of crucial stakeholders from governmental entities, private sector enterprises, educational institutions, and civil society. It should primarily concentrate on augmenting cybersecurity consciousness, forging resilient legal structures, bolstering technical proficiencies, and fostering collaborative ties on the global stage.

### 4.5.4. Strengthen Cybersecurity Framework

Government must allocate resources towards the creation and sustenance of a resilient cybersecurity framework, encompassing cutting-edge technologies, tools, and proficiency. This initiative entails the establishment of a ***National Computer Emergency Response Team*** to proactively monitor, swiftly respond to incidents, and facilitate the exchange of information.

### 4.5.5. Foster International Cooperation and Public-Private Collaborations

Government should actively participate in international forums and forge strategic partnerships to foster enhanced cooperation on cybersecurity matters. It should also collaborate closely with neighboring nations, international organizations, and global initiatives dedicated to cybersecurity, facilitating the exchange of valuable information, intelligence, and exemplary approaches. We must engage in capacity-building initiatives and knowledge-sharing endeavors to enhance the expertise and proficiency of cybersecurity professionals in Pakistan. Harmonious collaboration between public and private sector entities should also be encouraged to collectively tackle cybersecurity challenges. Dynamic public-private partnerships will facilitate the sharing of resources, expertise, and threat intelligence. State should motivate private sector organizations to proactively invest in cybersecurity measures and willingly adopt industry best practices.

### 4.5.6. Promote Education, Research and Development in Cybersecurity

Educational boards should integrate cybersecurity educational initiatives into the curriculum of schools, colleges, and universities, ensuring that the upcoming workforce possesses essential skills to effectively counter cyber threats. Additionally, the government should dedicate resources to research and development endeavors, focusing on advancing cybersecurity technologies and methodologies by allocating funding and offer incentives to cybersecurity startups and entrepreneurs, enabling them to tailor solutions specifically tailored to Pakistan's unique challenges.

### 4.5.7. Foster International Trust

Pakistan should showcase its unwavering dedication to cybersecurity by upholding international norms, standards, and treaties. Engaging in diplomatic endeavors to cultivate trust and foster collaboration with other nations in the realm of cyberspace is the need of the hour. Government should actively participate in international dialogues concerning cyber norms and make substantial contributions to the formulation of comprehensive global frameworks for cybersecurity.

### 4.5.8. Regular Audits and Assessments

We must institute periodic cybersecurity audits and evaluations spanning government agencies, critical infrastructure, and private sector entities. These assessments should identify potential weaknesses, assess the efficacy of current cybersecurity measures, and propose essential enhancements.

## 4.6. Implementation Strategies

Following strategies can be adopted by the government for the implementation of above provided policy recommendations.

**Table 1**

*Policy Recommendations and Implementation Strategies*

| **Policy Recommendations** | **Implementation Strategies** |
|---|---|
| Increase Awareness | • Launch nationwide awareness campaigns to disseminate knowledge<br>• Conduct comprehensive cybersecurity education and training programs<br>• Promote awareness through various media platforms and social networks |
| Enhance Legislation and Regulation | • Engage legal experts and stakeholders to draft robust legislation<br>• Establish regulatory bodies to enforce cybersecurity regulations<br>• Regularly review and update legislation to align with evolving threats |
| Establish a National Cybersecurity Strategy | • Form a task force comprising key stakeholders to devise a comprehensive strategy |

| **Policy Recommendations** | **Implementation Strategies** |
|---|---|
| Strengthen Cybersecurity Framework | • Conduct thorough assessments and gap analysis to inform the strategy<br>• Define clear objectives and establish realistic timelines for implementation<br>• Invest in cutting-edge technologies and advanced cybersecurity tools<br>• Establish a National Computer Emergency Response Team (CERT) for proactive monitoring<br>• Foster public-private collaborations to leverage expertise and resources |
| Foster International Cooperation | • Engage actively in international forums and forge strategic partnerships<br>• Facilitate information sharing and exchange best practices with partners<br>• Participate in capacity-building programs and professional exchanges |
| Promote Education, Research and Development | • Integrate cybersecurity education into educational curricula at all levels<br>• Allocate substantial funding for research and development initiatives<br>• Provide incentives and grants to cybersecurity start-ups and R&D projects |
| Foster International Trust | • Engage in diplomatic efforts to cultivate trust and foster collaboration<br>• Actively participate in international dialogues on cybersecurity norms<br>• Contribute significantly to the formulation of comprehensive global frameworks |

| Policy Recommendations | Implementation Strategies |
|---|---|
| Regular Audits and Assessments | • Develop a robust framework for conducting regular audits and assessments<br>• Establish independent auditing bodies to ensure impartiality and transparency<br>• Enforce mandatory reporting of cybersecurity incidents to facilitate analysis |

*Note*: Policy Recommendations and Implementation Strategies are given by researcher

## 5. Conclusion

In conclusion, addressing cybersecurity challenges in Pakistan requires a comprehensive approach encompassing legislation, awareness, collaboration, and technological advancements. The policy recommendations presented in this paper offer a strategic roadmap to strengthen the cybersecurity framework and effectively mitigate cyber threats.

- Raising awareness about cyber risks and promoting best practices is crucial. Launching nationwide awareness campaigns and implementing cybersecurity education and training programs will empower individuals and organizations to protect their digital assets.
- Strengthening legislation and regulation is essential to establish a concise legal structure that combats cyber risks, safeguards data, and imposes sanctions for offenses.
- Formulating a national cybersecurity strategy is vital to coordinate efforts across governmental entities, private sector enterprises, educational institutions, and civil society. This strategy should focus on increasing cybersecurity consciousness, forging resilient legal structures, bolstering technical proficiencies, and fostering global collaboration.
- To strengthen the cybersecurity framework, investment in cutting-edge technologies and the establishment of a National Computer Emergency Response Team (CERT) are necessary. Collaborations between the public and private sectors will leverage expertise and resources to enhance cyber defenses and respond swiftly to incidents.
- Fostering international cooperation and trust through active

participation in global forums, strategic partnerships, and knowledge sharing is paramount. Pakistan should contribute to international dialogues on cybersecurity norms and play a significant role in formulating comprehensive global frameworks.

- Promoting education, research, and development in cybersecurity is pivotal for building a skilled workforce and driving innovation. Integrating cybersecurity education into curricula, allocating funds for research, and providing incentives to startups and entrepreneurs will enable Pakistan to effectively counter cyber threats.

By adopting these recommendations and implementing the outlined strategies, Pakistan can strengthen its cybersecurity framework, protect critical information infrastructure, and establish a secure and resilient cyberspace. This will contribute to national security, economic stability, and the well-being of its citizens in an increasingly interconnected world.

## 6. References

Ahmad, S. (2022). Cyber security threat and Pakistan's preparedness: An analysis of national cyber security policy 2021. *Pakistan Journal of Humanities & Social Sciences Research*, *5*(1), 33. https://doi.org/10.37605/pjhssr.v5i1.381

Ani, U. P. D., He, H., & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective. *Journal of Cyber Security Technology*, *1*(1), 32-74. https://doi.org/10.1080/23742917.2016.1252211

Awan, J. H., Memon, S., Khan, R. A., Noonari, A. Q., Hussain, Z., & Usman, M. (2017). Security strategies to overcome cyber measures, factors and barriers. *Eng. Sci. Technol. Int. Res. J*, *1*(1), 51-58.

Basit, A., Qazi, T. F., Niazi, A. A. K., & Niazi, I. A. K. (2023). Structural analysis of the barriers to address cyber security challenges. *Journal of Policy Research*, *9*(1), 221-236. https://doi.org/10.5281/zenodo.7908753.

Bechara, F. R., & Schuch, S. B. (2021). Cybersecurity and global regulatory challenges. *Journal of Financial Crime*, *28*(2), 359-374. https://doi.org/10.1108/JFC-07-2020-0149

Cristea, L. M. (2020). Current security threats in the national and international context. *Journal of accounting and management information systems*, *19*(2), 351-378.

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences*, *11*(10), 4580. https://doi.org/10.3390/app11104580

Haider, W., Ali, A., & Zubair, M. (2023). Prevention of Electronic Crime Act, 2016: An Analysis of the Act's Effectiveness in Controlling Misuse of Social Media in Pakistan. *Journal of Educational Research and Social Sciences Review (JERSSR)*, *3*(2), 48-54.

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, 102726. https://doi.org/10.1016/j.jisa.2020.102726

https://doi.org/10.1111/rego.12341

Ibrar, M., Li, H., Wang, J., & Karim, S. (2023). Tackling Pakistan's Cyber Security Challenges: A Comprehensive Approach. *International Journal of Network Security*, *25*(3), 529-536.

Khan, M. F., Raza, A., & Naseer, N. (2021). Cyber security and challenges faced by Pakistan. *Pakistan Journal of International Affairs*, *4*(4). https://doi.org/10.52337/pjia.v4i4.408

Khan, N. F., Ikram, N., Saleem, S., & Zafar, S. (2023). Cyber-security and risky behaviors in a developing country context: A Pakistani perspective. *Security Journal*, *36*(2), 373-405. https://doi.org/10.1057/s41284-022-00343-4

Khattak, I. (2017, January 19). Pakistan top target for foreign espionage: Senate committee told. *DAWN.* https://www.dawn.com/news/1309413

Lewallen, J. (2021). Emerging technologies and problem definition uncertainty: The case of cybersecurity. *Regulation & Governance*, *15*(4), 1035-1052. https://doi.org/10.1111/rego.12341

Malik, Z. U. A., Xing, H. M., Malik, S., Shahzad, T., Zheng, M., & Fatima, H. (2022). Cyber security situation in Pakistan: A critical analysis. *PalArch's Journal of Archaeology of Egypt/Egyptology*, *19*(1), 23-32.

Munk, T. (2022). *The rise of politically motivated cyber attacks: Actors, attacks and cybersecurity*. Routledge.

Rees, J., & Rees, C. J. (2023). Cyber-Security and the Changing Landscape of Critical National Infrastructure: State and Non-state Cyber-Attacks on Organizations, Systems and Services. In *Applications for Artificial Intelligence and Digital Forensics in National Security* (pp. 67-89). Cham: Springer Nature Switzerland.

Rouse, M. (2017, January 04). Information warfare. In *Techopedia.* https://www.techopedia.com/definition/29777/information-warfare#:~:text=Information%20warfare%20is%20the%20tactical,information%20to%20gain%20an%20advantage.

Shad, M. R. (2019). Cyber threat landscape and readiness challenge of Pakistan. *Strategic Studies*, *39*(1), 1-19. https://www.jstor.org/stable/48544285

Simon, T. (2017). Chapter seven: Critical infrastructure and the internet of things. *Cyber security in a volatile world*, *93*.