p-ISSN : 2708-2121 | e-ISSN : 2708-3616

DOI(Journal): 10.31703/gsssr
DOI(Volume): 10.31703/gsssr/.2024(IX)
DOI(Issue): 10.31703/gsssr.2024(IX.II)

www.gsssrjournal.com

GSSSR
Global Strategic and Security Studies Review
surveilling humanity

GSSSR

GLOBAL STRATEGIC & SECURITY STUDIES REVIEW

VOL. IX, ISSUE II, SPRING (JUNE-2024)

HumanityPublications
sharing research
www.humapub.com
US | UK | Pakistan

Double-blind Peer-review Research Journal
www.gsssrjournal.com

Humanity Publications(HumaPub)
www.humapub.com
Doi:https://dx.doi.org/10.31703

Article Title

A Controversial Hypercritical Examination of Cybersecurity Policies in Pakistan that Cannot Be Ignored

Global Strategic & Security Studies Review

p-ISSN: 2708-2121**e-ISSN:** 2708-3616
DOI(journal): 10.31703/gsssr
Volume: IX (2024)
DOI (volume): 10.31703/gsssr.2024(IX)
Issue: II (Spring-June 2024)
DOI(Issue): 10.31703/gsssr.2024(IX-II)

Home Page
www.gsssrjournal.com

Volume: IX (2024)
https://www.gsssrjournal.com/Current-issues

Issue: II-Spring (June-2024)
https://www.gsssrjournal.com/Current-issues/9/2/2024

Scope
https://www.gsssrjournal.com/about-us/scope

Submission
https://humaglobe.com/index.php/gsssr/submissions

Google Scholar

Visit Us

Abstract

Pakistan has witnessed a very fast digit transformation. The present article explains how this new technology has affected economic activities, critical infrastructure management, and communication dynamics in Pakistan. Without a doubt, digital infrastructure provides a way for the communication and interaction, which are also increasingly being targeted by hackers, cybercriminals, state proxy and governments. Resolving these risks involves a multi-dimensional solution that includes technical, organizational, and legal remedies. Moreover, the interplay of cyber law and cybersecurity occupies a paramount position as regards the safety of personal, organizational, and national data that are often the target of growing cyber threats. Through the discussion of the developing context of cyber incidents and the significant role of the legal and security environment, the article focuses on the aforesaid issue, the lack of proactive measures that should be taken to combat cyber risks and safeguard the integrity of the digital world.

Keywords: Digital Information, Cyberattacks, Cybersecurity, Vulnerabilities, Legal Frameworks, Economic Activities, Critical Infrastructure, Communication Dynamics National Security

Authors:

Rana Zaheer ud din Ahmad: Advocate, High Court, Pakistan.
Mirza Shahid Rizwan Baig: (Corresponding Author) Assistant Professor, Department of Law, Government College University Faisalabad, Faisalabad, Punjab, Pakistan.
Email: shahidrizwan@gcuf.edu.pk

Pages: 43-54
DOI: 10.31703/gsssr.2024(IX-II).04
DOI link: https://dx.doi.org/10.31703/gsssr.2024(IX-I).04
Article link: http://www.gsssrjournal.com/article/A-b-c
Full-text Link: https://gsssrjournal.com/fulltext/
Pdf link: https://www.gsssrjournal.com/jadmin/Auther/31rvIolA2.pdf

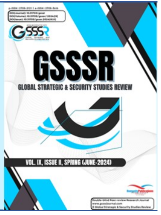
Humanity Publications (HumaPub)
www.humapub.com
Doi:https://dx.doi.org/10.31703

Citing this Article

04		**A Controversial Hypercritical Examination of Cybersecurity Policies in Pakistan that Cannot Be Ignored**						
		Author	Rana Zaheer ud din Ahmad Mirza Shahid Rizwan Baig	DOI	10.31703/gsssr.2024(IX-II).04			
Pages		43-54	Year	2024	Volume	IX	Issue	II
Referencing & Citing Styles	APA	Ahmad, R. Z. u. d., & Baig, M. S. R. (2024). A Controversial Hypercritical Examination of Cybersecurity Policies in Pakistan that Cannot Be Ignored. *Global Strategic & Security Studies Review*, *IX*(II), 43-54. https://doi.org/10.31703/gsssr.2024(IX-II).04						
	CHICAGO	Ahmad, Rana Zaheer ud din, and Mirza Shahid Rizwan Baig. 2024. "A Controversial Hypercritical Examination of Cybersecurity Policies in Pakistan that Cannot Be Ignored." *Global Strategic & Security Studies Review* IX (II):43-54. doi: 10.31703/gsssr.2024(IX-II).04.						
	HARVARD	AHMAD, R. Z. U. D. & BAIG, M. S. R. 2024. A Controversial Hypercritical Examination of Cybersecurity Policies in Pakistan that Cannot Be Ignored. *Global Strategic & Security Studies Review,* IX, 43-54.						
	MHRA	Ahmad, Rana Zaheer ud din, and Mirza Shahid Rizwan Baig. 2024. 'A Controversial Hypercritical Examination of Cybersecurity Policies in Pakistan that Cannot Be Ignored', *Global Strategic & Security Studies Review*, IX: 43-54.						
	MLA	Ahmad, Rana Zaheer ud din, and Mirza Shahid Rizwan Baig. "A Controversial Hypercritical Examination of Cybersecurity Policies in Pakistan That Cannot Be Ignored." *Global Strategic & Security Studies Review* IX.II (2024): 43-54. Print.						
	OXFORD	Ahmad, Rana Zaheer ud din and Baig, Mirza Shahid Rizwan (2024), 'A Controversial Hypercritical Examination of Cybersecurity Policies in Pakistan that Cannot Be Ignored', *Global Strategic & Security Studies Review,* IX (II), 43-54.						
	TURABIAN	Ahmad, Rana Zaheer ud din and Mirza Shahid Rizwan Baig. "A Controversial Hypercritical Examination of Cybersecurity Policies in Pakistan That Cannot Be Ignored." *Global Strategic & Security Studies Review* IX, no. II (2024): 43-54. https://dx.doi.org/10.31703/gsssr.2024(IX-II).04.						

e-ISSN:2708-3616 Volume: IX (2024) Issue: II-Spring (June-2024) p-ISSN:2708-2121

Global Strategic & Security Studies Review
www.gsssrjournal.com
DOI: http://dx.doi.org/10.31703/gsssr



Pages: 43-54 URL:https://doi.org/10.31703/gsssr.2024(IX-II).04 Doi: 10.31703/gsssr.2024(IX-II).04

Cite Us

Title

A Controversial Hypercritical Examination of Cybersecurity's Policies in Pakistan that Cannot Be Ignored

Contents

Abstract

Pakistan has witnessed a very fast digit transformation. The present article explains how this new technology has affected economic activities, critical infrastructure management, and communication dynamics in Pakistan. Without a doubt, digital infrastructure provides a way for the communication and interaction, which are also increasingly being targeted by hackers, cybercriminals, state proxy and governments. Resolving these risks involves a multi-dimensional solution that includes technical, organizational, and legal remedies. Moreover, the interplay of cyber law and cybersecurity occupies a paramount position as regards the safety of personal, organizational, and national data that are often the target of growing cyber threats. Through the discussion of the developing context of cyber incidents and the significant role of the legal and security environment, the article focuses on the aforesaid issue, the lack of proactive measures that should be taken to combat cyber risks and safeguard the integrity of the digital world.

Authors:

Rana Zaheer ud din Ahmad: Advocate, High Court, Pakistan.

Mirza Shahid Rizwan Baig: (Corresponding Author)
Assistant Professor, Department of Law, Government College University Faisalabad, Faisalabad, Punjab, Pakistan.
Email: shahidrizwan@gcuf.edu.pk

Keywords: Digital Information, Cyberattacks, Cybersecurity, Vulnerabilities, Legal Frameworks, Economic Activities, Critical Infrastructure, Communication Dynamics National Security

Introduction

As information technology becomes increasingly integral to daily life, Pakistan, like the rest of the world, is navigating a significant shift in communication and technology paradigms (Darwish & Lakhtaria, 2011). The uniqueness of the current information revolution in Pakistan isn't just about the advent of new technologies; rather, it's about the unparalleled capacity of these technologies to facilitate extensive global communication, enabling "one-to-many" and "many-to-many" interactions on an unprecedented scale (Hirtle & Raubal, 2013).

The digital information and communication infrastructure, underpinned by network technologies, has become ubiquitous, touching almost every aspect of life in Pakistan. With a significant portion of the population reliant on the internet for various economic, social, and political activities, cyberspace has become essential to modern existence. Predictions suggest that, within a few years, mobile broadband subscriptions will surge, reflecting a global trend that is mirrored in Pakistan. The proliferation of networked devices is set to redefine communication and social interaction, surpassing human numbers and altering traditional interaction concepts (Yusuf et al., 2013).

The influence of the Internet on changes in economic activities, critical infrastructure management, and communication is deep. Such connectivity also provides opportunities for Pakistan as it can now exchange information instantly without physical borders. Nonetheless, the current use of the internet far surpasses that of its original design which was meant for a small group of users and not the secure exchange of private information (Pătrașcu, 2021).

The design of the internet, which remains basically the same even though the applications got more diverse, as well as the anonymity feature make attacks on a scale that is never seen before possible. Pakistan dealt with complex targets for these attacks that brought diverse consequences and threats to customers, and industries, and created a government crisis. The worry of progressively complex cyberattacks is one fear since knowledge about such advanced methods of attacks gets more accessible and thus the barrier is lower for potential attackers (Lin et al., 2017).

In Pakistan, there is a task of dealing with weaknesses in technical, organizational, and legal system frameworks that are used by a variety of players ranging from criminal groups, hackers, state proxies, and governments. These weaknesses, accented by hyper-connectivity, are used for different purposes, for instance, obtaining commercial benefits and promotion of national interests. The discourse isn't about a new type of crime but about a transformation in interaction modes, resonating with historical academic debates on the social impact of technology. Just as the automobile once revolutionized societal norms, the internet today presents new opportunities and challenges, with cyber deviance emerging as a specific concern that national and international legal frameworks must adapt to address effectively (Rasheed et al., 2019).

In today's digital era, the significance of cyber-security and cyber law has escalated markedly, reflecting the deep integration of digital technologies into everyday life and the broader global economy. The substantial rise in internet users, along with the rapid digitalization of various sectors such as finance and healthcare, has underscored the critical role of cyber law and cyber-security in defending personal, organizational, and national interests. These legal and security frameworks establish crucial guidelines and protective measures against digital threats, governing online behavior, data protection, privacy, and intellectual property rights to shield individuals and systems from cybercrimes like hacking, identity theft, and unauthorized data breaches (Shandilya et al., 2024).

Cyber-security is a universal scope of strategies, technologies, and procedures meant to protect networks, devices, and data from cyber threats. In the other way, Cyber law is mostly intended to provide an official structure for lawful conduct online, as individuals, companies, and governments and to accommodate changes in order to address cybercrime, data leaks, and ethical usage of technology. The growing number of significant cyber incidents exposed the weak points in digital communications and the world witnessed huge financial losses, loss of trust in these communications, and ensuing concerns regarding national security (Lehto, 2013).

The main subject of this study is dealing with the development, adoption, and hurdles of cyber law and cybersecurity in Pakistan; however, within this context, different elements such as the geopolitics and the social-economic aspects will be analyzed as well, in order to highlight how these different aspects could influence the approach to the digital security and the legal governance in Pakistan. Cybersecurity strategies of Pakistan, USA, Canada, and Australia are the major concerns of this analysis for identifying the gaps and best practices. This can help to hone policies and laws related to cybersecurity (Newmeyer, 2014).

Pakistan being placed geographically in the whole of South Asia has to face some peculiar cyber-security problems which are directly related to the national security and the stability of the region. The nation's track of the expanding internet world, accompanied by high rates of internet usage, makes a huge difference in the development of the country's cyber law and security. As its strategic aim, the Pakistani Government is taking steps to strengthen cyber defenses including enacting legal frameworks, protecting the privacy of the data, ensuring integrity and institutions that help digital commerce and are also required for economic growth (Relia, 2015).

In summary, Pakistan's work to reinforce the cyber-security methods and frameworks overshadows the concluding phase of its digital trip, the reason which implies the necessity of a flexible, comprehensive approach that could help respond to the dynamic nature of cyber threats conveniently and acceptably and therefore clearly showed the necessity of digital safety and resilience.

Definition and Types of Cybersecurity

Cybersecurity comprises a holistic strategy that takes care of all computing devices, mobile units, servers, electronic systems, networks, and data irrespective of the form of attacks. It can be called cybersecurity, also known as information technology security or electronic information security. This field is applicable in a number of places, which include corporations, conflicts of interest, and mobile communications, to mention a few. It entails other minor areas (Perwej et al., 2021). Here are the following types:

- Network verifying Network defense is the provision of safeguards for networks from unauthorized access. This is done by trying to stop acts of targeted hackers among others. Its main aim is integrity, confidentiality, and information protection within Pakistan's cyber infrastructure.
- Software security Concentrates on safeguarding software and devices from potential hazards. If an application is breached, it might expose the very data it is intended to secure. Effective protection starts during the design phase, long before a software or device is implemented, which is a critical practice within Pakistan's technology landscape.
- Data security Data protection in Pakistan involves measures and practices designed to safeguard information from unauthorized access, disclosure, alteration, and destruction, ensuring the confidentiality, integrity, and availability of data within the country's digital and non-digital realms.
- Procedural security In Pakistan, operational security refers to the strategies and processes implemented to protect and manage essential operational procedures and sensitive data from unauthorized access or disclosure, ensuring the smooth and secure functioning of various sectors within the nation.
- Crisis recovery and organizational resilience In Pakistan, disaster recovery and business continuity refer to the systematic approach and strategic planning to ensure the resilience and swift restoration of operations and services in the face of disruptions or calamities, safeguarding the sustainability and stability of Pakistani businesses and organizations.
- User awareness training User training tackles the highly unpredictable element of cybersecurity human behavior. In Pakistan, individuals can inadvertently compromise a secure system by not adhering to robust security protocols. Educating individuals to avoid opening dubious email attachments, refrain from using unknown USB drives, and follow other critical security measures is essential for safeguarding any organization within the country.

Research Methodology

This paper offers a critical and perhaps contentious examination of cybersecurity policies in Pakistan. It takes a hypercritical approach, scrutinizing these policies and highlighting their shortcomings. The aim is to spark a much-needed discussion about potential weaknesses in Pakistan's cybersecurity defenses and advocate for necessary improvements.

Change of Digital Legislation and Cyber Security Techniques

The progression and refinement of cyber law and cyber-security policies reflect the dynamic and ever-evolving landscape of the digital domain. As technological advancements permeate every aspect of daily life and the global economy, the significance of these legal and protective measures has become increasingly paramount. The escalation in internet connectivity, alongside the digital transformation of key sectors such as finance and healthcare, has heightened the necessity for robust frameworks to shield personal, organizational, and national interests from cyber threats (Möller, 2023).

Cyber security involves various activities and measures, as well as technological solutions and procedures aimed at the protection of networks, devices, and data from cyber assaults. On the other side, cyber law is about stipulating the basic legislative requirements governing digital interactions and internet use, which are evolving as they embrace the complex issues facing cybercrime and ethics (Petrenko, 2022).

Primarily Pakistan situated in South Asia have it with complex cyber-security problems intertwined with national security issues and regional matters. While the country gets deeper into the digital realm against the emerging cyber law regulations and security parameters, the efforts to maneuver cyber defense and legal provisions are of great importance to reach a trusted, resilient, and secure digital future. The development of cyber law and cybersecurity in different countries shows the changing nature of this topic in which technological advances, cyber danger, and the legal framework implemented are trying to reach a balance. Such an exploration goes into the historical development and current state of cyber law and cyber security in Pakistan, highlighting significant changes and legal acts that helped to form the present cybersecurity environment in Pakistan (Malik, 2018).

At the time, Pakistan has many cyber incidents mostly from famous names, which shows that the country has many obstacles in the area of cybercrimes. Such events not only lead to serious social and legal consequences but also contribute to the constant development of cyber law enforcement for the state. This can be seen through the 2015 case of the Ax Act - a Pakistani IT company charged with a huge global diploma mill scheme that was extensively covered by foreign media and made evident the complexity of cyber fraud and its underlying challenges of prosecuting cross-border cyber crimes (Menon & Guan Siew, 2012).

Harassment on social media has been a reason for legal attention in Pakistan, with significant cases having a significant impact on the country's jurisprudence thereby establishing the significance of online harassment. For instance, a Lahore court´s decision to send a man to prison for cyberbullying and blackmailing a lady on Facebook occurred to be a landmark event in legal actions against online harassment. The financial sector has also come under the ambit of cybercrime with the number of ATM skimming attacks in the year 2018, evading the authorities through the clever use of international people. This event triggered a review of IT security dimensions applied in the national banking system. Another trademark case was the 2008 Sadia Mirza which was reported for cyberstalking through a dummy social media account, via the Electronic Transaction Ordinance 2002, leaving a legal framework for such cyber offenses (Shah, Zada, & Bibi, 2022).

Similarly, in the Lahore Bank hacking incident, Cybercriminals swiped a large amount of money by exploiting the loops in banking system security, emphasizing the issues of Pakistan's banking security system. Those examples just speak for the need for cyber laws, which are strong, effective, and form comprehensive guidelines for dealing with cybercrime (Ullah et al., 2015).

The vision of Pakistan in transforming its cyber law and cyber policy from the ETO of 2002 onward is meant for the authorized use of electronic media for communications and transactions. The Prevention of Electronic Crimes Act came into force in 2016 which further strengthened the cyber laws. Encompasses cyber terrorism and fraud with cyberstalking and spamming*. Additionally, it set out standards for the management of electronic evidence.

Execution of Cybersecurity Strategies

In Pakistan having an executable strategy for cybersecurity is evidence of an important stage in advancing toward a safe digital infrastructure in the course of changing cybersecurity threats. The present scenario in Pakistan illustrates an integrative approach to improve the country's cyber security defense that will help to overcome current obstacles and take advantage of future development.

The fundamentals of Pakistan's cybersecurity approach are integrated and enforcement of a rigorous set of policies to protect digital assets, maintain the privacy of citizens and make critical information infrastructure resilient. It embraces the strategic deployment of cutting-edge technological solutions, formulation of governance frameworks as well as the collaboration of public-private sectors on cybersecurity projects.

In Pakistan, the cyber security policy is implemented through an Act called the Prevention of Electronic Crimes Act (PECA), 2016, which is a legal framework meant to tackle cyber crimes in an efficient way. PECA provides for the provisions of mechanisms dealing with unauthorized access offenses, data breaches, cyberstalking, and other transgressions committed in the digital field, accordingly, law enforcement will be at liberty to enforce these laws and send a strong message to any potential criminals in the cyber world.

Besides, Pakistan uses all possible efforts to empower its cyber security architecture with dedicated institutions including national response centers like NR3C. Through this organization, agencies acquire major support for cybersecurity and can rely on its forensic expertise, incident response services, and coordinating efforts to handle cyber threats. The government also includes spreading such information to people as well as organizations. It emphasizes the fact that organizations and citizens should use the best tactics and measures to be safe. For example, Security training, cybersecurity awareness programs, and the integration of these principles in academic curricula are among the important initiatives that help foster a culture of cyber awareness and resilience.

Cyber diplomacy in Pakistan is developed with the support of international partners to exchange knowledge, upgrade technical capabilities, connect with efforts to align Pakistan's cybersecurity strategies and match the efforts with international best practices. This partnership promotes a comprehensive strategy for best safeguarding the country's interests in the sphere of cybersecurity because it is transnational and should be flexible and active in the global cybersecurity environment. In the context of Pakistan, the adoption of cybersecurity laws serves as evidence of the nation's preparation to stand up against threats to the cyber ecosystem in an ever-changing digital environment increasingly posing threats. Interaction of the governmental authorities and the private sector is the key success factor to hardening the cyberspace of the country, the reason why the strategy should be imagined as being the very milestone.

Main organizations of the country, such as the National Response Centre for Cyber Crime (NR3C) and Pakistan Telecommunication Authority (PTA) form the regulatory body for the information technology-related departments which therefore shape the cyber security of the country. NR3C deals with the issue of crimes that are based on cyber control and the improvement of investigative capabilities, while PTA controls the Internet and telecommunication services compliance with the cybersecurity codes. MoITT which is the main entity responsible for the formulation of IT and Cybersecurity strategy aligned with the national IT strategy which reflects a holistic approach to digital security.

Public-private partnerships, while not new, are gaining traction as an essential thing for the implementation of cybersecurity measures in Pakistan. The government's close cooperation with infotech companies and other international associations is intended to serve as a medium of knowledge management and also improvement of technology as a way of further strengthening the national cyber defense. Collaborations provide a win-win situation whereby knowledge base, resources, and expertise are mutually exchanged and used to shore up Pakistan's cybersecurity integrity.

The main drivers behind the closer partnerships in this context show a worldwide trend where the integration of private and public sectors' efforts is acknowledged as an essential element of cybersecurity. Cyber resilience is indeed not only about defending cyberspaces in Pakistan but also creating a culture of cyber awareness and enhancing the cyber security form for government institutions as well as private entities where they are well equipped to respond to the digital challenges in contemporary times.

The importance of working hard on the legal framework, the institutional capacity, and the overall collaboration which includes all actors of this ecosystem is the key to success to which Pakistan is currently dedicated. This complex strategy aims to build a classified resilient cybersecurity system capable of protecting the country's interests and citizens from cyberattacks and interacting with the Internet in all aspects. Globally, Pakistan is collaborating with different nations on their impetus on cybersecurity and aiming to match global standards. International cybersecurity dialogs and collaborations enable Pakistan to be resilient, fast and responsive, and in sync with the secure cyber-policies world trends and challenges.

The cybersecurity aspect has become increasingly important as more and more lives and jobs move online. Interestingly, Pakistan, specifically, is enduring some distinct difficulties in this area. The country faces resource deficits and a shortage of cybersecurity experts while cyberattacks are being raised every day with the examples of ransomware, phishing emails, and hacking victims. Conversely, there is good news as well and NCSA (National Cyber Security Authority – a body that oversees the creation of policies on cybersecurity and in the end, achieves international cooperation) came about only in 2020.

Pakistan's commitment to overcoming the fast-developing cyber threats is affirmed by its recent enforcement of a National Cyber Security Policy concerned with the creation of appropriate legal systems, technical measures, capacity building, awareness campaigns, and international cooperation. To further bolster its cybersecurity landscape, Pakistan must to further bolster its cybersecurity landscape by following measures:

Establish a strong national strategy on cyber security format having well-defined goals and collaboration models for relevant players that comprise the government, private sector, education, and civil society.

- Increase cybersecurity culture by conducting targeted education and training, making our people aware of evolving cyber threats for organizations.
- Foster public-private partnerships to draw them together and have them pool their expertise for the collective benefit of societal threats, giving a forum for shared threat intelligence and best practices.
- Invest in technology, which is an internal cybersecurity capability, and look for the formation of specialized groups, and generate competent human resources of cybersecurity experts as an outcome.
- Develop and enhance cyber laws and the policing structure to deal with cybercrimes we face so appropriately. Additionally, this should include updating existing laws in accordance with the evolving digital technology dynamics.

These tactics are the most crucial milestones for Pakistan to concrete its cyber security policy and eventually produce a private and strong digital village where national development and security are available to everyone.

Obstacles in Cyber Legislation and Information Security

In Pakistan, the cyber law and cyber security context involve many distinct challenges. The national journey to build a formidable cyber defense is hindered by a host of challenges ranging from legislative lapses to technical inadequacies, which entail far-reaching and comprehensive approaches.

Primarily, the legislative process of cyber law in Pakistan is still in development. While the PECA has brought lots of progress, it's still quite unclear how things like privacy and freedom of speech will be safeguarded. The very nature of cyber threats is that it is fluid, with continuous updates required for the laws to address them and defend against new and novel cyber threats.

The issue of the law enforcement of the existing cyber law is also crucial. Technology development is often faster than the speed for the legal system to implement the given laws precisely making a gap between the formulation of the policies and the enforcement of on-site implementation. Moreover, the absence of a specially trained workforce among law enforcement agencies leads to the problem of handling cybercrime well which is complex in nature.

Public awareness about cybersecurity and educating them are called the major challenges. A considerable percentage of the population is clueless about safe online practices which makes them vulnerable to cybercrime such as fishing, malware, and online scams. An awareness and understanding of cybersecurity and digital literacy across all levels of society is foundationally important for building a unitary defense against cyber threats.

To add to that, one of the challenges of Pakistani cybersecurity is its deficiency in developing a skilled workforce in that field. There is an urgent necessity for educational and training programs that will create a new breed of competence that will battle eventual cyber threats and infections. It is key to develop this human resource base to not only fend off cyber-attacks but also to have a quick response when they occur.

Nevertheless, international cooperation that needs to be enhanced is a key element of Pakistani cyber security strategy. Cybercriminals mostly operate across different nations, therefore there is a need to collaborate with other countries in order to have a secure information-sharing forum, best practices, and strategies to curb cybercrime.

Cyber law and cybersecurity issues make up the types of problems encountered by nations all over the world, as progress in technology as well as the nature of cyberspace (borderless) and of cyberspace itself (more complex and dangerous) are constantly evolving. The challenges can be global, but the others, contribute a bit to the nation's particular socio, political and cultural context. Oftentimes, a common problem is the fast rate of growth of technology which exceeds the statutory and regulatory structures in place, thus creating loopholes that technology-based criminals can penetrate and manipulate to attack users. International cooperation is one of the most important prerequisites, although global politics is ever-changing to be compounded by varying cyber powers Pakistan's policy actions for handling the challenges are emboldening digital literacy to raise public and organizational awareness of cyberspace and cyber-crimes. Boosting the capacity of legal and law enforcement institutions alongside the development of an explainable and coherent legal framework that can be effortlessly adjusted to suit the increasing change in technology is the last and equal concern.

The worsening situation of the National Cybersecurity Policy led to the recent release of the 'Pegasus scandal'. This led to the fast intensification of the situation on the one hand. So the situation turned its focus to the necessity of a comprehensive National Cybersecurity Policy. This process revealed an abuse of the software called Pegasus, which is a piece of highly ingenious spyware coming from the Israeli company NSO and allegedly licensed for fighting criminality. But the reality might be different: it has been reported that the software might be used as surveillance tools outside of the government's lawful purposes. Besides this, the prime minister of Pakistan, Imran Khan, and several other Pakistani individuals have been strikingly alleged to be among the targets of Pegaspy Spyware including India, a foremost client of the NSO. These concerns have brought up many issues for Pakistan.

This policy is a shift from how Pakistan has been dealing with its cybersecurity threats and constitutes a step further to the direction it was heading by introducing measures that are multi-dimensional including strong legal frameworks, a focus on building domestic expertise, and international partnerships in monitoring and protecting the cyber domain.

Role of the Masses

- In Pakistan, securitization, which means an exchange of views, puts an emphasis on the active involvement of citizens. However, the following challenge in this content is the poor correlation between the Pakistan population and the cybersecurity dialogue on the state level. Just to explain the danger of cyber-attacks as seriously as possible does not automatically equate to their securitization. The cybersecurity agency in charge should acknowledge the immediate and comprehensible nature of these measures and communicate the necessity to the citizens in a way that will boost the public support of necessary methods for cybersecurity.
- In the case of Pakistan, the effort of securitizing cyberspace often faces the challenge of the simplistic idea and the audience in this process is not thoroughly taken into account of. Cyber activities involve tension about whether cyber security is just an announcement from the authorities or an open-to-all two-way process. In some spots, securitization seems to be a mutual approach, however, in others, it is as simple as a definitive statement by the state. Pakistan's political and security establishments should realize the essence of merging such forces and bear the objective of strengthening cybersecurity policies.
- Cyber-related matters in Pakistan are usually addressed in terms of instructions given by authorities and in a rather traditional way without explaining the common subjective aspects of securitization. Such a process, which is rife with bureaucratic and traditional methods, misses an important feature of the participatory dimension of securitization thus

risking the legitimacy crisis of the governance of cyberspace. In that case, improve the process of securitization by making the dialogue more responsive and involved among the citizens about cybersecurity.

Media Depiction

- Over the last decade, electronic media has evolved as one of the vital entities and contributed substantially to shaping the views about threats to security within Pakistan. This medium reveals the diverse areas—psychological, economic, social, cultural, and political—where these cyber securitization narratives unfold. Apart from that, it is a channel for public interaction with stories that can shape public perception and influence reactions to cybersecurity activities.
- In view of the ongoing cybersecurity situation in Pakistan, the media's role swings by and by. During an "effects in the media discussion," the media itself becomes the audience's reaction. In opposition, "media effects" emphasize its positive or negative influence on cybersecurity initiatives. Herein lies a critical challenge: the media could possibly stress the problems like human rights violations and the investigation authority abuse overshadowing the principal elements of advanced cybersecurity.
- Apart from the fact that the cyber realm is a new area of security that the majority of people have barely any knowledge about, media framing has become a powerful strategic instrument. By using contextual framing, the Pakistani government and securitizing agencies can shape the narrative in their favor, emphasizing the benefits of cyber-security actions. This strategic communication focuses on obtaining support from different sectors of society, such as political antagonists, neutral entities, and human rights groups, by presenting expert and authoritative voices in the media. The key element here is to achieve a comprehensive agreement in Pakistan on the significance of cybersecurity measures.

Digitalization and Data Security

The broadband user base in Pakistan witnessed a significant surge, escalating from 7.7 million in 2014 (3.4% penetration) to 124 million by the 2021-22 period (56.0% penetration), as reported by the Pakistan Telecommunication Authority (PTA). Mobile internet constitutes the primary mode of online access, accounting for 54.6% of the total 56.0% penetration rate.

Despite the rapid digital expansion, awareness regarding cybersecurity remains limited. The 2020 Global Cybersecurity Index positioned Pakistan 79th among 194 nations globally, highlighting its susceptibility to cyber threats. Furthermore, in the 2023 World Internet Development Report, Pakistan was ranked 45th among 52 nations.

With Pakistan's digital transformation, particularly in essential services, the potential for cyber threats has increased. This is illustrated in the case of Islamabad which had a SCADA system for its water supply but was a victim of a breach by a Russian cyber-attacker. Into the story, Pakistan started using AI in healthcare with products such as Nayya Jee and made digital health platforms like Marham and Sehat Kahani.

This digital evolution has outstripped the capability of cybersecurity technologies, and now there is a gap where innovation is uncontrolled by impairments, and therefore assurances, on the other hand, cannot keep up. Many cybersecurity investments are made by the private sector, however, these are not accounted for nor monitored. The country is then solely relying on foreign expertise and technology for its cybersecurity. Cybercrime in Pakistan took a huge jump in which public institutions especially the National Database and Registration Authority (NADRA), were among the major victims. Banks, telecommunications, and the electricity sector also became the targets of cybercriminals.

For the sake of its strong digital infrastructure, Pakistan is directing its cyber protection program to a comprehensive cybersecurity policy which is much more profound than sectoral directions, and is embracing the Participant Society approach. This strategy is anchored on four main tenets: convincedness

prevention, legislative activities, and punishment, we can protect national network infrastructure from cyber criminals.

Pakistan: Computerized Evolution, Financial Advancement, and Cybersecurity Stance

Pakistani cyberspace can be seen in the area of challenging domestic and regional socio-political landscape as a battleground of cyber threats. The country's cyberspace is continuously growing and has new threats that are steadily increasing, including cyber-organized crime, cyber-espionage, and cyber-terrorism during the period of unrest among many regional countries Social media platforms are at the center of the attacks being carried out by perpetrators such as hacking, cyber bullying, and extortion as reported by the national cybercrime agencies. Also in 2015, Pakistan had a massive rise in malware attacks. Students in colleges and other individuals are often targets of such cyber-operators. Extremist groups spread their ideologies via the digital platforms.

The unemployment figures, mainly the young, boosted them to digital portals for employment with freelancing as a vital source of living. This is founded on the fact that Pakistan has a large youth population, many of whom have technical skills and thus provide the country with a prominent position in the ICT outsourcing industry which yields enormous revenue. The gig sector, which is mainly populated by the youth, plays an important part in the digital industry growth of Pakistan.

In view of the upsurge in cases of cyber threats and the importance of students in the economy, the need to sharpen cybersecurity awareness and practices cannot be overemphasized especially among students in higher learning institutions. This aspect is very critical to combatting cyberattack threats and ensuring the sustainable development of the digital economy of Pakistan.

During the last decade, behavioral cyber security studies have witnessed rapid development, a trend that shows concern for the academic sector. Research programs within tertiary institutions have shown active participation of students in risky online conduct; this is thought to be the characteristic of students when compared to academic and staff colleagues. For example, in a sample group of 385 students from the educational institution, they found students are the most vulnerable group when it comes to cybersecurity risks. Furthermore, other sources support the research - they demonstrate students' lack of discipline in cybersecurity behavior, and a lot of them for instance, demonstrate inadequate computer skills. Pakistan, like the rest of the world, is gravely affected by the current trend of ill fates where students are frequently exposed to diverse threats. For example, spikes in malware and cybercrimes cases were detected, and most of the cases involved students who were victims of various cyber-crimes. The flourishing digital economy in Pakistan which is exceptionally attracting the youth to come up with and utilize digital platforms, for purposes of employment, also clearly shows the invaluable nature of well-rooted cybersecurity awareness and education particularly in academic institutions.

While information regarding cybersecurity is available and easy to access, this gap is persistent between students' awareness and actual participation in cyber protection practices. This difference of perspective is a compelling reason why educational institutions ought to be more engaged in facilitating students' cybersecurity behaviors. Besides, it is of paramount importance that students are taught not only theoretical practice but also practical skills required in this digital era.

Armed Forces' Viewpoints on Digital Realm

The cyber security environment has developed and in a serious military sense, is utilized by armed forces worldwide, including Pakistan Forces, and as well that Pakistan's outlook has also taken the edge of cyber-attack. With the digital territory now placing itself at the center stage of modern warfare, we need to revamp our national security plans accordingly. With the country's level of digitalization getting deeper, there is an increasing challenge for the military to defend against intrusions originating in cyberspace and critical infrastructure.

Pakistani military considers cyberspace as a very essential domain where space intersects with national security; thus, this aspect has a massive role in shaping its cyber defenses. The military is increasingly concerned regarding the multifaceted nature of cyber threats. The range varies between cyber-espionage and cyber-terrorism. This tendency leads to the integration of both defensive and offensive capacities through a comprehensive approach.

There is a practice of cyber security within the boundaries of Pakistan's defense framework as well which is similar to the global trend as shown in the fellow countries' strategies through their strategic documents. Nonetheless, Pakistan's context differs due to the regional dynamics and domestic security concerns which directly there is impact their cyber defense posture. By far the greatest concern among the nation's military strategists is that cyber warfare extends way beyond the conventional frontlines, impairs every aspect of the communication system, and stays on a critical national infrastructure too.

Due to that, Pakistan is also improving its cyberwarfare capabilities and this phenomenon is in strict accordance with the trend of military use of cyberspace that has been registered widely everywhere. What is clear, though, is that the specific methodologies and internal processes are classified, however, the emphasis is evident on the development of cyber defense strategies, which lead to overcoming the imbalance of cyber threats, and the importance of bolstering cyberinfrastructure. Likewise, Pakistan remains analogous to other countries where military authorities are secretive about acquisitions of cyber offensive capabilities on the one hand but the strategic importance of such weapons being in their armory is agreed upon. In line with the assumption that cyberspace defense is also about the prevention of preliminary actions and retaliatory measures, thereby deterrence of potential cyber attackers.

Digital Diplomacy and E-Governance

Cyber diplomacy, usually perceived as just an extension of the diplomacy practice through the lens of the digital era, speaks highly regarding the leveraging of digital information technology into the diplomatic procedure. This development has vastly extended the area of diplomacy so that states can now also interact with the global population as well as each other. This has led to a new dimension added to international relations and policy-making.

It is known that among international strategies like the Netherlands' and Germany's, there is a clear focus on developing collaboration in cyber-related issues. The emphasis made on the collaborative efforts of all the actors in this regard clearly indicates how international organizations create a safe and secure cyber environment (many of them established, for instance, the UN, NATO, and the G-8).

At the very core of Internet governance, civilians and industries are basically involved directly with the Internet Architecture Board (IAB) and the Internet Engineering Task Force (IETF) being the key actors. Such multistate holder bodies, more inclined to civilians, reflect a shift to decentralization and to more participative internet governance of today.

Looking at the UK, the International Cyber Policy Unit demonstrates the resolve of the country to be an active participant in influencing global cyber rules and building cooperation. The UK's way of building a complete system of cyber laws internationally is different from France's which accentuates applying national legal frameworks while the cyber sphere evolves.

The United States, in its "International Strategy for Cyberspace", points out a vision that acknowledges cyberspace as a domain space that will require international collaboration. Joint U.S. strategy is noted for its focus on freedom of information, legal culture, and international cooperation, which further substantiates the strategic change from the previous, more domestically informed "National Strategy to Secure Cyber Space."

The Comparative Analysis

Peer comparison of cyber laws and cybersecurity policies among Pakistan, the USA, Canada, and Australia, which were tailored to the individual social and geographical features of the countries, reflects different ways. Although the uncovering strategies are in sight, the characterized constants are evident, namely the shared principles on how to deal with the worldwide problems caused by the emergence of technology and the need for global collaboration.

The peculiarity of the cybersecurity environment in Pakistan is the fact that it is conditioned by a certain sociopolitical situation and security threats emanating from the region. The state is no exception to the trend and has passed the Prevention of Electronic Crimes Act (PECA) which is geared toward quelling cybercrime. Nevertheless, the application of such laws is dead on its arrival owing to problems such as digital illiteracy and resource shortages. Improving digital capabilities and infrastructure is needed so badly that Pakistan may possibly address its cybersecurity issues in an efficient manner.

USA's discernible cyber-savvy infrastructure showers attention to all portals of cyberspace employment, and this method is apt in countering cyber threats strategically. The USA enjoying a high-tech background also utilizes contemporary security tools and cybersecurity techniques. The DHS and NSA, for instance, are some of the agencies mandated with the job of framing policies to direct security efforts while crafting best practices to minimize the perils of cyber-attacks. The United States' acknowledgment of cybersecurity is further portrayed by the existence of great research expenditures and the physical strengthening of the critical infrastructure (Aftab et al., 2022).

Canada's acts toward cybersecurity reveal the nation's norms of data protection which is the key feature of its democratic principles. With acts like the Personal Information Protection and Electronic Documents Act (PIPEDA) and a nationwide strategy on cybersecurity, Canadians express that they are willing to trade individual privacy rights as long as larger national security shows its face. The alignment to international tasks, like the GDPR, proves in no uncertain terms Canada's commitment to the interoperability of global cybersecurity.

Australia's cybersecurity policy is created in light of its geographical position in the Asia Pacific region towards addressing these regional geopolitical complications and new threats. The creation of the Australian Cyber Security Centre (ACSC) shows its commitment to the cyber resilience building of the country wherein the primary goal is the protection of critical infrastructure and national security. Legislation like the Assistance and Access Act in Australia has started debate about how the two sides, privacy and security, should be balanced, internationally (Dart & Ahmed, 2023).

Prompt Suggestions for Enhancement

Enhance Digital Proficiency: It is important that the government of Pakistan pays critical attention to the development of a digital literacy program, which will help the masses to understand cybercrimes and the laws associated with them. Consequently, the people will be able to know how to act when accidents happen and know their rights. The Government has a duty to form a cybersecurity strategy that not only cleans up but also plugs any gaps in existing laws such as the Prevention of Electronic Crimes Act (PECA) and legal frameworks. The strategy should accommodate the shielding of the relevant data across multiple sectors by including the protection of the relevant data in multiple sectors.

References

Aftab, R. M., Ijaz, M., Rehman, F., Ashfaq, A., Sharif, H., Riaz, N., Hussain, S., Arslan, M., & Maqsood, H. (2022). A Systematic Review on the Motivations of Cyber-Criminals and Their Attacking Policies. *3rd International Conference on Innovations in Computer Science & Software Engineering (ICONICS)*,. https://doi.org/10.1109/iconics56716.2022.10100569
Google Scholar Worldcat Fulltex

Darwish, A., & Lakhtaria, K. I. (2011). The impact of the new Web 2.0 technologies in communication, development, and revolutions of societies. *Journal of Advances in Information Technology*, 2(4). https://doi.org/10.4304/jait.2.4.204-216
Google Scholar Worldcat Fulltex

Hirtle, S. C., & Raubal, M. (2013). Many to many mobile maps. In *Lecture notes in geoinformation and cartography* (pp. 141–157). https://doi.org/10.1007/978-3-642-34359-9_8
Google Scholar Worldcat Fulltex

Lehto, M. (2013). The ways, means and ends in cyber security strategies. In *Proceedings of the 12th European Conference on Information Warfare and Security*.
Google Scholar Worldcat Fulltex

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on Internet of things: architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, *4*(5), 1125–1142. https://doi.org/10.1109/jiot.2017.2683200
Google Scholar Worldcat Fulltex

Malik, M. B. (2018). Architecture of cyberspace as an evolving security paradigm in South Asia: Pakistan-India cyber security strategy. *Institute of Regional Studies, Islamabad*, *36*(2), 3-35.
Google Scholar Worldcat Fulltex

Menon, S., & Siew, T. G. (2012). Key challenges in tackling economic and cyber crimes. *Journal of Money Laundering Control*, *15*(3), 243–256. https://doi.org/10.1108/13685201211238016
Google Scholar Worldcat Fulltex

Möller, D. P. F. (2023). Cybersecurity in digital transformation. In *Advances in information security* (pp. 1–70). https://doi.org/10.1007/978-3-031-26845-8_1
Google Scholar Worldcat Fulltex

Newmeyer, K. P. (2014). *Cybersecurity strategy in developing nations: A Jamaica case study* [Doctoral dissertation, Walden University]. Walden University Dissertations and Doctoral Studies.
Google Scholar Worldcat Fulltex

Pătrașcu, P. (2021). Emerging Technologies and National Security: The Impact of IoT in Critical Infrastructures Protection and Defence Sector. *Revista Academiei Forțelor Terestre*, *26*(4), 423–429. https://doi.org/10.2478/raft-2021-0055
Google Scholar Worldcat Fulltex

Perwej, D., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A Systematic Literature Review on the Cyber Security. *International Journal of Scientific Research and Management*, *9*(12), 669–710. https://doi.org/10.18535/ijsrm/v9i12.ec04
Google Scholar Worldcat Fulltex

Petrenko, S. (2022). *Cyber security innovation for the digital economy: A case study of the Russian Federation*. River Publishers.
Google Scholar Worldcat Fulltex

Rasheed, H., Hoellein, L., Bukhari, K. S., & Holzgrabe, U. (2019). Regulatory framework in Pakistan: situation analysis of medicine quality and future recommendations. *Journal of Pharmaceutical Policy and Practice*, *12*(1). https://doi.org/10.1186/s40545-019-0184-z
Google Scholar Worldcat Fulltex

Relia, S. (2015). *Cyber warfare: Its implications on national security*. Vij Books India Pvt Ltd.
Google Scholar Worldcat Fulltex

Shah, N., Zada, H., & Bibi, A. (2022). Harassment in the purview of Social Media: A Cross-Sectional Analysis of Youth in District Dir Lower. *Pakistan Languages and Humanities Review*, *6*(III). https://doi.org/10.47205/plhr.2022(6-iii)43
Google Scholar Worldcat Fulltex

Shandilya, S. K., Datta, A., Kartik, Y., & Nagar, A. (2024). Achieving Digital Resilience with Cybersecurity. In *EAI/Springer Innovations in Communication and Computing* (pp. 43–123). https://doi.org/10.1007/978-3-031-53290-0_2
Google Scholar Worldcat Fulltex

Ullah, S., Amir, M., Khan, M., Asmat, H., & Habib, K. (2015). Pakistan and cyber crimes: Problems and preventions. *First International Conference on Anti-Cybercrime (ICACC)*,. https://doi.org/10.1109/anti-cybercrime.2015.7351951
Google Scholar Worldcat Fulltex

Yusuf, H., Dragomir, M., Thompson, M., Watts, G., Chan, Y.-Y., & Nissen, C. S. (2013). *Mapping digital media: Pakistan*. Open Society Foundations.
Google Scholar Worldcat Fulltex