Journal of Climate and Community Development
A Double-Blind, Peer-Reviewed, HEC recognized Y-category Research Journal
E-ISSN: 3006-7855 P-ISSN: 3006-7847

A Thematic Analysis of Pakistan's Cybersecurity Policies, Regulations and Implications

Unzur Kaifa [1] **Dr. Zahid Yaseen** [2] **Dr. Muhammad Muzaffar** [3]

[1] M Phil Scholar, Department of Politics and International Relations, Government College Women University Sialkot, Punjab, Pakistan.

Email: unzurkaifa18@gmail.com

[2] Associate Professor, Associate Professor, Department of Politics and International Relations, Government College Women University Sialkot, Punjab, Pakistan.

Email: zahid.yaseen@gcwus.edu.pk

[3] Assistant Professor, Department of Politics and International Relations, Government College Women University Sialkot, Punjab, Pakistan.

Email: mmuzaffar.rps@gcwus.edu.pk

Corresponding Author: *unzurkaifa18@gmail.com*

Vol. *4,* ***Issue*** *1, 2025*

Article Information

Received:

2025-01-05

Revised:

2025-02-15

Accepted:

2025-03-20

ABSTRACT

Cybersecurity risks are growing, making strong legislative frameworks necessary to ensure adherence and protect digital infrastructures. Because of changing cyber threats, regulatory loopholes, and enforcement constraints, cybersecurity policy compliance in Pakistan continues to be a major concern. This study examines the existing cyber laws, their effectiveness, and capacity building in implementation, specifically in Pakistan. This study draws upon interviews with 15 respondents from different fields: Federal Investigation Agency (FIA) agents from the cyber unit, prosecutors from the criminal unit, and cyber victims. The purpose of the interviews was to delve into the respondents' views on the current cyber laws and their effectiveness. Analyzing the collected data from in-depth interviews applying thematic analysis while identifying key themes, for instance, the gaps in the victim's support mechanism and effectiveness in the existing legislative framework. The results highlight the dire need for significant modifications to address these challenges, for instance, public awareness campaigns, institutional capacity building, and technical expertise, and to provide significant new details about Pakistan's cybersecurity laws' inadequacies through providing policymakers essential details to strengthen legislative measures and prevent individuals from cyber threats.

Keywords: *Cybersecurity Legislation, Cyber Policies Implementation, Cyber Threats in Pakistan, PECA 2016, Digital Governance.*

Citation: APA

Kaifa, U., Yaseen, Z & Muzaffar, M. (2025). A thematic analysis of Pakistan's cybersecurity policies, regulations and implications, Journal of Climate and Community Development, 4(1), 39-54.

1. Introduction

This study addresses a major gap in the literature on cybersecurity governance by providing the first comprehensive thematic analysis of Pakistan's adherence to cybersecurity regulations. Previous studies examined at Pakistan's cybersecurity legislation and cybercrime rates (Bokhari, 2023) but limited scholarly attention has been paid to policy compliance, enforcement strategies, and stakeholder problems. Based on empirical data conducted interviews from Federal Investigation Agency (FIA) officers, Prosecutors and Cyber victims, this study analysis offers qualitative insights into the areas where policy enforcement is lacking. With digital change at the forefront of today's society, cybersecurity has emerged as a critical national security concern for governments globally (Awan, Memon, & Burfat, 2019). Strong regulatory frameworks are now necessary due to the increase in the frequency and complexity of cyberthreats, including ransomware attacks, data breaches, and cyber espionage (Kosseff, 2017). To safeguard their digital environment, several nations have implemented stringent cybersecurity laws and compliance procedures (Buzdugan & Capatana, 2022). Pakistan is rapidly transitioning to a digital economy and has implemented a number of cybersecurity laws, including the National Cyber Security Policy 2021 and the Prevention of Electronic Crimes Act (PECA) 2016. By defining institutional responsibilities, enforcement tactics, and legal frameworks, these initiatives aim to provide an environment that is secure online. It is yet unclear how effective these regulations are in terms of implementation and compliance (LJ Bikoko, Tchamba, & Ndubisi Okonta, 2019), though. Notwithstanding these legislative advancements, problems including regulatory fragmentation, insufficient enforcement, and a lack of institutional expertise still exist, casting doubt on Pakistan's overall cybersecurity resilience. Even if Pakistan's cybersecurity laws have advanced, there is still a substantial gap between the formulation of regulations (FlorCruz & Seu, 2014) and their practical implementation. Compliance with these cybersecurity regulations is hindered by several problems, including institutional inefficiencies, a lack of technological expertise, limited resources (Burns, Whitworth, & Thompson, 2004), and low public awareness. Furthermore, disparities in the way rules are applied across various organizations result from the absence of a unified cybersecurity governance structure. Globally, governments, international organizations, and multinational enterprises place an elevated priority on cybersecurity compliance (Abdullahi et al., 2022). Strict enforcement and compliance procedures are shown by regulatory frameworks such as China's Cybersecurity Law (Gallagher, Giles, Park, & Wang, 2015), the United States' Cybersecurity and Infrastructure Security Agency (CISA) standards (Bronk & Conklin, 2022). To enhance global digital security, organizations like the World Economic Forum (WEF), International Telecommunication Union (ITU), and United Nations (UN) advocate for standardized cybersecurity regulations (Lim & Taeihagh, 2018). However, due to financial, technological, and legal constraints, developing countries like Pakistan (Saleem et al., 2024) find it difficult to adopt these international practices.

2. Factors Influencing Cyber Security Policy Compliance in Pakistan:

This study examines the areas that require legislative changes and potential mediators to achieve cyber security in Pakistan by comparing Pakistan's cybersecurity compliance framework to international standards. It also considers the creation of a distinct entity to oversee and carry out cybersecurity measures. Increasing the technical expertise of law enforcement and IT professionals via training and capacity development; promoting information-sharing partnerships between governments, businesses, and international organizations; and inspiring individuals and organizations to adopt cybersecurity practices. By tackling these problems, Pakistan might strengthen its cybersecurity defenses and reduce the dangers of non-compliance. This study will offer a

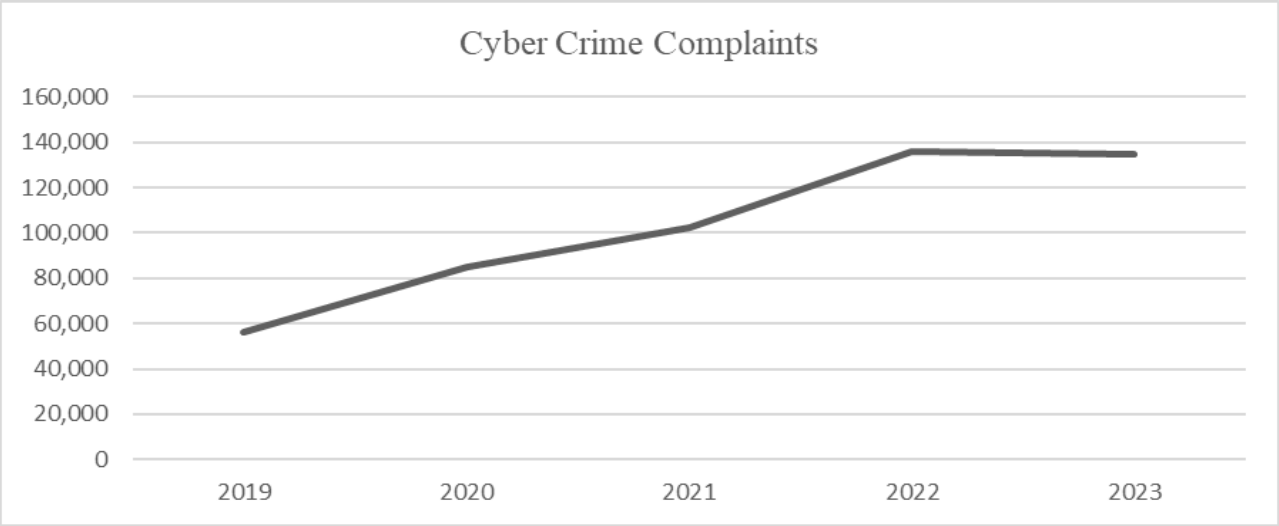
comprehensive thematic analysis to clarify the effectiveness of existing rules and pinpoint practical solutions for improved enforcement.

3. Existing Legislation Regarding Cyber security in Pakistan:

Table 1: *Source by Author, Legislative Measures Regarding Cyber Security in Pakistan.*

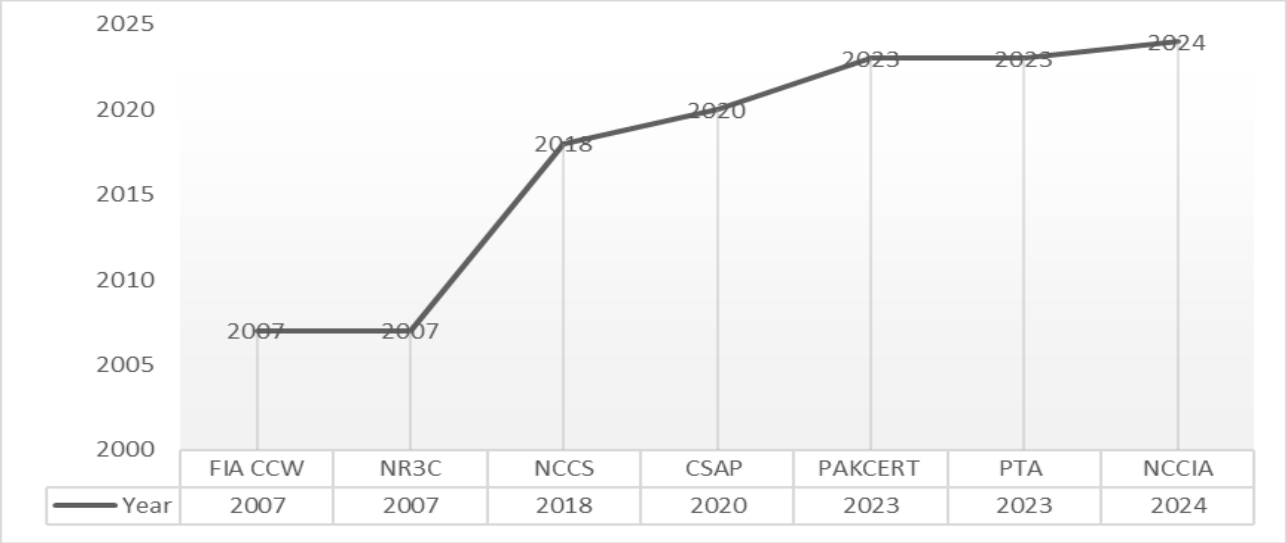
Laws	***Offences***	***Penalties***
Pakistan Telecommunication (Re-Organization) Act, 1996	Any contraventions against this Act, Ecommerce Fraud, Fabricated messages sent by means of other networks, Commit mischief	Imprisonment 3 years, fine 10 million or both, Monetary or mental loss will be paid to those who have suffered
Electronic Transaction Ordinance, 2002	Providing deceptive details, False certificate issue, Violation of personal data, Information system damage.	Imprisonment 7 years, fine 10 million and under this act all offences are non-billable
Electronic Crime Act 2004	Misuse of Devices, Offensive Messages, Digital false rumors, Identity theft	Fine, Imprisonment, Restitution and Probation
Payment Systems and Electronic Fund Transfers Act, 2007	Unauthorized Transactions, Fraudulent Monetary Activities, Manipulation of payment system	Fine which may extend to one million rupees, Suspension of licenses of an institution
The Prevention of Electronic Crime Ordinance Pakistan (2007)	Data interference, Cyber terrorism, Identity theft, Phishing, False and misleading information, Cyber stalking, electronic fraud, Invasion of privacy	Fine and imprisonment vary based on the nature and severity of crime
Prevention and Control Cyber Crime Ordinance Act (2009)	Proliferation of malware, Child pornography, Violation of privacy and many are mentioned under law (PECO 2007)	Fine and imprisonment vary based on the nature and severity of crime
Protection of Pakistan Ordinance Act (2014)	Information technology crimes, online terrorism and incitement, cyber harassment	Death sentence for Cyber terrorist attacks, lifetime prison on the severity of crime, up to ten years in prison for specific offenses
The Electronic Documents and Prevention of Cyber Crime Ordinance Act (2014)	Content offences, tempering with electronic evidence, spreading false information online, unauthorized access, cyber attacks	Fine and imprisonment on the severity of a crime
Prevention of Electronic Crimes Ordinance Act (2015)	Data interference, Malicious code, cyber bullying, Violation of copyright, spreading offensive content	Unauthorized access: 3 years' imprisonment Data misuse: 5 years and fine Cyber Terrorism: 14 years and fine Identity Theft: 7 years and fine Spreading false information: 5 years Child Pornography: Extreme severe penalties
Amendment of Electronic Crimes Ordinance Act (2016)	This law address mostly all crimes related to cyber like hate speech, harassment, digital sectarian miscommunication, child pornography and so many others	It depends on the nature and severity of a crime

Even having the legislation regarding cybersecurity there are still immense cybercrimes Pakistan's citizens dealing with. As the "Prevention of Electronic Crime Act (PECA)," passed in 2016, (Naseer & Amin, 2020) now governs cybercrime laws in Pakistan. Although this framework is more extensive than earlier laws, it does not address every aspect of cybercrime that is now practiced in Pakistan, and it frequently seems to be more thorough in theory. The majority of the literature on cybercrimes is up to 2019 (Imran, Murtiza, & Akbar, 2022), which is why these particular years were chosen to check the rate. In order to fully assess this, the study looked at how widespread cybercrime is in Pakistan (Rasool, 2015).



Graph 1: *Source by Author, Cyber Crime Rate in Pakistan 2019-2023*

Currently, there are several institutes and organizations in Pakistan which are currently dealing with the rapidly increase in cyber-crimes and have shown the effectiveness as well.



Graph 2: *Source by Author, Cyber Institutional Formation in Pakistan*

4. Material and Methods

This study's main goal is to investigate the exploration of cybersecurity legislations and implementations specifically in Pakistan. To analyze the data, a mono method approach and inductive Thematic analysis was applied which included the coding, patterns and themes for a deeper understanding of collected data. To collect the data, interviews were conducted for the better findings of this study.

4.1. Sample Size Selection:

Based on the profound understanding of the legislative and implementation process regarding cyber security the data was taken from three main distinct categories consisting of the sample size of 15 respondents, 5 from each group for the better evaluation of how society has been affected. Federal Investigation Agency (FIA) agents from Cyber unit, Prosecutors dealing with cybercrimes and Cyber victims were selected as samples for this study. The main goals were to evaluate the professional standard of the course material and determine the number of fundamental resources needed for cybersecurity experts.

4.2. Semi Structured Interviews:

Semi-structured interviews with FIA agents

from the cyber unit, prosecutors, and victims from Gujranwala and Sialkot, Pakistan, were part of the data collecting process for this study. This semi-structured interviewing methodology was selected since it is appropriate for this study and can be used to explore people's opinions (Barriball & While, 1994). Discussions on cyber security awareness, cyber laws, and the implications of cyber laws in Pakistan were covered in the semi-structured interviews.

The coordinators' insights into the curriculum's strengths and possible areas for improvement, as well as a detailed grasp of its complexities, were made possible by this qualitative approach. This study sought to produce prosperous and context-specific data that would aid in a more thorough examination of the cyber legislation and implementation impact on the competencies of future cybersecurity professionals by gathering firsthand information from FIA agent's Cyber unit, Prosecutors and victims. Semi-structured interviews methodology that entails creating an outline with subjects and inquiries. Nonetheless, the natural adaptability of semi-structured interviews made it easier to collect more thorough data. Although there was a set of leading questions, the interviewer was able to ask more complex and nuanced questions than those originally proposed through the participants' responses (Harrell, 2009).

The data collected was recorded during the procedure by taking notes and recording the discussion. Semi-structured interviews use a conversational approach with a single respondent at a time. They include a combination of open-ended and closed-ended inquiries, frequently complemented by follow-up inquiries such "why" or "how" (Adams, 2015). There are two primary reasons why semi-structured interviews were selected as the data collection method. First, they made it easier to probe for more details and clarification by enabling the examination of respondents' views and opinions on delicate and complicated subjects. Second, using a standardized interview was impractical due to the sample group's varied professional and victims.

The interviews for this study were conducted physically because it was more comfortable for the respondents, even if evidence suggests that respondents may show better interest and confidence in face-to-face interviews. In considering this, all interviews took place in the offices of prosecutors and FIA agents, but victims were given comfortable surroundings to ensure that there was some sense of in-person communication. Strong interpersonal skills are crucial for the interviewer to use interviews as a research method (Walsham, 2006). This aspect was very important throughout the study's interview phase. Before the recording started, it was made sure that participants were at ease with the interview being recorded.

4.3. Ethical Considerations:

Qualitative research examines the intimate experiences and viewpoints of individuals; ethical considerations are intricately entwined with the study. This transition from private to public domain emphasizes the necessity of giving careful thought to and openly sharing personal thoughts with study readers (Brinkmann & Kvale, 2005). The ability to guarantee the appropriate development of research methods and practices is the justification for incorporating ethical considerations (Recker, 2021). Concerns about informed consent and confidentiality are among the ethical issues that come up in qualitative research (Corti, Day, & Backhouse, 2000). These issues must be addressed since qualitative data frequently produces vivid, memorable statements, pictures, and narratives that could jeopardize the privacy of personal information. Furthermore, anonymity and the possible effects and harm to participants are considered (Sanjari, Bahramnezhad, Fomani, Shoghi, & Cheraghi, 2014).

Confidentiality was given top priority in this study to allay these concerns, particularly considering that there are only 15 respondents accessible for interviews with all possible participants. Prior to and during the interviews, participants received information about the value of confidentiality. To preserve anonymity, this study does not reveal

identifying information such respondent names or professional status. Ethical considerations were continuously given top priority during the research process to foresee and resolve any associated problems (Roig, 2006).

4.4. Data Analysis:

After the interviews, the discussions were transcribed as part of the data collection process. To facilitate the data analysis that follows, transcription is the process of turning oral contents such as recorded interviews into text (Kvale, 2012). Writing facilitates the evaluation of possible meaning connections and the clarification of interconnections (Galletta & Cross, 2013). Additionally, a variety of recording equipment was used during the transcription process. This method made sure that no details were overlooked while transcribing. Interpreting what is seen or heard and using background knowledge to decipher its meaning are crucial steps in the analysis of qualitative data. If a participant calls a program "wicked," for example, is this a sign of severe displeasure or passionate approval? Furthermore, considering elements like the participant's age can reveal information about the desired significance of their assertion. Recalling the emotional tone of the interviews is also seen to be essential for the analyzing process. This was made easier by recording the interviewees' perceptions and introspective thoughts for future use.

5. Results and Discussion

5.1. Mapping Courses of FIA agents and Prosecutors from Cyber Unit:

Interviewed FIA agents from cyber units were asked to provide a description of the highlighting a critical gap in public understanding of cybersecurity threats and reporting mechanisms. They were asked to explain whether and how Pakistani public awareness could be raised, as well as potential strategies.

5.2. Limited Public Awareness and Education:

This theme emerges strongly across all interviews, highlighting a critical gap in public understanding of cybersecurity threats and reporting mechanisms. The finding from the interview data regarding cyber awareness and campaigns for cyber enhancement indicated that there is a lack of awareness in our society about cyber security threats. Regarding the cyber campaigns, most of the respondents proposed that they take advantage of existing platforms, such as schools, colleges, universities, and other radio stations, such as FM radio stations, to raise awareness. This way, the public will be made aware of the issue and will be able to avoid it. And there ought to be a subject for that, one that is taught, as well as frequent campaigns to raise public awareness of the crimes that are occurring in today's society and the strategies that are being used to combat them.

> *"Cybercrime, people are not aware of it. People still go to the police station to report cybercrime. Because there has not been a briefing about it yet. People are not aware of it." - FIA Agent 2*

Additionally, they said, "We have seen numerous instances where students are easily victimized because they are unaware of these things." From their Facebook or WhatsApp profiles to sexual harassment and their financial scams, which we might refer them as electronic scams. Mostly the victims are those who lack education and are impoverished.

> *"It should be made compulsory for our educational institutes, there should be a subject for that, because students are mostly victimized as they lack awareness so they should be taught and there should be regular campaigns regarding awareness among the masses" - FIA Agent 4*

Prosecutors, on the other hand, frequently highlight the fact that there is a significant lack of awareness regarding cyber security in Pakistani society. They say that some cases are related to cybercrime and the Anti-Terrorism Act, but people are unaware of this special law, which has been introduced and laid, which is why people haven't read it yet,

its knowledge hasn't been shared, and no information has been given to anyone. Additionally, those who use social media and the internet are not aware of their security as well.

> *"The locality does not know very well about cybercrimes. Most of the people are reluctant to file an application against the culprits because of family honor at stake." - Prosecutor 4*

As prosecutors suggested, different methods could be adopted for raising awareness like introducing campaigns in educational institutes, seminars and workshops. Informing someone when there will be restrictions or promotions indicates that there are many ways to implement the law, including imposing restrictions, raising awareness through pamphlets, and incorporating it into education. However, the concern is that this is a special law. By starting the student digital competition, we can continue to improve it. Participants in the competition will at least be aware of the benefits and drawbacks of the internet.

> *"I think it is not common in our society yet. People just scroll the videos and use it for entertainment. There is a dire need to educate the people, especially in our region and more especially in Pakistan. And the related law, even the lawyers don't know about this law, because its practice is very less." - Prosecutor 1*

As the FIA agents and prosecutors collectively posed that there is no awareness of cybersecurity in society. And we cannot only blame the legislative process for it, as if there are legislation, then the practical implementation and adaptation of those policies and laws matter, which is not possible until people are acknowledged about it. Awareness can harness the utilization of existing laws and regulations.

5.3. Resource Constraints and Implementation Challenges

This theme discusses the operational difficulties that Pakistani cybersecurity enforcement has, especially with relation to infrastructure and personnel. Most agents recommended that we secure our communication system. Undoubtedly, the Pakistan Telecommunication Authority and FIA are among the institutions in Pakistan that are also carrying out the laws that the government has created. Therefore, it makes a significant difference if the information is not protected. Safeguarding the information will make it extremely easy for everyone. People's confidence in utilizing a secure network and protecting their privacy and identity will increase as a result. As a result, they will receive significantly higher compensation.

> *"We have very few resources, we don't have a number of cybercrime stations, we need more stations like one in Gujranwala, one of our stations deals with multiple cities, whereas it should be separate in every district" - FIA Agent 3*

According to other agents, there are still nearly 2,000 incidents pertaining to cyber security issues from 2020. Legislation or a lack of funding may be the cause at times, but not generally; instead, it is the workload that each investigating officer must handle. More investigative officers must be employed by the government to guarantee prompt work. Even with the availability of assets, advanced technology, and institutional capacity building to implement regulations, they won't be effective until society is more conscious of cyber security.

> *"All we need is more hiring, more workforce. Because I was just reading the report of United Kingdom police report, which they said that an inspector or some detective must need to focus only on 10 to 15 cases" - FIA Agent 1*

As the Prosecutors didn’t have a distinct stance from FIA agents, they state that the level of the laws we have passed is really significant, but the implementation is crucial, though. There is no implementation, yet our implementation class is present. Although we have many amenities, they are not being used.

There are explanations for that. The organizations that uphold them are understaffed and underfunded. They lack the technology necessary to track them down. The fact that we have a statute that states, "They say, delay defeats justice," is what matters most. Our laws are being enforced, but it takes so long to get a decision that both the effectors and the complaint are dissatisfied. Although the laws are in place, the implementation must be improved.

> *"We have a lot of facilities, but they are not implemented. There are reasons for that. I have understood that our institutions that enforce them have a lack of workforce and resources. They don't have the technologies to trace them." - Prosecutor 2*

> *"They might have introduced a separate organization for cyber-R&D or a separate unit to deal with it, but the thing is human resource is same and professional expertise level is same so until Pakistan won't improve the expertise and other related things, there won't be benefits for the society." - Prosecutor 5*

5.4. Digital Economy and Security Interface:

This theme explores the relationship between cybersecurity measures and Pakistan's economic growth, particularly in the digital sphere. As most of the FIA agents suggested that the absence of laws, particularly in Pakistan, was a prevalent view regarding the internet economy. Since COVID, however, the digital economy has been booming. Online enterprises are attracting a lot of individuals. And for that reason, Pakistan is receiving a lot of foreign exchange. However, we still have less potential. Our generation grows with the size of the nation. We have very little proportion in that regard. We're still discussing $1 billion and $2 billion. India reached $100 billion last year. We must continue to work on the laws that we have already created. And specifically, to add one more law pertaining to cryptocurrencies. Particularly in our laws, we need to address this cryptocurrency, Bitcoin, and internet investing. I would suggest that this is one of the primary causes of data breaches, cyberbullying, and online frauds. You believe that Bitcoin is an informal economy and that it would benefit Pakistan's economy. Additionally, we must enact regulations to appropriately collect taxes from those investments to legalize the introduction of cryptocurrencies, including Bitcoin, into the tax market. This will undoubtedly benefit Pakistan's economy.

> *"Especially in Pakistan, after COVID, the digital economy has been uprising. A lot of people are getting involved in it. And that's why a lot of foreign exchange is coming to Pakistan. However, our ability to handle the risks posed by foreign exchange is still inadequate." - FIA Agent 3*

Since the other respondent suggested legislation that may improve Pakistan's cyber security:

> *"We need to work on the previous laws, the laws which we have already made. And I just wanted to add one more piece of legislation, especially regarding cryptocurrency. We must cover this cryptocurrency, Bitcoin, and this online investment, especially in our legislation" - FIA Agent 5*

The persistent problems are shared by most prosecutors. Significant foreign investment is essential to strengthening the Pakistani economy, but instead of offering them the opportunity to work together, the Pakistani government is not even trying to promote the country's present legislation. Foreign investors are unlikely to consider a state as worth investing in if it does not safeguard the public interest. The incapacity of the institutions to develop capacity for progress is the cause of this. The government should provide incentives that draw people's attention so they can utilize the digital economy. However, FBR has started charging 1 rupee (PKR) for each online transaction or

purchase rather than offering incentives to the public. It's not about 1 rupee; instead of altering the user's attitude regarding online transactions, FBR taxes them for using them. This way, the usage will become widespread, and awareness will be raised until the public stops using it. For the user, it is regarded as a financial loss.

> *"Cyber Security Committee are affecting our dependence on foreign investment. Foreign investors look at the situation in their own countries. They see that there is no safety, there is no implementation of the laws. their capital is not saved, so the investment decreases." - Prosecutor 2*

The government's participation is crucial, as few Prosecutors indicating that, if the judiciary can follow instructions and shut down other cases, then there need to be a deadline of one month for the case's resolution. Additionally, it will be quicker, people will feel more secure, and it may be enhanced if the appeal is resolved within a year. Public trust will decline the more they exaggerate the need for resolve. To assist us to wrap up the matter as quickly as possible, the police should be involved. People will become less confident if a case is heard in court and the proceedings are delayed so instead of using the digital economy their stance will automatically divert towards the use of cash. Rather than to legalize the use of bitcoin and cryptocurrencies they have banned it, to secure the foreigner fraud and theft.

> *"PECA 2016 criminalizes the digital foreign currency which is Bitcoin and cryptocurrency. If Pakistan legalized the use of bitcoin and cryptocurrency it can help to stable the Pakistan's economy" - Prosecutor 3*

5.5. International Collaboration and Technological Gap:

This theme emphasizes the necessity for international cooperation as well as Pakistan's cybersecurity stance in comparison to developed countries. Most agents held the opinion that Pakistan was accepting more assistance for various platforms, such as signing agreements with foreign nations to strengthen the economy. However, there aren't many initiatives pertaining to cyber security, but if Pakistan concentrates on cyber issues, working with other nations might greatly benefit us. Because they are far more technologically advanced than developing states, advanced states can even access the personal information of Pakistani citizens through social media and banking because these states are far ahead from us in technology and also as we use their platform Facebook, WhatsApp and other social media apps we don't have our initiative, so this is how developed countries have access to our national affairs to individual affair. Although they can embrace the ideas, Pakistan has not been able to satisfy their technological standards.

> *"Pakistan has just joined this field. The other countries like UK, USA, India and China are very far ahead. They have people from our area which we call brain drain they use our manpower but still the resources and technology they have we cannot meet that so still they are far ahead of us" - FIA Agent 3*

As international collaboration can show significant impact in any state's affairs, as Pakistan is far behind in this specific field some prosecutors suggesting that, international institutions with a focus on cyberspace should exist to offer support and help cease the cyberwar between states. Since only MOUs between states or international organizational collaboration can offer such assistance, Pakistan PECA 2016 does not offer the kind of security that would ensure that, in the event of an international cyber security incident, PECA would at least prevent it at the national level in Pakistan.

> *"States should collaborate on international level as recently Israel pager attacked on Lebanon is a cyber-attack which can further convert into cyber war. So, to stop*

this kind of international attacks countries should collaborate to stop such attacks just like UNO assists with global peace" - Prosecutor 5

"*We should contact the foreign institutions for collaboration so that they could train our youth and introduce such training sessions. I haven't experienced it yet but yes in our prosecution circle through UNODC they are providing us with training and adding cyber security as a subject. Other than this I have not witnessed other than this institution to work on cyber security" - Prosecutor 2*

5.6. Legislative Framework and Enforcement:

This theme discusses the effectiveness of cybersecurity laws as they are currently being implemented. There is a lot of work being done on this, both in terms of legislation and implementation, according to the most responsive agents. However, that is insufficient. Furthermore, legislation alone will not resolve this issue. People awareness is required for this. Because the likelihood of someone being detained will decrease if you can raise awareness with a single button, particularly in the case of cybercrime. The lack of bonding between these institutions and the public is the ultimate barrier.

"It is not like there is a lack of legislation. Public confidence in online transactions and service is impacted by implementation cyber security legislation. Due to the lack of awareness people are having hurdles in reporting the cases" - FIA Agent 1

"PECA 2016 is specifically to cover cyber-crimes and of course it is prioritizing victim prevention, but law itself cannot secure the victim but how it is practically functioning matters" - FIA Agent 2

Either additional legislation is required, or Pakistan's cyber security may be improved only by implementation efforts. Few prosecutors have disclosed the areas in which issues have arisen. When the initial procedures are functioning effectively, more steps should be taken. Because new policies are introduced and practically implemented by the government that takes power in Pakistan, but the policies also change when a new administration takes over. Sometimes there is no responsibility, and other times they are not taken into consideration. The problem with Pakistan's government changes is that their policies should remain active, much like the UK's policies have remained consistent despite having two or three prime ministers in the previous two years.

"According to my knowledge, the legislation is limited to only PECA 2016. They are not further working on it when there is a must need to revise the law or add additional measures in the law to cover the new emerging threats in society." - Prosecutor 3

My view is that the government should do it, but the judiciary can do more. They have no such risk; their tenure is fixed. and after the case is filed, everything is handled by them and there is an acquisition of evidence in this concept, and it needs to be loosened a little so that even if there are some contradictions the punishment and conviction of someone can be done so that the complainant is satisfied. Starting at the very beginning, steps must be taken to raise awareness, such as updating the curriculum for students rather than teaching them unstructured subjects that don't address current trends.

"PECA might be verbally providing protection to victims but there is no implementation of this law because to make the laws is not a problem but not implementing them is the problem." - Prosecutor 1

5.7. Mapping Courses of Cyber Victims:

The victims' experiences with cybercrime and their encounters with law enforcement were examined using a reflective thematic analysis, with a focus on the type of cyber incident that

led to their entrapment. This reflects the new cyber threats that society is facing. Economic cyber theft is the most common type of fraud that victims in Pakistan encounter. Because they may be discouraged from coming forward to report the crime by criticism and ridicule, victims of online harassment typically do not file a complaint. It's possible that law enforcement agencies lack the expertise and capacity to handle the registered reports in an efficient manner. Victims may lose faith in the institutional handling of their cases as a result, believing that their claims are not being given due consideration. According to the victims, although there are many laws in existence, they are not always enforced. Insufficient resources and systemic issues may cause people to lose their confidence in the judicial system.

5.8. Lack of Cyber Security Awareness:

Most of the victims' opinions on society's awareness of cyber threats are not strongly held:

> *"There is no awareness about cyber security in Pakistan. It is just limited to a scrolling world. It is moving rapidly towards a technological area. But Pakistan is not able to cope with new emerging threats." (Victim 1)*

With the world going digital, Pakistan is confronting a new era of cyberthreats. As few victims suggested that comprehensive seminars and awareness programs are needed to not only acknowledge the use of emerging technology but also to raise awareness about how to handle situations where victims are experiencing such incidents, who to contact in time for assistance, and how to use online portals for beneficial purposes.

> *"I think there is not enough awareness because people are afraid of going to the cyber security offices. They are just reluctant because they think that officers will not cooperate. Neither are they conducting such seminars or awareness programs so that people have awareness of how to report them and how to respond on time to the officials of the cybersecurity center." (victim 3)*

5.9. Sophisticated Fraud Techniques:

According to the interviews, scammers deploy advanced impersonation and social engineering strategies to look authentic. Most victims have reported experiencing economic fraud as part of their encounters with cyber theft. Sometimes a phishing call is made by someone close to them, requesting money to be sent to them, or they receive a professional call asking them to reveal the code to confirm their banking information. Economical frauds may be reported, but harassment cases are typically not since families prefer to remain quiet because they fear that their dignity will be compromised. Every other day, they visit the offices to check on the status of their reported cases because, until they are truly checking, they will receive a response from the officers, either positive or negative, but if they don't, there won't be any response at all.

“He was providing details like his name, date of birth, and CNIC number. He was well-informed. He was aware already. Therefore, it gets confused when he provides too much information. They ensnared me in a situation where they produced a phone ambiance, such as a ringing office phone and voices coming from behind. It resembled an office setting exactly." (Sadia)

5.10. Institutional Response Challenges:

The challenges victims have when requested assistance from cybersecurity and law enforcement agencies are encapsulated by this issue. The discussion emphasizes the steps victims had to take and how they reported to the FIA cyber unit. Even after several months, most victims stated that their issue has not been remedied. Victims are urged to permit a little longer after speaking with FIA agents, and even then, it appears that their report is disregarded.

> *"I filed a complaint against the scammers in Gujranwala FIA cyber unit office, the officers called me and told me that they will solve the case in 45 days but after 45 days, they*

closed my complaint. it's been 7 to 8 months, but my complaint is still pending, nothing has been done about it yet" (Victim 2)

According to some victims' online reports, there are several online portals that victims may use to conveniently file their reports. However, victims have complained that they have not received any response even after using these portals, thus it was suggested that these portals be functional. Online portals are also readily available. Therefore, to assist victims and effectives, these online resources need to be responsive and active.

"I emailed them several times, but I got no response. Also, I gave them a call several times on their helpline as well. They didn't even response me the call just got connected and the computer and the voicemail are saying please wait on the line" (Victim 5)

5.11. Regional Access Barriers:

The analysis shows how victims face more difficulties when they have physical distance from cybercrime units. Geographical access is one of the victims' primary issues. Because there are only four cybercrime wings in the Lahore zone—Gujranwala, Islamabad, Multan, and Lahore itself, victims in some areas have difficulty contacting authorities for help, as most victims showed. As a result, victims must travel far to physically register the report, which causes issues for those who have jobs. These online organizations are unable to resolve the victim's issues, which makes it challenging for the victim to pursue justice, even after overcoming such geographical obstacles.

"It is a very hectic process. We have spent a lot of time and money. And we have also incurred a financial loss because we have to travel from Sialkot to Gujranwala. I feel that the FIA should be in Sialkot so that the victims from Sialkot or nearby rural areas can go there easily to get their complaints processed as soon as possible" (Victim 5)

"For me it was convenient to go their cyber security office because it was near my home, but it is not it is not convenient for everyone I think that there should be fast services and separate office in every city" (Victim 3)

This analysis reveals significant systemic issues in Pakistan's cybersecurity infrastructure, from public awareness to institutional response capabilities. The experiences of these victims highlight the need for more accessible services, improved response times, and better public education about cyber threats. The contrast between victim 3, successful case resolution and the ongoing struggles of other victims suggests inconsistency in how cases are handled, pointing to the need for standardized procedures and more efficient processing of cybercrime complaints.

6. Validity and Reliability

A variety of techniques were used in this study to guarantee a precise answer to the research topic. Although combining different methodologies and interpretative methods may not directly increase validity, there is growing evidence that doing so can greatly increase the breadth and depth of understanding, (Fielding, 2001). As a result, successfully integrating approaches requires a thorough comprehension of the validity risks included in the combined approaches. Mixed methodologies necessitate a well-considered research design and a clear justification to lessen these risks. Stated differently, it is essential to explain why this method was considered preferable to a mono-method approach. Several important considerations impacted the choice to use a mixed methods approach in this study. First, frameworks improve consistency by providing an organized way to arrange data and make analysis easier. in interpretation (Dupin & Borglin, 2020). Second, the integration of various data sources may result in the collection of information from a variety of professionals and victims for cybersecurity content. Conducting semi-structured interviews required a thorough

comprehension of the study landscape in advance, allowing for more targeted inquiry and in-depth investigation of important topics (Grant & Osanloo, 2014).

Integration is used when the inquiries need to be addressed and the facts available are readily comprehended, (Brazhnik & Jones, 2007). A systematic approach was used to validate this portion of the study, and a framework-based approach to analysis was used to improve validity. To provide a thorough overview and support the study's validity, a three-step process comprising elicitation, reduction, and visualization is used (Romano Jr, Donovan, Chen, & Nunamaker Jr, 2003). The cyber security professionals, especially FIA agents and Prosecutors served as the primary means of defining and validating the findings and data collection procedure.

7. Findings

In order to handle the growing cyberthreats in Pakistan, this study has evaluated the efficacy of the implementation processes and ascertain whether further legislation is required. Although 15 protocols were developed to help address the gaps in Pakistan's legislative process or execution, victims were not specifically targeted by these protocols because unstructured interview was conducted from victims. The victims explained the kind of cybercrime they came across and how they informed the FIA cyber unit about it. The study's conclusions show how well policies designed to counteract cyberthreats may be implemented in practice and adjusted accordingly.

8. Conclusion

In a time when digital threats are continually evolving, Pakistan’s efforts to legislate more efficient cyber laws and execution have become more important. As the major challenges Pakistan is facing are a lack of awareness in the public, inefficient capacity building, unskilled professionals, no accountability, a lack of resources for enforcement, and so many more. The most recent cyber law that exists is PECA 2016, and it has covered most of the cyber infrastructure compared to the previous laws, for instance, the Electronic Transaction Ordinance, 2002, and the Electronic Crime Act 2004. Still, there is a need to annex the PECA 2016 with the ongoing cyber threats to provide accountability to the public through implementation. Despite the existence of cyber laws, the effectiveness of their implementation is still uncertain because the entities that facilitate them lack the training about new technologies and coordination. Initiatives to strengthen cybersecurity concerns should be uncompromising while facilitating the entities with training sessions and seminars on cybersecurity and threats, and for the public, Additionally, public awareness campaigns about cyber security must begin, possibly starting with a curriculum since student awareness is crucial to securing Pakistan's future. Because until the public is not aware of the threats, the organizational work cannot be understandable for them. Pakistan must enhance the policy making and implication enforcement in organizations like the "National Cyber Coordination Center" in addition to increasing its professional expertise in the area to improve cooperation between defense and civil organizations. Better law enforcement agency collaboration will therefore result in stricter cybersecurity policy implementation, enhancing Pakistan's cybersecurity environment.

9. Recommendations

- There should be formulation of thorough cybersecurity regulations, measures to enhance law enforcement's competence, and proactive cooperation with the corporate sector. Legislation or a lack of funding may be the cause at times, but not generally; instead, it is the workload that each investigating officer must handle. More investigative officers must be employed by the government to guarantee prompt work. Even with the availability of assets, advanced technology, and institutional capacity building to implement regulations, they won't be effective until society is more conscious of cyber security.

- Regarding the cyber campaigns, most of the respondents proposed that we take advantage of existing platforms, such as schools, colleges, universities, and other radio stations, such as FM radio stations, to raise awareness. This way, the public will be made aware of the issue and will be able to avoid it. And there ought to be a subject for that, one that is taught, as well as frequent campaigns to raise public awareness of the crimes that are occurring in today's society and the strategies that are being used to combat them.
- Pakistan was accepting more assistance for various platforms, such as signing agreements with foreign nations to strengthen the economy. However, there aren't many initiatives pertaining to cyber security, but if Pakistan concentrates on cyber issues, working with other nations might greatly benefit us. Because they are far more technologically advanced than developing states. The digital economy has been booming. Online enterprises are attracting a lot of individuals. And for that reason, Pakistan is receiving a lot of foreign exchange. However, we still have less potential. Pakistan must continue to work on the laws that we have already created. And specifically, to add one more law pertaining to cryptocurrencies. Particularly in our laws, we need to address this cryptocurrency, Bitcoin, and internet investing that this is one of the primary causes of data breaches, cyberbullying, and online frauds. Bitcoin is an informal economy and that it would benefit Pakistan's economy while collaborating with other countries.
- Geographical access is one of the victims' primary issues. Because there are only four cybercrime wings in the Lahore zone Gujranwala, Islamabad, Multan, and Lahore itself, victims in some areas have difficulty contacting authorities for help, as most victims showed. As a result, victims must travel far to physically register the report, which causes issues for those who have jobs. These online organizations are unable to resolve the victim's issues, which makes it challenging for the victim to pursue justice, even after overcoming such geographical obstacles.

Conflict of Interest

The authors showed no conflict of interest.

Funding

The authors did not mention any funding for this research.

References

Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: *A systematic literature review*. *Electronics*, *11*(2), 198. https://doi.org/10.3390/electronics11020198

Adams, W. C. (2015). Conducting semi-structured interviews. *Handbook of practical program evaluation*, 492-505. https://doi.org/10.1002/9781119171386.ch19

Awan, J. H., Memon, S., & Burfat, F. M. (2019). Role of Cyber Law and Mitigation Strategies in Perspective of Pakistan to Cope Cyber Threats. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *9*(2), 29-38. doi: 10.4018/IJCWT.2019040103

Barriball, K. L., & While, A. (1994). Collecting data using a semi-structured interview: a discussion paper. *Journal of Advanced Nursing-Institutional Subscription*, *19*(2), 328-335. https://doi.org/10.1111/j.1365-2648.1994.tb01088.x

Bokhari, S. A. A. (2023). A Quantitative Study on the Factors Influencing Implementation of Cybersecurity Laws and Regulations in Pakistan. *Social Sciences*, *12*(11), 629. https://doi.org/10.3390/socsci12110629

Brazhnik, O., & Jones, J. F. (2007). Anatomy of data integration. *Journal of biomedical informatics*, *40*(3), 252-269. https://doi.org/10.1016/j.jbi.2006.09.001

Brinkmann, S., & Kvale, S. (2005). Confronting the ethics of qualitative research. *Journal of constructivist psychology*, *18*(2), 157-181. https://doi.org/10.1080/10720530590914789

Burns, R. G., Whitworth, K. H., & Thompson, C. Y. (2004). Assessing law enforcement preparedness to address Internet fraud. *Journal of Criminal Justice*, *32*(5), 477-493. https://doi.org/10.1016/j.jcrimjus.2004.06.008

Buzdugan, A., & Capatana, G. (2022). Cyber security maturity model for critical infrastructures. Paper presented at the Education, Research and Business Technologies: *Proceedings of 20th International Conference on Informatics in Economy (IE 2021)*.

Corti, L., Day, A., & Backhouse, G. (2000). Confidentiality and informed consent: Issues for consideration in the preservation of and provision of access to qualitative data archives. Paper presented at the Forum Qualitative Sozialforschung/Forum: Qualitative Social Research.

Dupin, C. M., & Borglin, G. (2020). Usability and application of a data integration technique (following the thread) for multi-and mixed methods research: A systematic review. *International Journal of Nursing Studies*, 108, 103608. https://doi.org/10.1016/j.ijnurstu.2020.103608

Fielding, N. (2001). On the compatibility between qualitative and quantitative research methods.

FlorCruz, J. A., & Seu, L. (2014). From snail mail to 4G, China celebrates 20 years of Internet connectivity. CNN news report. http://edition. cnn. com/2014/04/23/world/asia/china-internet-20th-anniversary.

Gallagher, M., Giles, J., Park, A., & Wang, M. (2015). China's 2008 Labor Contract Law: Implementation and implications for China's workers. *Human Relations*, *68*(2), 197-235. https://doi.org/10.1177/0018726713509418

Galletta, A., & Cross, W. E. (2013). Mastering the semi-structured interview and beyond: From research design to analysis and publication (Vol. 18): NYU press. https://doi.org/10.18574/nyu/9780814732939.001.0001

Grant, C., & Osanloo, A. (2014). Understanding, selecting, and integrating a theoretical framework in dissertation research: Creating the blueprint for your "house". *Administrative issues journal*, *4*(2), 4.

Harrell, M. (2009). Data Collection Methods: Semi-Structured Interviews and Focus Groups. RAND Corporation.

Imran, M., Murtiza, G., & Akbar, M. S. (2022). The Rise of Cyber Crime in Pakistan: A Threat to National Security. *Journal of Development and Social Sciences*, *3*(4), 631-640.

Kosseff, J. (2017). Defining cybersecurity law. Iowa L. Rev., 103, 985.

Kvale, S. (2012). Doing interviews: Sage.

Lim, H. S. M., & Taeihagh, A. (2018). Autonomous vehicles for smart and sustainable cities: An in-depth exploration of privacy and cybersecurity implications. *Energies*, *11*(5), 1062. https://doi.org/10.3390/en11051062

LJ Bikoko, T. G., Tchamba, J. C., & Ndubisi Okonta, F. (2019). A comprehensive review of failure and collapse of buildings/structures. *International Journal of Civil Engineering and Technology*, *10*(3).

Naseer, D. R., & Amin, D. M. (2020). Cyber-threats to strategic networks: Challenges for Pakistan's security. *South Asian Studies*, *33*(1).

Rasool, S. (2015). Cyber security threat in Pakistan: Causes, Challenges and Way forward. *International Scientific Online Journal*, *12*, 21-34.

Recker, J. (2021). Scientific research in information systems: a beginner's guide: Springer Nature.

Roig, M. (2006). *Ethical writing should be taught. BMJ*, *333*(7568), 596-597. doi: https://doi.org/10.1136/bmj.38946.501215.68

Romano Jr, N. C., Donovan, C., Chen, H., & Nunamaker Jr, J. F. (2003). A methodology for analyzing web-based qualitative data. *Journal of Management Information Systems*, *19*(4), 213-246. https://doi.org/10.1080/07421222.2003.11045741

Saleem, B., Ahmed, M., Zahra, M., Hassan, F., Iqbal, M. A., & Muhammad, Z. (2024). A survey of cybersecurity laws, regulations, and policies in technologically advanced nations: A case study of Pakistan to bridge the gap. *International Cybersecurity Law Review*, *5*(4), 533-561.

Sanjari, M., Bahramnezhad, F., Fomani, F. K., Shoghi, M., & Cheraghi, M. A. (2014). Ethical challenges of researchers in qualitative studies: The necessity to develop a specific guideline. Journal of medical ethics and history of medicine, 7.

Walsham, G. (2006). Doing interpretive research. *European journal of information systems*, *15*(3), 320-330. https://doi.org/10.1057/palgrave.ejis.3000589