Analyzing Legislative Framework and Cyber Security Responses against Violent Extremism and Terrorism

Rana Saifullah Hassan, Dr Naeem Ahmad

August 2023
All rights reserved.

No part of this report may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or information storage and retrieval system, without prior written permission of the publisher.
A publication of the Sustainable Development Policy Institute (SDPI), Islamabad. The opinions expressed in this Policy Brief are solely those of the authors, and stakeholders where mentioned, and publishing them does not in any way constitute an endorsement of the opinion by the SDPI.

Sustainable Development Policy Institute is an independent, non-profit research institute on sustainable development.

First edition: August 2023

© 2023 by the Sustainable Development Policy Institute
Abstract

This study evaluates the existing legislative framework and security responses against cyber extremism and cyber terrorism. Unfortunately, Pakistan falls among the top seven vulnerable countries when it comes to cyber security. The study finds that the existing laws, including Cyber Security Policy and National Security Policy, are basically operating at the institutional and organizational level and cyber extremism as a separate phenomenon is not exclusively being dealt with under any law. The legislation and the courts are still unable to differentiate between cyber extremism and cyber terrorism. Only Pakistan Electronic Cyber Act, 2016 discusses “cyber terrorism” but that is too broad and requires judicial interpretation and legislative clarity, yielding instances of abuse and misuse of the process of law. This study, through a comprehensive theoretical analysis and practical insight on the subject, stresses upon the need for coining an exclusive and operational definition of the term, “Cyber extremism” and how it is different from cyber terrorism. The methodology for this study is purely qualitative analysis using primary and secondary data. The Legislative Framework and all existing laws, including judgments of the appellate courts on cyber offenses are analyzed through document analysis. This study proposes to have an exclusive Countering Violent Extremism (CVE) strategy and legislative framework at the provincial level, separate courts, exclusive law on sentencing, training of investigation officers and prosecutors, community policing, effective policy implementation plan at public and community level, socio-psychological profiling of accused persons and introduction of specialized courses on CVE in Cyber Security degree programmes in Pakistan under Higher Education Institutions (HEI).

Keywords: Cyber Extremism, PECA 2016, Cyber Security Policy, Legislative Development. Countering Violent Extremism (CVE), Law of Sentencing.
Analyzing Legislative Framework and Cyber Security Responses against Violent Extremism and Terrorism

Rana Saifullah Hassan¹, Dr Naeem Ahmad²
August 2023

1 Civil Judge and Judicial Magistrate, Karachi (Malir) & PhD candidate, Department of International Relations, University of Karachi
2 Chairperson, Department of International Relations, University of Karachi
# Table of Contents

Introduction 6

Literature Review 7

Methodology 9

Discussion and Findings 10

Policy Recommendations 13

References 15

Appendix - 1 16
Introduction

Cybercrime is the general term used to describe all such illegal behaviours carried out by intentionally assaulting or influencing the actions of other states and societies through the use of computer systems and the internet. Data theft, cyber-espionage, electronic counterfeiting, cyber-terrorism, defamation campaigns, hate-mongering, bank frauds, and other similar crimes are typical examples of this crime as per the existing legislation (Dennis 2019). Cybersecurity is the practice of protecting computer systems, networks, and digital information from unauthorized access, damage, theft, and other cyber threats to ensure the confidentiality, integrity, and availability of digital assets (Kaspersky 2019). On the contrary, Cyber Extremism is the use of online platforms to promote and spread extremist ideologies, radicalization, and hate speech may it be from the perspective of language, culture, sect, race, caste, religion, region or anything aiming to incite violence or recruit members, whereas Cyber Terrorism is utilizing cyber-attacks to cause harm, disruption, and fear among the population for political, ideological, or religious reasons, with the primary goal of instigating terror (Weimann 2014). Cyber technology is frequently employed around the world to commit cybercrimes for monetary, political, economic, or strategic advantages. The concept of cybercrime is conceptually and practically broad. Different experts define it differently. Several illegal actions performed through cyber technology result in different implications.

These terms differ in their motivations and objectives with cybersecurity serving as a proactive measure to defend against cyber threats while cybercrime, cyber extremism, and cyber terrorism involve harmful or illegal activities conducted on the internet for various reasons.

Effective cyber security is now necessary since millions of cyberattacks have marred the infrastructure and services in recent years. Understanding the relationship among user privacy, data sovereignty and cyber security is crucial in this emerging cyber age for a nation’s territorial integrity. As a result, Pakistan’s essential infrastructure, governance, and institutional framework all confront cyber security issues. Pakistan’s national security is currently under jeopardy due to a technical and organizational gap, according to the Global Cyber Security Index (GCI) (Baloch 2022). In addition, it is imperative to highlight the use of cyberspace in promoting violent extremism in the modern-day technology driven outlets where the accessibility of information is readily available, making citizens, especially the youth, most likely to fall prey to extremism.

To explore the multifaceted nature of these phenomena, this study examines legal frameworks, national coping strategies, and global responses in this regard.

It also unfolds the dynamics of violent extremism through cyber space and examines the existing framework for addressing ‘cyber extremism’ in Pakistan and highlights the limitations of the Electronic Transaction Ordinance and the subsequent attempts to introduce comprehensive legislation. It further delves into the current state of cyber extremism and terrorism in Pakistan,
shedding light on how extremist groups exploit online platforms to spread radical ideologies and recruit individuals.

**Literature Review**

Cyber extremism and cyber terrorism have emerged as significant challenges in the digital age, posing threats to national security and societal stability. Warfare is an art that is constantly evolving. Pakistan is one of the 10 nations that are most susceptible to cyberattacks, according to Symantec (Khalil 2020). Cyber-terrorism has emerged as a major issue in the global information and network warfare conflict because it raises the possibility that terrorists may target innocent people and cause mayhem as a result of their reliance on networked communications.

Pakistan was named among the top 10 expanding cyber economies in the world (Information Economy Report 2017). In Pakistan, there are about 65 million broadband customers. Out of the total, 63 million broadband subscribers use 3G and 4G smartphones to access the internet. (GSMA 2017)

A survey found that more than 92% of people regularly use social media, the people aged 18 to 24 made up over 62% of the total (Gallup Pakistan 2016).

Facebook is the most widely used social media platform. Nearly 30 million people use it nationwide (Syed, Khaver and Yasin 2019). The social media platform is now viewed as having two sides. On the one hand, it has linked a number of voices that oppose religious fanaticism to the forefront, but on the other, it gives people the chance to spread false information and level blasphemous charges against others. In Pakistan, controversial sermons (known as khutbas) used to be the main source of crowd violence, but now social media is serving as a new platform. In April 2017, a group of Mashal’s classmates dragged him from his hostel room. He was shot and beaten, and his body was then dismembered only after a rumour that Mashal had uploaded offensive material online (Mahmood 2017).

The goals of cyber-terrorism can be social, political, ideological, religious, or similar. For instance, the motive behind state-sponsored cyber-terrorist attacks can be political. Cyber-terrorism activities carried out by anonymous groups may have social or ideological agenda. Cyber-terrorists achieve their goals through a number of acts, such as destroying critical infrastructure and information systems, compromising communication systems, obtaining classified information, spreading propaganda, intimidating people, launching Distributed Denial of Service (DDOS) attacks, and planting Advanced Persistent Threats (APTs).
Syed, Khaver and Yasin (2019) said:

“The nature of the internet makes it possible to hide behind its free for all infrastructures. This is especially so when cyber-attacks are state sponsored. Also because of the asymmetry of attacks, the hackers enjoy anonymity.”

Ghani (2019) says:

National security is not a constant but is defined by a multitude of challenges, both external and internal. National Security Policy should therefore be dynamic and evolve with the emerging challenges. Apart from the traditional security concerns, innovative issues such as terrorist financing, money laundering, increased use of technology by criminals, militants and terrorists, cyber-related issues need to be addressed through these policies.

Ali (2022) opines:

Cyber terrorism is likely to turn out to be an immediate threat to the country’s national security. This could be the use of internet by terrorists to plan, recruit, and communicate with other terrorists inside and outside the territorial boundaries. While the terrorists may not have the advanced skills to target critical, sensitive infrastructure, they are likely to use the vulnerability of the internet or its unmonitored facilities to communicate, recruit, and plan terrorist attacks.

Electronic Transaction Ordinance, 2002 (ETO 2002) was created with the intention of giving electronic information a legal standing. While it gave electronic information legal legitimacy, the ordinance did not address cybercrimes or cyber extremism and cyber terrorism. The government enacted the Prevention of Electronic Crimes Ordinance, 2007 (PECO 2007), which is another law. The significant PECO provisions are those dealing with cybercrimes, their penalties, their prosecution and trial, and the establishment of agencies for investigation and prosecution. Cyberterrorism, illegal data interception, spoofing, spamming, cyber-stalking, abuse of encryption, misuse of electronics equipment and systems, electronic forgery, electronic fraud, system damage, data damage, and criminal data access are only a few examples of the various types of cyber offenses that PECO deals with. The ordinance instructed the federal government to establish a cell with the Federal Investigation Agency (FIA) rather than forming a distinct department for cybercrimes. Various aspects of the ordinance underwent refinement in PECO over the years. The Electronic Transaction Act (ETA), Perspective Analysis of Cyber-Crime Act (PACCA), Electronic Fund Transfer Act (EFTA), Prevention of E-Crime Ordinance Act (PECOA), and Electronic Documents and Prevention of Cyber Crime Ordinance Act (EDPCCOA) are additional significant laws and ordinances relating to cybercrime. Understanding the value of security and privacy for digital services provided and used by various government departments. The “Khyber Pakhtunkhwa Cyber
Emergency Response Center (KPCERC)” initiative was launched by the Khyber Pakhtunkhwa Information Technology Board (KPITB). By creating a center that provides various cyber security services to public and commercial bodies and serves as a technical support base for the provincial government in domains, the project’s goal is to meet the requirement for cyber security. Though Pakistan has various cyber security laws, not enough effective countermeasures had been adopted in this regard, Ahmad and Khan (2022) quoted the former interior minister, Rehman Malik, as saying. Pakistan’s cyber security policy faces significant critiques, including a lack of ownership and commitment, weak enforcement of existing statutes, and inadequate resources allocated to cyber security efforts. The policy lacks continual improvement and assessment mechanisms, leading to challenges in adapting to evolving cyber threats. Moreover, the shortage of skilled professionals, weak inter-departmental coordination, and inadequate authorization standards further hinder the country’s cyber defense capabilities. The government has planned to achieve the capacity building of stakeholders within the first year of the policy. However, the policy text is vague on the issue of the overall implementation timeline. No specific time limit has been set for the achievement of the proposed mechanisms. Therefore, in the interim period, the federal government will prioritize initiatives for the banking, telecom, educational, and provincial institutions. Yet, the term “interim period” also remains undefined. These shortcomings underscore the need for enhanced commitment, enforcement, and resource allocation to establish a robust and resilient cyber security framework in Pakistan. The implementation of the National Cyber Security Policy 2021 may face significant challenges, particularly regarding the establishment of a centralized body to regulate cybersecurity at various levels. The ambitious scope and lack of specified funding sources could hinder the practicality of the implementation process in a resource-constrained country like Pakistan. Moreover, the policy’s placement in the overall order of government actions seems improper, as policies usually follow strategies and legislation. While the policy is a comprehensive document, its effectiveness relies heavily on timely and efficient implementation to achieve the intended impact.

Methodology

The study employs qualitative data collected through primary and secondary methods followed by a comprehensive and multidisciplinary approach through content review and theoretical analysis. The review helps establish the conceptual framework and identify research gaps. Primary data is collected through interviews from the major stakeholders, including office-bearers of the supreme court and high court bar associations, additional director and inspectors of Federal Investigation Agency (FIA), Former Additional Inspector General (AIG) Police, social scientists, journalists, and researchers on law and justice. As many as 15 interviews were conducted (Appendix-1).
Discussion and Findings

The terms ‘Cyber-crime’ and ‘Cyber-terrorism’ are used interchangeably in the existing legislative framework. The two phrases, however, take different approaches. Cybercrime is an illegal activity in which the use of computer technology as a weapon, a target, or both is involved. Hacking, fraud, forgeries, money laundering, and illicit data interception are examples of it that could jeopardize the availability, confidentiality, and integrity of information. Similarly, cyber terrorism can be an act that strikes fear among populations through a variety of means, including endangering state security, destroying vital assets, uprooting habitats, displacing people, and harming nations’ economies.

Following research questions were framed and findings thereof are as follows:

**To what extent, National Security Policy of Pakistan 2022-2026 and National Cyber Security Policy are effective in Pakistan’s response to P/CVE?**

The study argues that cyber extremism is the unfortunate reality of the socio-legal, cultural, and political fabric of the state and none of the two national security policies exclusively calls for the action/measures against cyber extremism.

The most significant finding of this study is that neither the National Security Policy 2022 to 2026 nor the National Cyber Security Policy 2021 consider cyber extremism and cyber terrorism as two distinctive phenomena using cyberspace. Both the policies, particularly the cyber security policy, largely focus on the cyber-attacks on the national institutions and organizations by using cyberspace. The study finds that the existing policy framework, including Cyber Security Policy and National Security Policy are basically operating at the institutional and organizational level and cyber extremism, as a separate phenomenon, is not exclusively being dealt with under any policy. It is quite astonishing that there is no clue of countering violent extremism through cyberspace. Fundamentally, cyber extremism is required to be identified as a distinctive phenomenon in socio-political, cultural, and legal dynamics of Pakistan, but the existing policies are too much institution and organization centric that they do not cater to the acts of cyber extremism as an exclusively ideologically driven incidents causing serious internal threat to the communal, provincial as well as national security. This study also outlines “cyber extremism” as an ideologically driven act or a cause of violence using cyberspace. It is not necessary that such acts can be perpetrated by someone from outside the territorial jurisdiction of Pakistan and an attack on sophisticated data of institutions or organizations. It can be at the very micro level arising out of the dispute between two individuals or a group.

Furthermore, the cyber security policy itself calls for enhancing existing legislative and institutional frameworks. It concedes to having weak enforcement of statutes in Pakistan besides lack of data governance as well as inadequate and poor quality of resources. Even in Part 2.3 (objectives) of cyber security policy, cyber extremism and the measures to curb cyber terrorism are not even touched
upon. There is a strong need to identify countering violent extremism in cyber security policy. Pakistan does not have a professional workforce against cyber extremism. Policy implementation is weak, and in fact there is no implementation at all.

Though Higher Education Institutions (HEI) have initiated courses on cyber security, post Cyber Security Policy and National Action Plan; Surprisingly, none of the course modules or elective subjects mention “cyber extremism or cyber terrorism” as a fundamental course of these programmes.

**How effective are the present legislative responses in countering violent extremism and terrorism using cyberspace?**

The legislation as well as the courts are still unable to distinguish cyber extremism from cybercrimes and cyber terrorism whereas the latter is only discussed in the Prevention of Electronic Crimes Act, 2016 (PECA 2016) and that has a broad interpretation yielding instances of abuse and misuse of process of law. The legislation has left the definition of the word “terrorism” too broad in the statute exclusively dealing with the cases of terrorism, Anti-Terrorism Act, 1997. In this regard, the Supreme Court of Pakistan made a landmark attempt in the case of Ghulam Hussain and Others versus The State, judgment cited as PLD 2020 Supreme Court 61 to settle the parameters for the offences qualifying to be treated under ATA 1997 and as an act of terrorism. Whereas bare reading of the judgment also reflects that parliament is yet to clarify the distinction between an act of terrorism and an act of violent extremism. Similarly, no law or statute has outlined a distinction between cyber extremism, cybercrime, cyber offences and cyber terrorism.

In the cases of terrorism, there is no law on sentencing and the discretion as to quantum and gravity of punishment lies solely on the discretionary power of the court. As such, there is a dire need for comprehensive law making and legislative development against cyber extremism.

The scope and effectiveness of the Witness Protection Act is also questioned and the witnesses in the cases of violent extremism do not have adequate security, therefore, prefer either to avoid court hearings or give false testimony.

With respect to PECA, 2016, the Section 2 of the act is completely silent regarding definition of cyber extremism whereas Section 10 of Chapter 2 defines cyber terrorism which is as follows:
Cyber Terrorism: Whoever commits or threatens to commit any of the offences under section 6, 7, 8 or 9, where the commission or threats is with the intent to:

- Coerce, intimidate, create a sense of fear, panic or insecurity in the Government, or the public or a section of the public or community or sect or create a sense of fear or insecurity in society; or
- Advance inter-faith sectarian or ethnic hatred; or
- Advance the objections of organizations or individuals or groups prescribed under the law, shall be punished with imprisonment of either description for a term which may extend to fourteen years or with fine which may extend to fifty million rupees or with both.

Now, the bare reading of the relevant sections in juxtaposition with varied and multiple definitions of Cyber Extremism, appears to be a clear inadequacy and major lacuna in the legislation as the instances of cyber extremism originates from distinctive socio-cultural, psychological, and political dynamics of the society. Extremism can be personal, regional, linguistic, religious, and culturally driven outcome and the fundamental definition of cyber terrorism does not cover the “mens rea” (intent to commit crime) eventually resulting in acquittal or failure of prosecution during criminal trial. Extremism can be even academic, racial, ethnic and in many other facets.

The relevant part of PECA, 2016 describes the punishment, but fails to chalk out the sentencing criteria on the face of the law. The law does not cover the aspects of academic, linguistic, and culturally driven outcomes of extremism. Importantly, the ambit / scope of the definition and clauses as mentioned in the statute is clearly too wide that the probability of misuse and abuse of the process of law cannot be ruled out. In addition, even section 6, 7, 8 or 9 is unclear as to what exactly is infrastructure and what comes under the ambit of organizations and infrastructure.

The term “extremism” in law is yet to be separated from the word “terrorism”. Unless the definitional gap is not confined or exclusive measures are not taken, the law and existing framework on CVE measures will remain ineffective.

Cases of cyber terrorism in Pakistan are presently investigated by the Federal Investigation Agency (FIA) and National Response Centre on Cyber Crime (NR3C). There is a shortage of investigation officers and prosecutors with FIA and those entrusted with such cases lack required competence and training. There is a separate unit in FIA set up under Anti-Money Laundering Act (AMLA) to control external and terrorism financing, but there is no unit or a separate wing for countering cyber extremism.

Another finding is that there is no exclusive or speaking law of sentencing in the cases of cyber extremism. The court has the discretion to decide the quantum of punishment, which creates inconsistency in the law and criminal procedure.
Policy Recommendations

- To strengthen Pakistan’s response to cyber extremism and cyber terrorism, several key recommendations are proposed.
- A comprehensive and exclusive cyber extremism legislation needs to be tailored to address the evolving nature of cyber threats. The legislation must cover a wide range of social, cultural, academic, regional, legal, and politically driven factors and actions, which qualify to become an act of extremism inciting violence.
- It clearly identifies the offences related to cyber extremism and other cybercrime while defining the elements of cyber extremism. As existing legislative and security responses lack dynamic and focused CVE responses, therefore, there is a dire need to identify CVE measures in cyber security as well as national security policy.
- Furthermore, capacity building and training programmes for law-enforcement agencies, intelligence agencies, and judicial institutions are essential to enhance skills and expertise of law enforcement personnel in tackling cyber threats.
- A separate CVE wing should be set up in the National Response Centre for Cyber Crimes (NR3C).
- Public awareness campaigns need to be launched to educate the general public about cyber extremism and cyber terrorism, with a focus on secure online behaviour and the reporting of suspicious activities.
- There is a need to strengthen cyber infrastructure through robust cybersecurity measures, vulnerability assessments, and collaboration with cybersecurity experts.
- Since extremism is rooted in socio-cultural and regional dynamics, a federal law such as PECA, 2016 is not sufficient to deal with the robust instances of cyber extremism. It is, therefore, proposed to introduce provincial legislation in a similar way as of Child Marriage Restraint Act, which has been passed by the provincial assembly of Sindh.
- Higher Education Institutions should introduce a course module on cyber extremism and countering violent extremism measures through effective use of technology in academia.
- Specialized and dedicated workforce in the investigation wing equipped with international training need to be introduced in the police training academy. Similarly, special training courses may be introduced in the Federal Judicial Academy to sensitize judicial officers presiding over the cases of violent extremism.
- Since conventional courts cannot try cyber cases, therefore, separate courts may be set up to hear the cases of cyber extremism and cyber terrorism making it a prerequisite for a judicial officer to hold a certification at least in cyber security laws and practice.
- Similarly, selection of prosecutors and investigation officers in such courts need to be equally competent with expertise on cyber security.
- Since the internet users are continuously on the rise, socio-psychological profiling is very important for all the accused persons, as the offenses are likely to fall under cyber-extremism are not confined to any age or educational criteria.
• Similarly, the office of the prosecutor general needs to be taken on board and competent Additional Prosecutor General (APG) needs to be identified to appear before the Hon'ble High Courts and the apex court in appeal matters.
• Exclusive and effective Witness Protection Law is required to be enacted and implemented effectively. Besides, the present Witness Protection Act may include amendments related to the witnesses appearing in the cases of cyber extremism.
References


**Appendix - 1**

<table>
<thead>
<tr>
<th>No</th>
<th>Name</th>
<th>Designation</th>
<th>Department/Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Muhammad Hussain Bux Baloch</td>
<td>Additional Prosecutor General</td>
<td>Government of Sindh</td>
</tr>
<tr>
<td>2</td>
<td>M. Aziz Khan</td>
<td>Vice President</td>
<td>Supreme Court Bar Association, Pakistan</td>
</tr>
<tr>
<td>3</td>
<td>Ibbad ul Hasnain</td>
<td>Advocate</td>
<td>Supreme Court of Pakistan</td>
</tr>
<tr>
<td>4</td>
<td>Lutufullah Seelro, Alvi</td>
<td>Advocate Ex-President</td>
<td>Sindh High Court</td>
</tr>
<tr>
<td>5</td>
<td>Mazhar Hussain Alvi</td>
<td>Advocate Ex- Additional Inspector General of Police.</td>
<td>Sindh High Court</td>
</tr>
<tr>
<td>6</td>
<td>Idrees Seelro</td>
<td>Additional District Public Prosecutor,</td>
<td>Malir, Karachi, Govt of Sindh</td>
</tr>
<tr>
<td>7</td>
<td>Nasir Rizwan</td>
<td>Advocate</td>
<td>Supreme Court of Pakistan</td>
</tr>
<tr>
<td>8</td>
<td>Javed Akhtar</td>
<td>District Public Prosecutor</td>
<td>District (South)</td>
</tr>
<tr>
<td>9</td>
<td>Qadir Lashari</td>
<td>Journalist</td>
<td>Express News</td>
</tr>
<tr>
<td>10</td>
<td>Younas Baloch</td>
<td>District Public Prosecutor</td>
<td>Govt of Sindh, Karachi East</td>
</tr>
<tr>
<td>11</td>
<td>Barrister Jahanzaib</td>
<td>Advocate</td>
<td>Sindh High Court</td>
</tr>
<tr>
<td>12</td>
<td>Dr Riaz Shaikh</td>
<td>Dean, Faculty of Arts and Social Sciences</td>
<td>SZABIST, Karachi</td>
</tr>
<tr>
<td>13</td>
<td>Salabuddin Khan Gandapur</td>
<td>Advocate</td>
<td>Supreme Court of Pakistan</td>
</tr>
<tr>
<td>14</td>
<td>Aijaz Kalwar</td>
<td>Additional Director</td>
<td>Federal Investigating Agency (FIA)</td>
</tr>
</tbody>
</table>