Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 3, Issue 11, 2025

DIGITAL FRONTLINES: THE ADEQUACY OF PAKISTAN'S COUNTER-TERRORISM LEGAL FRAMEWORK IN THE AGE OF CYBER-TERRORISM AND FINTECH

Mujeeb U Rahman Khuhro[*1], **Abdul Razzaque Mirani**[2]

[*1]*Assistant Professor at Shaheed Zulfiqar Ali Bhutto University of Law*
[2]*Lecturer at Shaheed Zulfiqar Ali Bhutto University of Law*

[*1]mujeeb.rehman@szabul.edu.pk, [2]abdul.razzaque@szabul.edu.pk

DOI: https://doi.org/10.5281/zenodo.17548788

Keywords
Cyber-Terrorism, Anti-Terrorism Act (ATA), Prevention of Electronic Crimes Act (PECA), Terror Financing (TF), Virtual Assets (VAs), FATF Compliance, Online Radicalization, Legislative-Operative Gap (LOG)

Article History
Received: 15 September 2025
Accepted: 25 October 2025
Published: 07 November 2025

Corresponding Author: * Mujeeb U Rahman Khuhro

Abstract

The strategic location of Pakistan and its uncompromising threat environment require a sound and unified counter-terrorism (CT) jurisprudence. In reaction to transnational militant organizations, including Tehreek-e-Taliban Pakistan (TTP), the Balochistan Liberation Army (BLA), and Islamic State Khorasan Province (ISKP) that have shown an advanced use of digital platforms, Pakistan uses a multi-layered legal framework (Arshad Khan, 2018; Institute for Economic and Peace, 2025). The framework is largely based on the Anti-Terrorism Act (ATA) 1997 which is given supplementary by the Prevention of Electronic Crimes Act (PECA) 2016 and historically the now abolished Pakistan Protection Act (PPA) 2014 (Arshad Khan, 2018; Aziz, 2018). Through this study, the doctrinal legal analysis, which is concerned with statutory interpretation, international comparative standards, and critical policy criticisms, including the outcomes of the Financial Action Task Force (FATF) are used. The overriding point is that the current regime is poor, internally contradictory and has harsh jurisdictional overlaps. Three fundamental failures of this vulnerability include consistency in defining cyber-terrorism as a concept, the broad legislation of which leads to violation of human rights in combating the spread of internet radicalization (Center for Strategic & International Studies, 2018), and operational gaps in the control of Virtual Assets (VAs) in financing terrorism (U.S. Department of State, 2025), despite the critical amendments being made to the ATA. These systemic problems, which can be defined in terms of the Legislative-Operative Gap paradigm, not only compromise the national security goals but also highly important international compliance requirements, which require urgent consolidation of the legislative framework and a firm demarcation of the enforcement power.

1. Introduction:

Modern conflict has shifted dramatically to the new form of dynamic and transnational digital security governance as opposed to the conventional kinetic counter-insurgency efforts. The different terrorist groups that have been working in the Pakistan-Afghanistan border region, especially the TTP and the ISKP have been able to strategically rely on cyberspace as an essential continuation of their operations. The advanced use of online resources by organizations like ISKP (with its multilingual propaganda division, Al-Azaim) proves that there is a definite change towards a stronger focus on influence on a scale that goes well beyond regional roots and makes effective use of both local and international viewers to recruit and radicalize (Institute for Economic and Peace, 2025). This quick adaptation by militant groups forms an inherent asymmetry, in which zippy digital threats are well ahead of the often lumbering, linear system of legislative and institutional change. Good national security demands a legal framework, which can respond swiftly, technically knowledgeable, and rights congruent to online propaganda, experimental infrastructure attacks, and the utilization of decentralized digital currencies to fund it(Center for Strategic & International Studies, 2018).

1.1 Overview of the three-tiered CT regime in Pakistan

The development of legislative responses towards the problem of terrorism in Pakistan has traditionally been defined in terms of repeated legislative responses to ad hoc security emergencies and the pressure of international organizations, which led to an elaborate and contradictory legal framework.

- **Tier 1 (Foundational) - The Anti-Terrorism Act (ATA) 1997:** The ATA 1997 is the foundation of the anti-terror law in Pakistan, and it substitutes the previous Suppression of Terrorist Activities Act of 1975 (Ali, 2023). Although having been originally created to offer prevention and fast justice in heinous crimes, the ATA has faced several amendments especially after the 9/11 era, in reaction to international counter-terrorism financing (CFT) requirements imposed by resolutions like UNSCR 1373 (Lynch, McGarrity, & Williams, 2010). Although the amendments have been broadened to cover terror related activities that are non-traditional, the main emphasis of the ATA has been to qualify terrorism in terms of intent (to cause fear or physical harm) and creation of special courts. The issues of scope creep are apparent as seen by modifications put forward to bring offences such as adultery or sodomy involving children below the age of sixteen within the scope of the ATA on grounds that such offenses evoke the fear of the people hence they are considered terrorism (Jawad, 2022).

- **Tier 2 (Punitive/Expedited) - The Protection of Pakistan Act (PPA) 2014:** The philosophical and procedural legacy of the PPA 2014, notwithstanding the fact that it is no longer being applied, had a tremendous impact on the CT landscape. The PPA was described by broad, unprecedented powers given to the military and law enforcement force such as preventive administrative detention with no proper safeguarding and establishment of special courts with a procedure that does not respect the right to a fair trial (Jawad, 2022). Human rights groups criticized the law saying that it would increase violations rather than curb them, especially in areas that dealt with secret arrests, enforced disappearance and torture (International Commission of Jurists, 2014). The PPA represents one such trend, where expedited and punitive justice is given precedence over a carefully conducted and rights-adherent investigation and prosecution (Waseem, 2024).

- **Tier 3 (Digital/Cyber) - The Prevention of Electronic Crimes Act (PECA) 2016:** PECA 2016 was introduced to deal with the increasing number of electronic crimes and is designed to be the law of the day on digital crimes. It expressly includes Cyber terrorism (Section 10), and gives specific procedural authority to conduct digital investigation, such as expedited preservation and acquisition of data, search and seizure warrants, and real-time gathering of information (Arshad

Khan, 2018). The broadening scope of PECA, however, is receiving significant criticism as well as its poorly defined terms, as well as how it is subsequently being used as an instrument of silencing political dissent in the name of combating cyber threats (Waseem, 2024).

The analysis establishes that the current legal framework, which is the ATA, the heritage of the PPA, and PECA, is a system of multiple fragments and overlaps. Although legislative initiatives have been effective to bring in the aspect of cyber and financial regulation, the general consistency and operational effectiveness are highly undermined. This paper argues that this multi-layered legal framework is unsatisfactory, inconsistent among itself and characterized by the jurisdictional overlaps that cripple counteraction to online radicalization, technical cyber-terrorism and fintech-based terror finance, thus dramatically affecting the national security agenda and international compliance requirements most of all relevant to the FATF. The subsequent sections will provide a theoretical framework for these findings, examine the relevant research, and conduct a thorough critical analysis of the weak spots, leading to essential recommendations for institutional and legislative reform.

2. Legal Fragmentation and Digital Governance

2.1 The Evolution of Pakistan's CT Law and the Scope Creep

In Pakistan the process of counter-terrorism legislation started with the Suppression of Terrorist Activities (Special Court) Act of 1975 and later replaced by the ATA 1997. ATA 1997, especially with the amendments which took place in 2013 and 2014, was directly developed following the changing nature of international requirements and security threats. An example of such laws is the Anti-Terrorism (Second Amendment) Act, 2014, which was designed to rectify deficiencies in the area of terror financing provisions in accordance with the international requirements, which would enhance the law enforcement agencies with more effective means of investigation (Ali, 2023).

One of the most important issues that emerge in literature regards the functional dilution, or scope creep, of CT law. This is clearly seen in the amendments that are motivated by security issues to broaden the definition of terrorism to include crimes that are not necessarily related to organized militancy. Indicatively, the 2015 amendment to the ATA has involved adultery or sodomy involving a child under sixteen claiming that such atrocious crimes are breeding fear and therefore amount to some sort of terrorism, and will be speedily tried in special courts. Although the specified purpose was the fear prevention, this addition diverts resources and focus to the fundamental structured terror threats, which is a contributor to the ambiguity of definitions and overworking of the special CT courts. Such expansion waters down the strength of the law required to prosecute actual militant operations and is an indication of a movement toward applying the ATA to a broad array of grave, non-terror offenses as a means of expediency (Durrani, 2020; Rafique & Manan, 2019).

2.2 Critiques of Cybercrime Legislation

The prevention Electronic Crimes Act (PECA) 2016 has received regular and strenuous criticisms on its content and implementation as a law by both legal researchers and human rights organizations, with academic agreement being that PECA is an ill-conceived document with ambiguity, vagueness, and over breadth (Arshad Khan, 2018). Although the law is considered to be aimed at containing the contemporary digital hazards in the form of frauds and cyberstalking, it is regarded as having been formulated in the context of a national security policy that essentially presupposes the violation of constitutional rights, such as the freedom of speech (Article 19) (Chaudary, 2023).

Certain clauses of PECA, including those that criminalize the glorification of terrorism-related crimes, including Section 9, are noted to be especially problematic (Aslam, Ashraf, Mukhtar, & Ashraf, 2025). According to scholars, these provisions are too broad and have been shown to cause a chilling effect on freedom of expression. This impact is felt where citizens are intimidated

by the possibility of severe punishments based on an ambiguous law by being afraid to exercise any legal right. More so, there is a long history of using laws meant to combat cyber-terrorism to serve political purposes. As an example, PECA, especially Section 20, has been applied by the investigative agencies in cases involving political activists who are accused of engaging in propaganda against the armed forces and the state institutions and to turn the cybercrime law into a tool of policing the political narratives and silencing of dissent (Suddle, Khan, & Nawaz, 2025). This trend, which has been observed in the repealed PPA, giving police a blanket power with rights-abusing characteristics, is a long-established aspect of the governance philosophy of Pakistani security, in which the application of future legislation such as PECA is influenced.

2.3 Nexus of Terror Financing (TF) and Virtual Assets (VA)

Terror financing (TF) poses special legal issues to money laundering (ML). Whereas ML is aimed at covering the illegal source of money, TF is about finding the funds, which can be a legitimate source or a traditional criminal business, to be transferred to a terrorist group. International instruments, especially UN Security Council resolutions, entail the member states making it a criminal offense to fund the terrorist groups and individuals without relating to a particular terrorist act (United Nations Office on Drugs and Crime, 2021).

This is one of the key global standards established by Financial Action Task Force (FATF). Recommendation 5 by FATF requires that the countries should criminalize TF according to the Terrorist Financing Convention, but the offences should be classified as predicate offences of money laundering (United Nations Office on Drugs and Crime, 2021). More importantly, Recommendation 15 covers "New Technologies" which mandates that Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) frameworks must be responsive to the new financial technologies, specifically Virtual Assets (VA) and Virtual Asset Service Providers (VASP) (Khan, 2025). The FATF has stepped up its efforts in this sector, calling for more global action to reduce the risks of illegal finance in VAs because they are easy to hide and traverse borders. Pakistan's compliance in this area is important for both national security and its place in the global financial system (FATF, 2025).

3. Theoretical Framework

3.1 Legislative-Operative Gap (LOG) Model in Security Governance

This analysis uses the Legislative-Operative Gap (LOG) model in order to comprehend why the CT laws of Pakistan do not tend to provide corresponding enforcement outcomes. The LOG explains the institutional detachment between the official legal requirements enacted by the legislature (the legislative element) and the real ability, resources, political unity, and implementation framework needed to carry out such laws properly on the ground (the operative element) (United Nations Office on Drugs and Crime, 2021).

This discontinuity is sharp as far as digital counter-terrorism is concerned. The legislature can quickly pass tough legislation like PECA, which will give broad powers to the investigative community to gather and store information. Nevertheless, the working mechanisms, the investigative agencies, the forensic labs, the judicial system, and the training infrastructure do not usually have the specialized resources, inter-agency trust, or the steady judicial support it can be needed to bring to bear on bringing transnational cyber-terrorism cases to trial. It is not the lack of law that is the failure, but rather in the implementation of the law (Bokhari, 2023).

3.2 Legal Pluralism and Jurisdictional Competition

Deep-rooted legal pluralism in Pakistan reinforces the LOG by having specialized judicial and law enforcement agencies that act under different, and in many cases, conflicting legislation (Saiya, 2020). The system in Pakistan has parallel legal regimes: the ATA Special Courts, the Code of Criminal Procedure, the Pakistan Penal Code, and separate cyber wings which work under PECA (Jawad, 2022).

Such a pluralistic setting is bound to encourage high levels of jurisdictional rivalry. Legal framework would require coordination of the Federal Investigation Agency (FIA) Cyber Crime Wing (CCW), providing technical expertise at digital forensics as is necessary to PECA, and the provincial Counter-Terrorism Departments (CTD), which are mandated by the ATA to act punitively and in speed. The resultant bureaucracy of implementing the CT response is that in a case where an act constitutes both a cybercrime (PECA) and a terror intent (ATA), the resultant cross-agency jurisdictional problem over who is the primary investigative agency and which court is to conduct the trial causes a bureaucratic delay and internal tensions and frustrations which reduces the effectiveness of the CT response. The analysis reveals that this institutional rivalry, which is a major operational failing, lets advanced digital threats get through, no matter how strict the laws are (Malik, 2025).

3.3 Defining Parameters for Legal Adequacy in Digital CT

Three key parameters have to be met in order to determine the sufficiency of the Pakistani regime:

- **Transparency of Definitions:** The legislation should include internationally recognized and clear-cut definitions, particularly of the emerging notions such as Cyber-Terrorism and Critical Infrastructure, such that the prosecutional standard is evident and justifiable.
- **Judicial Consistency:** Specialty courts (ATA) should not co-exist with ordinary/cyber courts because they cause judicial inconsistency and procedural gaps that can be exploited to grant acquittals according to jurisdictional or procedural technicalities.
- **International Compliance (Effectiveness):** This requirement is that compliance with international standards, specifically FATF Recommendation 15 on Virtual Assets, must be effectively manifested. It involves going beyond paper compliance to enforcement regulation which is active and enforceable and which can follow and discourage digital terror funding streams.

4. Methodology

The Doctrinal Legal Research approach that has been used in the research paper is coupled with Qualitative Policy Analysis. The analysis of the study is based on the critical analysis and statutory interpretation of the main legal texts; The Anti-Terrorism Act (ATA) 1997 and its key amendments (2012, 2014, 2015), the Prevention of Electronic Crimes Act (PECA) 2016, and the Protection of Pakistan Act (PPA) 2014, mainly to grasp the philosophical and procedural heritage established by it.

The sources of data include more than just domestic legislation to subsidiary legislation (Rules and Notifications) and special security publications. The very important secondary data set is the international reports, especially the Mutual Evaluation Reports and specific updates issued by the Financial Action Task Force (FATF) to show whether or not Pakistan complies with the measures to fight money laundering and counterfeit financing. Moreover, the analysis is based on the reviews of the international organizations (UNODC, ICJ, Amnesty International) and scholarly publications that cover the aspects of cybercrime, online radicalization, and security governance in South Asia (Amnesty International, 1997; Arshad Khan, 2018; Asia Pacific Group, 2020; International Commission of Jurists, 2014).

The methods of analysis include a comparison of the legal framework in Pakistan with the developed international standards of CT and human rights (e.g. UNSCRs and FATF standards). The LOG model is used as a heuristic tool in explaining continued failures to enforce despite the activity of legislation. The goal of the study is to clarify how operational bottlenecks and vulnerabilities that are taken advantage of by cybercriminals are directly caused by legislative texts' ambiguities and jurisdictional conflicts.

5. Cyber-Terrorism and Critical Infrastructure Vulnerabilities

5.1 Defining Digital Threats Across Statutes

The fundamental issue with the prevention of digital terror is the definition of the crime itself. With amendments, the ATA remains conservative

with its emphasis on acts that are calculated to cause terror among the populace, which usually entails violence or physical disturbance. PECA Section 10, on the other hand, overtly prosecutes "Cyber terrorism" and makes a direct connection with disrupting digital systems, frequently via an unauthorized access or interference in information (Mohammed, 2016).

On an international level, the difference between the abstract concept of pure cyber-terrorism and the use of the Internet as a terrorist tool is fundamental. Cyber-terrorism Pure cyber-terrorism is a cyber-dependent offense that is carried out with political purposes in order to instill fear with the view to causing death, bodily injury, severe economic damages, or critical infrastructure damage (e.g., sabotage of power grid). Cyber-terrorism as defined by PECA is very wide, and the possibility exists that it involves any disruptive attack by known terrorist groups to the computer systems with the aim of creating alarm or panic (UNODC, 2025).

The conclusion drawn here is that the legal system of Pakistan confuses these two classes. The wide umbrella term in PECA Section 10 has the potential to reduce the prosecutorial bar, permitting these enforcement agencies to characterize acts of great digital nuisance as cyber-terrorism. At the same time, this breadth does not give the investigative and judicial accuracy necessary to prosecute actual, high-impact, pure cyber-attacks on critical national infrastructure (CI) with the seriousness that they deserve. The product is an overly punitive system that can be inadequate in technical terms during the event of a high-tech digital sabotage.

5.2 PECA and Critical Infrastructure Protection: Investigation of Crimes

PECA 2016 tries to eliminate the most vulnerable areas by criminalizing activities that are directly related to CI information systems. Sections 6, 7 and 8 address unauthorized access, copying/transmission, and interference of critical infrastructure data or systems. The most important aspect of CI security is protection, and the global tendencies prove this point since suspicious users target crucial networks like power grids and transportation networks more and more (Iftikhar, 2024).

There is, however, a critical weakness in the implementation: the legal meaning of a critical infrastructure information system is not clearly and narrowly defined in the legal texts at hand. Such ambiguity may result in court controversies concerning what kind of attacks should be subject to the harsh punishment that Section 10 (Cyber Terrorism) imposes or should be considered as a regular cybercrime offense (Iftikhar, 2024). When the scope of CI is too imprecise the courts may have a hard time being consistent, especially when it comes to deciding whether digital vandalism or a sophisticated Denial of Service attack on a utility company qualifies under the necessary statutory definition of the term terrorism (Baezner, 2018).

5.3 Conflict in Enforcement Jurisdiction

Institutional fragmentation fundamentally undermines the enforcement structure by developing a debilitating operative gap. PECA is investigated by FIA Cyber Crime Wing (CCW), the special investigative agency with digital forensic and technical investigation skills (Ahmad, Asghar, & Afzal, 2025). On the other hand, the Counter-Terrorism Department (CTD) is an ATA mandate and it concerns herself with the intent of terror and the special CT courts (Durrani, 2020).

In a case which contains a PECA violation (e.g., disrupting critical infrastructure under Section 8) and terrorist intent (ATA criterion), there is an irresolvable jurisdictional conflict. Would it be the FIA, with its cyber specialization on the forefront, or would it be the CTD, with its mandate on the subject of terror prosecution? Experts have verified that the establishment of several bodies to address certain crimes leads to internal rivalry and duplication. Although institutional restructuring of the FIA (such as centralization of jurisdiction with proposed systems of NCCIA) could well solve the friction in the FIA cyber response mechanism, it does not eradicate the central ATA (CTD) against PECA (FIA) division (Ahmad et al., 2025; Malik, 2025).

This is a weakness in the structure that leads to a political policing priority that compromises CT effectiveness. The breadth of PECA Section 10 is

used frequently by the state as a muzzling device to prosecute critics using cybercrime statutes (Section 20 cases of political activists prosecuted) (Aziz, 2018). The following table illustrates the prevailing friction points in the digital counter-terrorism enforcement landscape:

Table 1 Jurisdictional Conflict Matrix: Digital Terror Investigations

Threat Type	Legal Basis (Primary)	Investigative Agency	Judicial Venue	Vulnerability/Overlap
Pure Cyber Terrorism (CI Attack)	PECA 2016 (Sec 10, 6-8)	FIA Cyber Crime Wing (CCW)	Special Courts established under PECA/ATA	Jurisdictional friction with CTD; technical evidence standards clash with ATA court speed
Online Glorification/Propaganda	PECA 2016 (Sec 9)	FIA/CTD (discretionary)	Special Courts/High Courts	Overbreadth, frequently used against political dissent, causing a chilling effect on constitutional rights
Terror Financing (Digital Assets)	ATA 1997 (Sec 11/11-O)	FIA/CTD/NACTA/Police	Special Courts/Accountability Courts	Enforcement gap due to lack of enforceable penalties for VASP non-compliance

6. Online Radicalization and The "Chilling Effect"

6.1 The Scope of Digital Glorification (PECA Section 9)

The expansion of transnational terror groups in spreading propaganda online is a worldwide recognized menace with the internet providing low cost instant communication to sell extremist content globally. Organizations such as ISKP particularly use the powerful means of multilingual propaganda campaigns (including Al-Azaim) to increase their reach and recruitment pool (Institute for Economic and Peace, 2025; Whittaker, 2023).

The main statute of the legal action against this menace in Pakistan is PECA Section 9 which criminalizes the glorification of a terrorism related crime, a convicted person or a prohibited organization through electronic means. Punishments to this crime are harsh such as serving a sentence of up to seven years in prison and a huge amount of fines. This is a provision that tries to directly address legislatively the digital spread of extremist ideas that lead to the intricate process of radicalization (Wolfowicz, Litmanovitz, Weisburd, & Hasisi, 2021).

6.2 Area of evaluation PECA Section 9 versus Constitutional Rights

Although there is a valid reason to fight terrorist propaganda, academic criticism is unanimous on the fact that PECA Section 9 has been written too broadly, and creates clauses that threaten constitutional rights to freedom of expression. According to the legal authorities, it is a textbook case of a law that creates a chilling effect and acts as it inhibits the exercise of legal rights in a legitimate way by the mere uncertainty of being approached by prosecution (Arshad Khan, 2018). It puts this over breadth enhancement to a higher degree. It has been shown that law enforcement agencies have utilized PECA sections many times, frequently alongside counter-terrorism requirements, to attack domestic political accounts and dissent. Indicatively, the FIA

counter-terrorism branch has filed charges against political activists claiming that they are propagating propaganda against the state institutions in violation of PECA (Aziz, 2018). This redefinition of a counter-terrorism law against political dissidents poses a severe threat to the legitimacy of anti-radicalization actions and is diametrically opposed to the international human rights requirements, raising serious questions about the capacity of the state to police online speech (Chaudary, 2023).

This confuses the law and results in a critical weakness: a lack of legitimacy. In the event that PECA 9 is regularly utilized in retaliation against political criticism, international organizations and internal judicial systems are strongly motivated to advance all the prosecutions provided by this section with a high degree of skepticism. This criticism unwillingly offers a procedural safe haven to real terrorist propagandists. The perception of the law as draconian and unfair in its application undermines its efficacy in dealing with the targeted populations, of which elaborate militant groups are considered, because legal cases against free speech and due due process become simpler to construct against sophisticated digital content allegations.

6.3 Operative Ineffectiveness

The legal ramification of the overbreadth of PECA is misdirection. The sheer scale of the law, which provides easy prosecution of domestic political targets, pulls away the limited investigative resources otherwise needed to track, map, and repress actual transnational terrorist content (e.g., the geo-fenced, technically complex operations of the Al-Azaim media of the ISKP) (Institute for Economic and Peace, 2025).

Law enforcement priorities are diverted to politically convenient targets rather than to the creation of trend-specific de-radicalization responses that take into account the multifaceted interplay of historical, geopolitical, socioeconomic, and religious factors that contribute to radicalization in Pakistan (Javed, Elahi, & Nawab, 2023). This is an operative misdirection that establishes a negative feedback loop towards security. The enforcement mechanisms targeted at the general population and punitive and rights-violating are part of the extremist discourse of the state oppression and injustice, which may contribute to the sociopolitical risk factors found in the radicalization studies and contribute to the ironic interdependence of the general population with individuals who are likely to be recruited into militant groups (Wolfowicz et al., 2021).

7. Terror Financing and The Fintech Regulatory Deficit

7.1 Legislative Progress

Pakistan has shown its legislative responsiveness to international pressure on the issue of terror financing (TF), especially following the scrutiny by the FATF. One of the legal successes was the 2012 amendment to ATA 1997 that established new definitions that expanded the range of what is considered a financial asset to be seized and prosecuted (Imran & Idrees, 2020). Most importantly, the definition of "money" was broadened to encompass "coins or notes in any currency, postal orders, money orders, bank credits, bank accounts, letters of credit, travelers' cheques, bank cheques, bankers' drafts, in any form, electronic, digital, or otherwise" (Imran & Idrees, 2020).

The necessity of this amendment was to make sure that the legislative framework of the state of Pakistan met the international standards so that the TF offences included all types of the financial assets, both tangible and intangible used to fund terrorist activities, organizations, or individuals regardless of the origin of the funds. This bill was an initial recognition of the menace of digital finance (United Nations Office on Drugs and Crime, 2021).

7.2 Operational Gaps

With this legislative background, there exist serious regulatory gaps in the operational stage, which validates the presence of a ghaston-operational Legislative-Operative Gap (LOG). It has been able to implement high-level preparatory measures having completed its National Risk Assessment (NRA) and Terror Financing Risk Assessment (TFRA). These tests acknowledged the

extreme risk, recognizing the crypto-currency as a high-risk medium of transnational TF (Asia Pacific Group, 2020). The Federal Investigation Agency (FIA) also recognized that new digital finance policy needed a paradigm shift to be in line with FATF Recommendation 15 (R.15) on New Technologies, namely Virtual Assets and Virtual Asset Service Providers (VASPs) (Khan, 2025).

Still, the shift between the identification of risks and their successful implementation is not a fully established one. Though Pakistan has updated manuals (e.g., of Exchange Companies) and also imposed similar requirements on state organizations such as CDNS and Pakistan Post in new AML/CFT Rules to perform risk assessment of new products, these tools have a critical flaw: they are not regarded as the means of enforcement as no penalties in case of non-compliance have been outlined so far (Asia Pacific Group, 2020).

The lack of detail of identified, discouraging penalties is an essential technical compliance failure within the FATF standards (Asia Pacific Group, 2020). FATF recommends a more powerful global response to the problem of illicit finance risks in Virtual Assets, since the jurisdictions themselves continue to struggle with the issue of regulating VASPs (FATF, 2025). The fact that Pakistan has not made enforceable penalties shows that agencies that fall within the confines of the nation, even those that deal with or serve virtual asset platform, have minimal legal deterrent against negligence, or intentional failure to comply with AML/CFT regulations.

7.3 The Enforcement Dilemma

The failure to specify penalties points to a trend where Pakistan has been undertaking fast-tracked, top-down lawmaking efforts (the legislative component of LOG) in order to meet international monitoring urgency needs, such as ensuring that it is not listed on the FATF greylist. It, however, finds itself in the difficulty of the second, tiring, organizational step of establishing strong enforcement capacity (the operational component of LOG). The fact that no particular punitive measures are mentioned in case of non-compliance implies that the whole system of regulations designed to rein in the abuse of virtual assets is a pun-less riddle. The danger is recognized; the procedure is outlined but the deterrent mechanism is absent.

The most severe effect of this shortcoming is the escalation of threats in the future. As the international focus on virtual assets grows, and FATF persistently requires the effective regulation of VASP (FATF, 2025), the porous enforcement situation in Pakistan may slowly become a swarm of more and more attractive nexus of international terror financing. This regulatory gap can be used by transnational militant organizations, such as ISKP and TTP, which are aware that a non-compliant local VASP will receive no more than a procedural penalty, and non-compliance using decentralized digital currencies. Failure to successfully punish non-compliant parties exposes the financial system to digital money transactions exploited by militant organizations, which opens a channel to fund terrorist activities that avoid the normal bank checks.

The following table shows how there was a gap between what is practiced and that what is required internationally:

Table 2 FATF Compliance Gaps in Digital Finance

FATF Recommendation	Requirement	Pakistan's Legal Status (ATA/PECA)	Key Deficiency (Risk/Compliance Gap)
R.5	Criminalization of TF	Criminalized via ATA; "money" definition expanded to include	Operational challenges; judicial consistency issues; enforcement effectiveness cited as suboptimal.

		"electronic, digital or otherwise".	
R.15	New Technologies (VAs/VASPs)	Risk assessed as high/medium-high in NRA/TFRA.[6] Policy proposed for alignment.	New regulatory instruments lack specified, dissuasive penalties, thus failing the FATF test for 'enforceable means'.
UNSCR 2462	Prohibiting funding without link to specific act	Covered by ATA TF provisions.	Difficulties in applying traditional CT measures to decentralized, cross-border VA flows without robust VASP supervision.

8.

Conclusion

This analysis shows that the existing multi-layered legal system of counter-terrorism in Pakistan, which includes the ATA 1997, the procedural legacy of the PPA 2014, and the PECA 2016 is in structural terms incapable of responding to modern digital threats. The main argument, which assumes that the framework is insufficient, inconsistent, and full of conflicts of jurisdiction, is validated through pieces of evidence in three areas of digital security governance.

The legislative-operative gap (LOG) is the source of the structural inadequacy. The lawmaking community reacts to crises and global pressure through amendments (2012 ATA amendments to digital money, PECA was enacted), but the capacity to operate, its coherence, and the implementation mechanism do not match.

This failure is typified by three concomitant shortcomings;

- **Conceptual Inconsistency:** The incoherent definition and extent of ATA (physical harm threshold) and PECA (digital disruption) creates a gray area on the definition of cyber-terrorism that constrains the successful, focused prosecution of critical infrastructure offenses.

- **Rights Failure and Political Misdirection:** The deliberate excessive nature of cyber-laws especially PECA Section 9 contributes to the systematic application of CT mechanisms in policing against political dissent. It is a weakness that the regime is not legitimized, the little resources are not channeled to actual counter-propaganda efforts against organizations such as ISKP, and that it may increase the socio-political forces behind radicalization.

- **Regulatory Enforcement Failure:** The state has failed miserably to define means of enforcement by specifying penalties over non-compliance of VASP despite identifying virtual assets as a high-risk TF vector and enacting regulatory tools (ATA amendments, AML/CFT rules). This leaves a big regulatory loophole that is open to abuse by terror finance networks in the international arena.

The aggregate price of this incongruity and disunity is an increased vulnerability of the nation. The frictional uncertainty of the jurisdiction between the FIA Cyber Crime Wing and the CTD slows down the investigation process, introduces gaps in the procedures, and, eventually, favors advanced digital offenders who take advantage of bureaucratic red tape and lax financial laws.

9. Recommendations

To mitigate the proven risks and close the Legislative-Operative Gap, the following reforms are essential:

9.1 Legislative Consolidation

The present state of the law needs a surgical intervention instead of the gradual amendment by bits. It is advisable that Pakistan should develop and implement one single, comprehensive Digital Counter-Terrorism Act (DCTA) that is specifically confined to the digital arena of militancy and that is expressly intended to be super imprisoned on the already overlapping provisions contained in both the ATA and PECA on the subject of terrorism.

- Narrow Definition: The DCTA should take a very small definition of cyber-terrorism that is internationally harmonized, and it should draw a distinct line between it and generic cybercrime and political dissent, and the emphasis of its consideration should be on the acts that are intended to cause death, significant economic damage or disastrous disruption of explicitly defined critical infrastructure.
- Rights Compliance: PECA Section 9 (Glorification) needs to be repealed or radically revised according to the international human rights standards to ensure that constitutional provisions of free speech are safeguarded and at the same time organized militant propaganda is being properly countered.

Jurisdictional Clarity and Specialization.

The structural issue of endemic jurisdictional conflict between the investigative (FIA/CCW) and security/prosecutorial (CTD/Police) arms needs to be eliminated with centralization and well-defined limits.

- Creation of CCTICs: The government needs to create federally proposed, multi-agency Cyber-CT Investigation Cells (CCTICs), consisting of integrated capabilities, combining the technical forensic skill of the FIA Cyber Crime Wing and operational threat analysis of the CTD and NACTA.
- Definition of thresholds: The DCTA should contain clearly defined legal thresholds explaining when the purely PECA-covered crime (digital intrusion) is to be categorized as a DCTA/ATA crime (terrorist intent) to reduce institutional friction and the lead agency role should always be assigned as soon as a complaint has been registered.

9.3 Regulatory Fintech Enforcement

There is an urgent need to make operational modifications to meet the international compliance requirements and prevent the exploitation of Virtual Assets (VA) to finance the financial ecosystem.

- Enforceable Penalties: To implement precise, extremely deterrent financial and criminal penalties for non-compliance by Virtual Asset Service Providers (VASPs) and other regulated entities (CDNS, Pakistan Post, Exchange Companies) listed in the AML/CFT regulations, immediate legislative action is required. In order to close the established FATF shortfall and turn existing regulatory instruments into "enforceable means," this critical step is necessary.
- Centralized VASP Regulation: In order to move decisively beyond policy proposals to efficient, supervised implementation that satisfies the international standard set by FATF, regulatory oversight of VAs and VASPs must be centralized and strictly enforced, most likely under the State Bank of Pakistan (SBP) or the Securities and Exchange Commission of Pakistan (SECP).

References:

Ahmad, W., Asghar, U., & Afzal, M. (2025). AN ANALYSIS OF THE EFFECTIVENESS OF FIA CYBER CRIME LAWS IN PREVENTING AND INVESTIGATING ONLINE FRAUD IN PAKISTAN: CHALLENGES AND RECOMMENDATIONS. Research Consortium Archive, 3(2), 836-852.

Ali, S. (2023). The Genesis and Development of Anti-Terrorism Policy in Pakistan: A Historical Context. Pakistan Social Sciences Review, 7(3), 539-550.

Amnesty International. (1997). PAKISTAN Legalizing the impermissible: The new anti-terrorism law. Online: Amnesty International.

Arshad Khan, E. (2018). The prevention of electronic crimes act 2016: An analysis. LUMS LJ, 5, 117.

Asia Pacific Group. (2020). Mutual Evaluation of Pakistan. Online: Asia Pacific Group.

Aslam, S., Ashraf, M. A., Mukhtar, M. A., & Ashraf, M. R. (2025). Balancing Free Speech and Counterterrorism: A Legal Analysis of Online Glorification Laws in Pakistan. Annual Methodological Archive Research Review, 3(5), 1-15.

Aziz, F. (2018). Pakistan's cybercrime law: Boon or bane. The Green Political Foundation.

Baezner, M. (2018). Regional rivalry between India-Pakistan: tit-for-tat in cyberspace: ETH Zurich.

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.

Center for Strategic & International Studies, C. (2018). Islamic State Khorasan (IS-K) - TNT Terrorism Backgrounder. https://www.csis.org/programs/former-programs/warfare-irregular-threats-and-terrorism-program-archives/terrorism-backgrounders/islamic

Chaudary, Z. (2023). Human Rights Defenders in the Clutches of Draconian Laws–Curtailment of Constitutional Rights in Pakistan. Islamabad Law Review, 7(2), 42-63.

Durrani, H. (2020). Critical Approach to Pakistan's Counter-terrorism Legislative Framework: McGill University (Canada).

FATF. (2025). FATF urges stronger global action to address Illicit Finance Risks in Virtual Assets. 2025, from https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html

Iftikhar, S. (2024). Cyberterrorism as a global threat: a review on repercussions and countermeasures. PeerJ Computer Science, 10, e1772.

Imran, M., & Idrees, R. Q. (2020). Anti-terrorism legal framework in Pakistan and challenges before the criminal justice system. Pakistan Journal of International Affairs, 3(2), 236-262.

Institute for Economic and Peace. (2025). Global Terrorism Index 2025. Online: IEP.

International Commission of Jurists. (2014). Pakistan: newly enacted counter-terrorism law endangers human rights. https://www.icj.org/pakistan-newly-enacted-counter-terrorism-law-endangers-human-rights/

Javed, A., Elahi, N., & Nawab, B. (2023). Decoding the radicalization puzzle: Uncovering the factors fueling the fire in Pakistan. Pakistan Journal of Terrorism Research, 5(2).

Jawad, A. (2022). An evaluation of Anti-Terrorism laws in Pakistan: Lessons from the past and challenges for the future. Security and Defence Quarterly, 38(2), 16-30.

Khan, H. A. (2025). Pakistan unveils first-ever policy to regulate digital assets in line with FATF guidelines, Arab News. Retrieved from https://www.arabnews.com/node/2596582/pakistan

Lynch, A., McGarrity, N., & Williams, G. (2010). Counter-terrorism and beyond: The culture of law and justice after 9/11: Routledge.

Malik, A. M. (2025). EXPLAINER: How new cybercrime law puts digital rights at stake, Dawn. Retrieved from https://www.dawn.com/news/1889378

Mohammed, F. (2016). PECA 2015: A Critical Analysis of Pakistan's Proposed Cybercrime Bill. UCLA J. Islamic & Near EL, 15, 71.

Rafique, N., & Manan, A. (2019). Countering Measures of Terrorism in Pakistan. Pakistan Journal of Humanities and Social Sciences Research, 2(02), 61-75.

Saiya, N. (2020). On the Need for a New Pluralism in South Asia. Retrieved from https://blogs.lse.ac.uk/religionglobalsociety/2020/12/on-the-need-for-a-new-pluralism-in-south-asia/

Suddle, F. R., Khan, A., & Nawaz, S. (2025). The Legislative Framework for Cybercrime in Pakistan: A Critical Analysis of PECA 2016. Annual Methodological Archive Research Review, 3(8), 1-14.

U.S. Department of State. (2025). Joint Statement on U.S.-Pakistan Counterterrorism Dialogue. https://www.state.gov/releases/office-of-the-spokesperson/2025/08/joint-statement-on-u-s-pakistan-counterterrorism-dialogue

United Nations Office on Drugs and Crime, U. (2021). Counter-Terrorism in the International Law Context. Online: UNODC.

UNODC. (2025). Cyberterrorism. from https://www.unodc.org/e4j/zh/cybercrime/module-14/key-issues/cyberterrorism.html

Waseem, Z. (2024). Inside the Punitive State: Governance Through Punishment in Pakistan. https://carnegieendowment.org/research/2024/06/pakistan-punitive-state-terrorism-police?lang=en

Whittaker, J. (2023). Online radicalisation: what we know.

Wolfowicz, M., Litmanovitz, Y., Weisburd, D., & Hasisi, B. (2021). Cognitive and behavioral radicalization: A systematic review of the putative risk and protective factors. Campbell Systematic Reviews, 17(3), e1174.