ADVANCE SOCIAL SCIENCE ARCHIVE JOURNAL
Available Online: https://assajournal.com
Vol. 05 No. 02. April-June 2026.Page# 8-17
Print ISSN: 3006-2497 Online ISSN: 3006-2500
Platform & Workflow by: Open Journal Systems

Why Pakistan Needs a Graduated Legal-Criminal Justice Response to Digital Radicalisation: Importance, Necessity, and Applications of the AYAZ KHAN Model

Mr. Ayaz Khan
Ph.D. (Law) Research Scholar, Department of Law, Abdul Wali Khan University Mardan Khyber Pakhtunkhwa, Pakistan
ayazkhan.law@awkum.edu.pk
Professor Dr. Muhammad Zubair Khan
Chairman/Supervisor, Department of Law, Abdul Wali Khan University Mardan, Khyber Pakhtunkhwa, Pakistan
mzubair@awkum.edu.pk

ABSTRACT
Digital radicalisation has transformed the legal and institutional landscape of counter-extremism in Pakistan. Online extremist ecosystems now operate through social media, encrypted messaging, video-sharing platforms, and increasingly fragmented digital environments that blur the boundary between protected expression, extremist advocacy, facilitation, and terrorism-linked conduct. Drawing on a wider socio-legal doctoral study, this article explains the importance, necessity, and applied value of the AYAZ KHAN Model, a structured legal-criminal justice framework developed to address digital radicalisation in Pakistan. The article argues that existing law remains fragmented across the Anti-Terrorism Act 1997, the Prevention of Electronic Crimes Act 2016 and its later amendments, regulatory practice, and institutional routines. That fragmentation produces conceptual instability, threshold ambiguity, evidentiary fragility, institutional overlap, and procedural vulnerability. In response, the AYAZ KHAN Model proposes eight integrated components: assessment of risk, yardsticks of legal threshold, authentication and attribution of digital evidence, zoned intervention and response, knowledge-led institutional coordination, human rights and procedural justice safeguards, accountability and appellate review, and neutralization, rehabilitation, and normative reintegration. The article demonstrates why this model is needed, how it improves on both the current Pakistani framework and selected comparative approaches, and where it can be applied across prevention, investigation, prosecution, adjudication, rehabilitation, and policy coordination. It concludes that Pakistan requires not a more punitive but a more coherent, reviewable, and evidence-based response to digital radicalisation.

***Keywords**: Digital Radicalisation, Pakistan, Criminal Justice, Preventive Justice, Digital Evidence, Terrorism Law*

Introduction

Digital communication technologies have altered the ecology of radicalisation. Contemporary extremist mobilization no longer depends only on physical spaces, face-to-face preaching, or organizational cells. It increasingly unfolds through platformed communication, encrypted messaging, algorithmic recommendation systems, cross-platform migration, and digitally sustained communities of grievance and belonging (Aryaeinejad & Scherer, 2024; Scrivens & Gaudette, 2024). For criminal justice systems, this creates a hard question: how can the state respond to harmful online pathways before violence materializes without collapsing the distinction between dangerous conduct and protected belief?

That question is particularly urgent in Pakistan. Pakistan's digital expansion has increased exposure to social media, mobile broadband, and video-sharing environments at the same time that the country continues to confront terrorism, sectarian violence, and institutional distrust. DataReportal estimated 71.7 million social media users in Pakistan in early 2024, while the Institute for Economics & Peace reported that Pakistan remained among the countries most affected by terrorism in the 2025 Global Terrorism Index (DataReportal, 2024; Institute for Economics & Peace, 2025). NACTA has also emphasized

the significance of prevention through the government's National Prevention of Violent Extremism policy process (National Counter Terrorism Authority [NACTA], n.d.-a, n.d.-b).

Yet Pakistan's legal response to online extremism remains fragmented. Relevant provisions are dispersed across the Anti-Terrorism Act 1997 (ATA), the Prevention of Electronic Crimes Act 2016 (PECA), subsequent amendments, platform-blocking practices, criminal procedure, and evidentiary rules. Rights groups and legal commentators have repeatedly warned that this framework contains vagueness, overlap, and procedural weakness, especially where online speech is close to ideological or political expression (Center for Justice, 2023; Digital Rights Foundation, 2025).

This article explains the importance, necessity, and practical application of the AYAZ KHAN Model, the central model derived from the underlying doctoral research from which this article is developed. The article makes three arguments. First, Pakistan needs a new framework because existing law is conceptually unstable and institutionally fragmented. Second, the AYAZ KHAN Model is important because it converts abstract concerns about digital radicalisation into a disciplined, staged, and rights-compatible legal architecture. Third, the model has concrete application across prevention, investigation, prosecution, adjudication, rehabilitation, and governance. In short, the article argues that what Pakistan needs is not simply stronger law, but better law.

Conceptual and Theoretical Foundation

The radicalisation literature consistently warns against conceptual overreach. Radicalisation can refer to ideological hardening, movement toward violence, group affiliation, or a broader shift in identity and political legitimacy. For legal purposes, however, the crucial distinction is between cognitive radicalisation and behavioural radicalisation. A legal system cannot legitimately punish people for holding extreme views as such; it must identify when online behaviour becomes incitement, facilitation, recruitment, or operational preparation (Borum, 2011a, 2011b; Neumann, 2013).

Digital research has also moved beyond the idea that the internet is a passive container for extremist content. Recent work funded by the National Institute of Justice emphasizes that internet and social-media dynamics can shape radicalisation through repeated exposure, network ties, social reinforcement, and interactional processes rather than through content consumption alone (Aryaeinejad & Scherer, 2024). Conway (2017) similarly argues that internet effects vary by user, platform, and context, and should be understood over time rather than as single-cause explanations.

The broader study behind the AYAZ KHAN Model integrated three bodies of theory. Social learning theory helps explain how repeated exposure, observation, symbolic reward, and digital community membership normalize extremist narratives (Bandura, 1977). Preventive justice theory frames the legal dilemma of whether and how the state should intervene before harm fully materializes, while warning against the erosion of legality and due process through excessive anticipatory intervention (Ashworth & Zedner, 2014). Procedural justice theory adds that compliance and institutional legitimacy depend not only on outcomes but also on fairness, neutrality, and reviewability (Tyler, 2003).

The significance of the model lies precisely in this theoretical integration. It treats digital radicalisation neither as speech alone nor as completed terrorism alone. Instead, it understands online extremism as a processual, evidentiary, institutional, and constitutional problem. The model's design therefore aims to preserve the preventive capacity of the state while disciplining that capacity through clear thresholds, evidence, and procedural oversight.

Methodological Basis of the Article

This article is derived from a broader qualitative and socio-legal doctoral study on digital radicalisation and criminal justice in Pakistan. The underlying study combined doctrinal analysis of Pakistani legislation, policy materials, comparative sources, and rights-based critiques with semi-structured interviews conducted across the criminal-justice field. Twenty-three respondents were purposively selected from the judiciary, prosecution services, police and counterterrorism institutions, the FIA, academia, policy bodies, defense practice, and rehabilitation settings. The qualitative design was chosen because the central questions concerned interpretation, institutional judgment, legal thresholds, evidentiary practices, and normative legitimacy rather than prevalence measurement alone.

The doctrinal component examined the Constitution of Pakistan, ATA, PECA, evidentiary rules, and prevention-oriented policy materials. The empirical component explored how criminal-justice actors understand digital radicalisation, where they locate thresholds of liability, what evidentiary problems they face, and why they perceive the current framework as adequate or inadequate. Thematic analysis identified recurring patterns including definitional ambiguity, threshold uncertainty, evidentiary fragility, institutional overlap, due-process concerns, and the underdevelopment of rehabilitation. Those findings became the building blocks of the model discussed in this article.

This methodological background matters because the AYAZ KHAN Model is not merely a conceptual synthesis from secondary literature. It is also a grounded response to institutional experience. Judges emphasized legality and proof, investigators emphasized urgency and platform migration, prosecutors emphasized the difficulty of transforming online traces into convictions, and prevention practitioners emphasized the need for non-penal pathways. The model's importance and necessity therefore arise not only from theory but also from how diverse Pakistani institutions already experience the problem.

At article level, the goal is analytical elaboration rather than full data reproduction. The present paper uses the broader study's insights to explain why the model matters, what legal deficits it addresses, and how it can be used. That makes the article suitable for journals interested in law, criminal justice, security governance, cyber regulation, or socio-legal studies of online extremism.

The Problem with the Existing Framework

The first reason the model is necessary is that the current framework is not truly a framework. It is a collection of overlapping tools. ATA provides terrorism-related offences and special procedures. PECA addresses cyber offences, data misuse, and online harms. Platform restrictions are managed through administrative and regulatory practices. Courts then have to interpret digital evidence through a general evidentiary framework that was not built with rapidly changing, cross-platform, and encrypted environments in mind. The result is uncertainty across every institutional stage.

Doctrinally, the problem is one of legal classification. When does extremist online speech remain protected or merely objectionable? When does it become glorification, hate speech, incitement, facilitation, recruitment, or terrorism-linked conduct? The broader study found that this was one of the most contested issues among respondents from the judiciary, prosecution services, investigation bodies, academia, policy institutions, and rehabilitation settings. That finding aligns with rights-based critiques of Pakistani cyber regulation, which warn that vague offences and broad enforcement powers can create arbitrary or selective application (Center for Justice, 2023; Digital Rights Foundation, 2025).

Institutionally, the framework suffers from fragmented ownership. The Federal Investigation Agency is central to cyber-investigation, Counter Terrorism Departments handle terrorism-linked matters at provincial level, police manage general law-enforcement processes, prosecutors face evidentiary conversion problems, NACTA performs policy coordination, and courts remain the final arbiters of legality. Without a common model, cases may begin under one logic and arrive in court under another. That weakens evidence collection, charge framing, and procedural coherence.

Evidentiary fragility deepens the problem. Digital content can be deleted, altered, fabricated, reposted out of context, or attributed to hacked and pseudonymous accounts. Encrypted platforms such as Telegram create particular investigative obstacles, yet Telegram has become increasingly relevant to extremist propaganda and coordination (Sohail, 2024). Without clear standards for attribution, preservation, chain of custody, and expert testimony, the state risks both failed prosecutions and unjustified interventions.

Finally, the existing system remains too binary. It oscillates between surveillance and punitive prosecution, with insufficient space for structured assessment, targeted prevention, and rehabilitative responses. That is analytically weak because radicalisation is rarely linear; and it is institutionally inefficient because not every online concern requires full criminalization at the outset. Warraich et al. (2023) show that online radicalisation in Pakistan intersects with youth vulnerability, weak opportunity structures, and socio-economic grievance. A system that criminalizes everything too early will likely misclassify risk, while a system that waits too long may miss escalation pathways.

What the Underlying Study Revealed

The broader study revealed a consistent pattern across respondent categories: all recognized digital radicalisation as serious, but they located the problem differently according to institutional role. Judicial respondents emphasized legality, proof, and the danger of criminalizing belief. Investigative respondents emphasized the tempo of online escalation, the difficulty of waiting for explicit incitement, and the way encrypted or closed channels can harden commitment. Prosecutors recognized both sides of the tension, repeatedly stressing that prevention may require early attention while prosecution requires far stronger proof. This triangular disagreement is one of the clearest reasons the model is needed: Pakistan's institutions are often responding to the same online behaviour through different conceptual lenses.

A second finding concerned manifestations and pathways. Respondents described digital radicalisation as a patterned process rather than a single act. They pointed to grievance narratives, emotionally charged victimhood claims, ideological sermon clips, closed-group repetition, and migration from open to encrypted spaces. Importantly, they did not describe the problem as beginning with obvious calls for violence. They described it as beginning with community, reinforcement, and narrative alignment. This matters because a legal framework that looks only for explicit attack planning will overlook early but meaningful shifts in digital behaviour, while a framework that treats every controversial religious or political statement as dangerous will collapse the difference between dissent and extremism.

A third finding involved evidence. Respondents repeatedly warned that online traces generate suspicion more easily than proof. Authorship, context, continuity, and authenticity were constant concerns. Investigators spoke of deleted content, account sharing, pseudonymity, and cross-platform migration. Prosecutors noted that screenshots rarely complete a case. Judges emphasized that ideological anxiety cannot replace evidentiary discipline. The model's authentication and attribution component therefore arises directly from the empirical record rather than abstract doctrinal preference.

Fourth, respondents described institutional overlap as a structural weakness rather than a temporary inconvenience. Cases were said to begin under cybercrime logic, migrate into counterterrorism logic, and arrive in court with neither a stable evidentiary chain nor a coherent legal narrative. Prevention actors also noted that policy talk about violent-extremism prevention often remained disconnected from criminal-process realities. The model's coordination component responds directly to this gap by insisting on shared routing standards and legal continuity.

Finally, the study found substantial support for differentiated response. Even respondents who favored strong early intervention acknowledged that not every exposure case should be handled as completed terrorism. Likewise, respondents strongly critical of overreach did not argue for passivity. What emerged instead was a conditional consensus: Pakistan needs a framework capable of distinguishing cases that require observation, cases that require targeted intervention, and cases that require prosecution. The AYAZ KHAN Model converts that consensus into a usable architecture.

The AYAZ KHAN Model: Core Architecture

The AYAZ KHAN Model was derived to answer these weaknesses through eight interdependent components: Assessment of Digital Radicalisation Risk; Yardsticks of Legal Threshold; Authentication and Attribution of Digital Evidence; Zoned Intervention and Response; Knowledge-Led Institutional Coordination; Human Rights and Procedural Justice Safeguards; Accountability and Appellate Review; and Neutralization, Rehabilitation, and Normative Reintegration. The model is best understood not as a slogan but as a sequence of legal disciplines.

Assessment is the model's starting point because digital radicalisation typically develops through repeated exposure, participation, migration toward more insulated environments, and relational reinforcement. The model therefore rejects an immediate punish-first orientation. It requires structured evaluation of online behavioural indicators, communicative patterns, platform migration, contextual vulnerabilities, and relational markers before coercive escalation.

Yardsticks of legal threshold form the second component. These yardsticks separate protected belief from advocacy, facilitation, and operational conduct. Their purpose is to preserve doctrinal clarity. Without them, the criminal law risks punishing ideology rather than legally actionable conduct. With them, the state can tailor its response to the seriousness and proximity of the conduct involved.

The authentication and attribution component addresses the reality that digital suspicion is not digital proof. The model therefore insists on technical verification, context-sensitive interpretation, chain of custody, and expert standards before online material becomes the basis of criminal liability. This is one of the model's most practically significant features because evidentiary weakness is a recurring source of both acquittal and abuse.

Zoned intervention and response then translate assessment and threshold-setting into operational practice. Lower-risk situations may justify monitoring or voluntary preventive engagement. Intermediate cases may justify disruption, formal investigation, or targeted restriction subject to review. High-risk cases involving incitement, facilitation, recruitment, or operational linkage justify criminal prosecution. The point is proportionality, not leniency.

Knowledge-led coordination addresses fragmentation. It demands shared definitions, case-routing protocols, common evidentiary standards, and institutional continuity across agencies. Human-rights and procedural-justice safeguards embed legality, necessity, proportionality, and fair process across all stages. Accountability and appellate review ensure that decisions remain challengeable and documentable. Finally, neutralization, rehabilitation, and normative reintegration recognize that some cases are best addressed through structured deradicalization, counseling, religious and psychological support, and reintegration rather than perpetual penal management.

Table 1 ***Core Components of the AYAZ KHAN Model***

Component	Core Function	Primary Institutional Value
Assessment	Identifies patterns, vulnerabilities, and escalation indicators before premature criminalization	Improves preventive triage and reduces impressionistic decision-making
Yardsticks	Separates protected belief, advocacy, facilitation, and operational conduct	Stabilizes charging, review, and judicial reasoning
Authentication and attribution	Verifies authorship, context, continuity, and integrity of digital evidence	Improves admissibility and reduces wrongful inference
Zoned intervention	Matches response level to assessed risk and legal threshold	Promotes proportionality and efficient use of coercive powers
Knowledge-led coordination	Creates common case-routing and inter-agency standards	Reduces duplication, overlap, and evidentiary discontinuity
Rights safeguards and accountability	Embeds legality, oversight, review, and remedies	Protects legitimacy and constitutional discipline
Rehabilitation and reintegration	Provides structured non-penal or post-penal pathways where appropriate	Reduces recidivism risk and punitive over-reliance

Why the Model Is Important

The importance of the AYAZ KHAN Model lies first in its conceptual discipline. Pakistan's legal debate has often been trapped between two unsatisfactory positions: either treat online extremism as ordinary speech until it becomes violent, or widen the net so far that vague and politicized enforcement becomes inevitable. The model provides an alternative by structuring judgment around thresholds, evidence, and institutional sequencing. It makes legal reasoning more precise and therefore more defensible.

Second, the model is important because it matches the processual character of digital radicalisation. Online extremist pathways frequently begin with grievance narratives, identity-focused messaging, emotionally charged selective victimhood, and repeated interaction within digital communities before becoming more explicit support for violence (Aryaeinejad & Scherer, 2024; Scrivens & Gaudette, 2024). A framework built only for completed offences is therefore too late, while a framework built only on suspicion is too broad. The model's staged architecture is better aligned with the phenomenon itself.

Third, the model is important because it protects the legitimacy of criminal justice. Tyler's (2003) procedural-justice account is especially relevant here: a system seen as arbitrary, opaque, or ideologically selective will lose social trust and cooperation. In Pakistan, where the legitimacy costs of overbroad counterterrorism practice can be especially high, a model that embeds reviewability and neutral standards is not a luxury. It is a condition of durable enforcement.

Fourth, the model is important because it creates operational coherence. A shared framework reduces the risk that investigators, prosecutors, judges, and policy institutions use different definitions and standards for the same behaviour. That coherence is not merely administrative. It affects the legality of surveillance, the quality of evidence, the framing of charges, and the availability of non-penal alternatives.

Fifth, the model matters comparatively. Selected international approaches offer valuable lessons but also cautionary examples. The EU Digital Services Act emphasizes platform accountability and systemic-risk governance (European Union, 2022). The United Kingdom's Online Safety Act reflects broad regulatory duties over online services (Online Safety Act 2023, 2023). Australia's eSafety architecture demonstrates the value of a specialized online-safety regulator (eSafety Commissioner, n.d.). Yet these approaches do not, by themselves, solve Pakistan's criminal-justice threshold problem. The AYAZ KHAN Model is significant precisely because it is tailored to that problem while learning from comparative practice.

Why the Model Is Necessary in Pakistan

Necessity is a stronger claim than importance, but it is justified here for at least five reasons. The first is terrorism resurgence. The Global Terrorism Index 2025 reported worsening terrorist impact in Pakistan, while transnational and regional militant dynamics continue to affect the country's security environment (Institute for Economics & Peace, 2025). In such a context, digital ecosystems cannot be treated as peripheral. They shape propaganda, recruitment, grievance amplification, and ideological reinforcement.

The second reason is technological reality. Pakistan's expanding internet, smartphone, and social-media environment increases both opportunity and exposure. That does not mean digitalization automatically produces terrorism. It does mean that legal and institutional systems must adapt to the ways in which contemporary extremist ecosystem's function. Research on Pakistan has already linked online radicalisation to youth vulnerability, encrypted communication, and digitally reinforced extremist narratives (Sohail, 2024; Warraich et al., 2023).

The third reason is statutory instability. PECA has already been criticized for vagueness and the risk of misuse, while post-2016 and post-2025 developments have intensified debate over speech regulation, procedural safeguards, and the scope of state discretion (Center for Justice, 2023; Digital Rights Foundation, 2025). Without a model that disciplines interpretation, more law may simply produce more inconsistency.

The fourth reason is evidentiary weakness. Pakistan cannot build a credible response to digital radicalisation on screenshots, decontextualized posts, or weak attribution alone. Any serious framework must address how evidence is generated, preserved, authenticated, and contested. This necessity is heightened by cross-border data storage, encrypted environments, and the growing relevance of virtual-asset financing standards in counterterrorism compliance (Financial Action Task Force [FATF], 2021).

The fifth reason is preventive balance. NACTA's prevention policy direction shows official recognition that violent extremism requires earlier and more structured intervention (NACTA, n.d.-a, n.d.-b). But prevention without legal thresholds and due-process safeguards can become arbitrary, while prosecution without preventive differentiation can become blunt and socially counterproductive. The model is necessary because it connects these two domains instead of forcing Pakistan to choose between them.

Applications of the Model

The model's practical value can be seen across six domains. The first is prevention. Assessment and lower-zone intervention allow authorities to distinguish cases requiring monitoring, referral, counseling, or community engagement from cases requiring immediate criminal escalation. This makes preventive work more rational and less dependent on impressionistic judgments.

The second domain is investigation. Authentication and attribution standards improve the collection and preservation of digital evidence, especially where multiple platforms, anonymous accounts, or encrypted

environments are involved. A model-led approach also helps determine when cyber investigators should retain a case and when a matter should transition to terrorism-focused investigation.

The third domain is prosecution. Yardsticks of legal threshold enable prosecutors to make clearer charging decisions and reduce the risk of overcharging or misclassification. Where the evidence supports Y3 or Y4 conduct, prosecution becomes more doctrinally disciplined. Where the evidence does not meet those thresholds, prosecutors can support alternate non-penal or civil responses instead of stretching criminal law.

The fourth domain is adjudication. Courts benefit from a framework that organizes threshold questions, evidentiary expectations, and procedural safeguards. Rather than approaching every case as a binary choice between dangerousness and acquittal, judges can assess whether the relevant threshold has actually been crossed, whether digital evidence is reliable, and whether state action remained proportionate.

The fifth domain is rehabilitation. The model's final component is especially important in cases of non-operational exposure, early-stage ideological hardening, disengagement, or return from higher-risk pathways. International experience shows that Muslim-majority jurisdictions have experimented with rehabilitation and reintegration strategies with varying levels of coercion and transparency. Pakistan requires a version grounded in legality, voluntariness where possible, and measurable outcomes rather than symbolism alone.

The sixth domain is governance and policy. The model can guide legislative drafting, judicial training, evidentiary reform, inter-agency protocols, and the design of specialized institutions. In this respect it offers not only a litigation framework but also a state-building framework for digital-radicalisation governance.

Comparative Value and Normative Strength

A key virtue of the AYAZ KHAN Model is that it combines lessons from comparative frameworks without transplanting them uncritically. The EU's DSA shows the value of systemic-risk obligations and platform accountability for large online services (European Union, 2022). The UK experience shows the importance and controversy of broad online-harm regulation and the political sensitivity of speech-related standards (Online Safety Act 2023, 2023). Australia's eSafety structure highlights the institutional advantages of a specialized regulator with clear public-facing functions (eSafety Commissioner, n.d.).

The model draws on these lessons while improving on them in three respects. First, it embeds judicial and review mechanisms more explicitly in preventive action. Second, it ties intervention to graduated legal thresholds rather than broad categories of harmfulness alone. Third, it integrates rehabilitation as a formal rather than peripheral part of the response. This gives the model a stronger claim to legality, proportionality, and rights-compatibility in the Pakistani context.

Normatively, the model is also stronger than the status quo because it rejects both punitive excess and naïve non-intervention. It assumes that digital radicalisation is real, serious, and capable of harmful escalation. At the same time, it insists that criminal justice must remain proof-based, bounded, and procedurally fair. That is the essence of legitimate preventive governance.

Responding to Likely Objections

One likely objection is that any preventive model risks normalizing earlier and broader intervention into online speech. That concern is serious, but it does not defeat the AYAZ KHAN Model. In fact, it is one reason for it. The model narrows rather than expands discretion by demanding threshold articulation, documented assessment, evidentiary verification, and reviewable procedures before coercive escalation. The alternative in Pakistan is not a rights-perfect status quo; it is a fragmented system in which vague powers and institutional improvisation may already operate without a coherent discipline.

A second objection is that the model may appear administratively ambitious for a resource-constrained system. Yet fragmentation itself is costly. Failed prosecutions, duplicated investigations, poorly preserved evidence, and unstructured preventive action consume time and public resources without producing stable outcomes. A model that improves routing, standards, and differentiation can therefore be defended on efficiency grounds as well as normative ones. In other words, the real comparison is not

between a costly model and a cost-free present; it is between coordinated reform and recurring institutional waste.

A third objection is that extremist actors will adapt, migrate platforms, and exploit legal safeguards. That is undoubtedly true. But legal systems cannot respond to adaptive threats by abandoning legality. What they can do is create processes that are flexible in application but disciplined in principle. The AYAZ KHAN Model is designed precisely for that balance. Its assessment and zoned-response features allow adaptation to changing technologies, while its threshold and evidence components ensure that adaptation does not become arbitrariness.

A final objection is that the model may be too context-specific to travel beyond Pakistan. Yet that criticism confuses portability with value. The model's doctrinal details are Pakistan-specific, but its core principles graduated thresholds, evidence-based intervention, institutional coordination, procedural safeguards, and rehabilitative integration are relevant to many jurisdictions confronting online extremism under conditions of institutional strain. Pakistan is therefore the model's immediate site of application, not the limit of its analytical significance.

Avenues of Applied Use Beyond Criminal Process

Although the model is built within a criminal-justice frame, its applications extend beyond the courtroom. Universities can use its lower-threshold logic to design referral systems that identify worrying online engagement without automatically securitizing student life. Regulatory and platform-facing agencies can use its threshold distinctions to separate unlawful incitement from objectionable but lawful expression, improving notice, preservation, and review practice. Civil-society prevention programs can use its assessment logic to target support to individuals showing signs of digital isolation, grievance fixation, or movement toward more insulated extremist ecosystems.

The model is also relevant to prison and probation systems. Individuals convicted of terrorism-related offences do not leave the digital environment at the prison gate. A structured approach to post-release supervision, reintegration planning, and online-risk assessment can help distinguish lawful reintegration from renewed extremist networking. Similarly, child-protection and youth-welfare systems can use the model's emphasis on staged escalation to avoid premature criminalization of adolescents whose online behaviour may reflect vulnerability, mimicry, or identity experimentation rather than settled terrorist intent.

Finally, the model has value for legislative interpretation itself. Even before comprehensive reform, judges, prosecutors, and investigators can use the model heuristically: asking what threshold has been crossed, what evidence is actually reliable, what intervention is proportionate, and what review mechanism applies. In this sense the model can begin functioning as a jurisprudential guide before it is fully codified.

Implications for Legislation, Policy, and Scholarship

For legislation, the model implies that reform should move away from vague catch-all offences and toward calibrated definitions linked to legally meaningful thresholds. It also suggests that Pakistan should treat digital evidence reform as central, not peripheral, to cyber and terrorism law. A legal system cannot meaningfully criminalize online extremist conduct if it lacks stable methods for proving authorship, context, and continuity of digital behaviour.

For policy, the model creates a bridge between prevention discourse and criminal-justice practice. NACTA's prevention work can be made more legally robust if it operates with threshold-sensitive referral pathways, while police and prosecutors can act more proportionately if prevention options are formalized rather than informal. In this sense, the model reduces the artificial divide between social prevention and legal response.

For scholarship, the model contributes a Pakistan-specific framework to a field that is often dominated by Euro-American debates. It shows how digital radicalisation should be studied as a socio-legal problem in developing legal systems facing simultaneous pressures of terrorism, rapid digitalization, institutional capacity constraints, and constitutional fragility. That comparative relevance is important because Pakistan is not unique in confronting these tensions, even if its specific legal and political context is distinctive.

Future scholarship should test the model through applied doctrinal analysis, implementation pilots, case-law review, and evaluation of risk-assessment and rehabilitation mechanisms. The present article therefore should be read not as the last word on the subject but as a structured platform for future empirical, doctrinal, and comparative inquiry.

Model-Based Scenarios for Pakistan

To appreciate the model's applied importance, consider three recurring Pakistani scenarios. In the first, a young user begins consuming polarizing and sectarian content, reposts grievance narratives, and joins increasingly closed online communities. Under a traditional binary framework, authorities either ignore the behaviour or attempt to force it into a criminal category prematurely. Under the AYAZ KHAN Model, the case is assessed, thresholder, and placed in an appropriate zone that may involve monitored engagement rather than prosecution. This protects legality while still taking the pattern seriously.

In the second scenario, a user administers channels that glorify attacks, distribute extremist operational manuals, and encourage others to connect with proscribed groups. Here the model directs the system toward a high-threshold response grounded in digital authentication, coordinated investigation, and prosecution. The advantage is that the state is not acting because the content is merely offensive, but because the assessed conduct meets a clearer facilitation or incitement threshold. This strengthens both prosecutorial clarity and judicial defensibility.

In a third scenario, a person disengaging from extremist networks remains digitally visible and vulnerable to re-entry. Current systems often lack structured post-risk management. The model's rehabilitation and reintegration component fills that gap by connecting legal supervision to psychological, educational, and community-based support. These examples show that the model is not simply a theory of law reform. It is a method for sorting real cases more intelligently.

Conclusion

This article has argued that the AYAZ KHAN Model is important because it converts a fragmented and unstable debate into a coherent legal architecture; necessary because Pakistan's digital, legal, and security environment has outgrown the current patchwork approach; and practically useful because it can be applied across prevention, investigation, prosecution, adjudication, rehabilitation, and governance. The model's central contribution is not severity. It is disciplined differentiation.

Pakistan's challenge is not simply to respond to online extremism more forcefully. It is to respond more intelligently. That means understanding digital radicalisation as a process, setting explicit legal thresholds, strengthening digital evidence standards, coordinating institutions, preserving procedural legitimacy, and reserving criminal punishment for conduct that genuinely justifies it. In that sense, the AYAZ KHAN Model offers a pathway toward a more coherent, rights-compatible, and operationally credible criminal-justice response to digital radicalisation in Pakistan.

References

Anti-Terrorism Act, 1997 (Act XXVII of 1997) (Pakistan).

Aryaeinejad, K., & Scherer, T. L. (2024). The role of the internet and social media on radicalization: What research sponsored by the National Institute of Justice tells us (NCJ 305797). National Institute of Justice. https://www.ojp.gov/pdffiles1/nij/305797.pdf

Ashworth, A., & Zedner, L. (2014). Preventive justice. Oxford University Press.

Bandura, A. (1977). Social learning theory. Prentice Hall.

Borum, R. (2011a). Radicalization into violent extremism I: A review of social science theories. Journal of Strategic Security, 4(4), 7-36. https://doi.org/10.5038/1944-0472.4.4.1

Borum, R. (2011b). Radicalization into violent extremism II: A review of conceptual models and empirical research. Journal of Strategic Security, 4(4), 37-62. https://doi.org/10.5038/1944-0472.4.4.2

Center for Justice. (2023). Section 20 of Pakistan's Prevention of Electronic Crimes Act: Urgent reforms needed. Clooney Foundation for Justice. https://cfj.org/wp-content/uploads/2023/10/Pakistan_PECA-Report_September-2023.pdf

Conway, M. (2017). Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research. Studies in Conflict & Terrorism, 40(1), 77-98. https://doi.org/10.1080/1057610X.2016.1157408

DataReportal. (2024). Digital 2024: Pakistan. https://datareportal.com/reports/digital-2024-pakistan
Digital Rights Foundation. (2025). The Prevention of Electronic Crimes (Amendment) Act, 2025: Analysis and recommendations.
https://digitalrightsfoundation.pk/wp-content/uploads/2025/01/The-Prevention-of-Electronic-Crimes-Amendment-Act-2025-DRF-Analysis-and-Recommendations.pdf
eSafety Commissioner. (n.d.). What we do. https://www.esafety.gov.au/about-us/what-we-do
European Union. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services (Digital Services Act). Official Journal of the European Union, L 277, 1-102. https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng
Financial Action Task Force. (2021). Updated guidance for a risk-based approach to virtual assets and virtual asset service providers.
https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html
Institute for Economics & Peace. (2025). Global Terrorism Index 2025: Measuring the impact of terrorism.
https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf
National Counter Terrorism Authority. (n.d.-a). Message from the National Coordinator.
https://www.nacta.gov.pk/message-from-the-national-coordinator/
National Counter Terrorism Authority. (n.d.-b). NCVEP policy. https://nacta.gov.pk/functions/p-cve-wing/ce/ncvep-policy/
Neumann, P. R. (2013). The trouble with radicalization. International Affairs, 89(4), 873-893. https://doi.org/10.1111/1468-2346.12049
Online Safety Act 2023, c. 50 (UK). https://www.legislation.gov.uk/ukpga/2023/50/contents
Prevention of Electronic Crimes Act, 2016 (Act XL of 2016) (Pakistan).
https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Jvbp8%3D-sg-jjjjjjjjjjjj
Scrivens, R., & Gaudette, T. (2024). Online terrorism and violent extremism. In Oxford Research Encyclopedia of Criminology and Criminal Justice. Oxford University Press.
https://doi.org/10.1093/acrefore/9780190264079.013.795
Sohail, S. (2024). Exploiting encrypted networks: A CPM analysis of Telegram's role in extremist propaganda and radicalization by terrorist organizations. Pakistan Journal of Terrorism Research, 6(2), 45-68. https://pjtr.nacta.gov.pk/index.php/Journals/article/view/140
Tyler, T. R. (2003). Procedural justice, legitimacy, and the effective rule of law. In M. Tonry (Ed.), Crime and justice: A review of research (Vol. 30, pp. 283-357). University of Chicago Press.
Warraich, S. K., Haider, A., & Mukhtar, A. (2023). Online radicalization in Pakistan: A case study of youth in South Punjab. Journal of Politics and International Studies, 9(1), 147-157.
https://jpis.pu.edu.pk/45/article/view/137