

The Use of AI for Predictive Intelligence in Pakistan's Fight against Terrorism

Haider Hasan Tiwana

Department of Marketing & Business, Bahria University, Islamabad, Pakistan
mhaiderhasan@gmail.com

Shamaila Amir

Former Instructor, NUST, Karachi Campus, Karachi Pakistan.
shaminhasan@hotmail.com

Abstract

Pakistan faces continued challenges in national security and counterterrorism as terrorism continues to rise. To conduct effective national security and terrorist activities, the country must implement cutting-edge technical approaches and solutions. Artificial intelligence (AI) has the potential to be a game changer in intelligence collecting, predictive analytics, and threat prevention, just as it has in other fields. As a result, this article examines predictive intelligence, which can be powered by artificial intelligence in the country's anti-terrorism efforts. The study focuses on the potential role of artificial intelligence (AI) in surveillance, data, cybersecurity, and terrorist threat prediction. First, it analyses the country's efforts and then it compares them with global practices for counterterrorism, especially the United States, China, and Israel, highlighting the AI-associated risks. This analysis, findings, conclusion and recommendations suggest that the country needs to maximise AI's effectiveness in counterterrorism and invest in its infrastructure. The recommendations specifically suggest that public-private partnerships and the development of suitable ethical frameworks are required for the deployment of any AI measure. Also, the AI-driven collaborations are required to be developed with various intelligence agencies of the region and globally to boost security measures. These are the only possibilities with which the country can reshape counterterrorism efforts with the help of AI.

Keywords: *Artificial Intelligence, AI, predictive intelligence, Pakistan, terrorism, predictive modelling, cyber security, surveillance, data analytics, etc.*

Introduction

Traditional counterterrorism strategies, which are primarily reliant on human intelligence (HUMINT) and signals intelligence (SIGINT), have always faced certain limitations in addressing dynamic threats effectively. Terrorist organisations have adopted sophisticated methods because of the rapid advancement of technology, including encrypted communications and cyber warfare tactics, which often outpace conventional intelligence approaches (Zia, 2021). This technological evolution necessitates the integration of advanced tools to enhance predictive capabilities and preempt potential attacks. Yet for security efforts, AI has emerged as a pivotal asset for counterterrorism, enabling them to carry out predictive intelligence, big data analytics, and natural language processing (NLP forthwith) to analyse extensive datasets, identify patterns, and forecast potential terrorist activities. AI processes information from social media, financial transactions, and communication networks, and this enhances the ability of security agencies to proactively

detect and disrupt threats. Surveillance carried out with the help of AI systems can help to analyse real-time data for the identification of suspicious behaviours, and security forces can pinpoint potential hotspots for terrorist activities with the help of predictive modelling (Wasil et al., 2024; Clarke & Knake, 2019).

Pakistan has long been stuck in the war against terrorism, facing threats from several extremist groups such as the Tehreek-e-Taliban Pakistan (TTP forthwith) and the Baloch Liberation Army (BLA). 2024 was the year when Pakistan witnessed significantly escalated terrorist activities. At least 685 security personnel lost their lives in 444 different attacks, and the year was not only marked as the deadliest year for Pakistani security forces but also indicated the complex and evolving nature of terrorism within the country (Sattar, 2025; Junaidi, 2024; Khan, 2024a; Khan, 2024b).

With the surge of terrorism in Pakistan, the adoption of AI for counterterrorism also gained momentum. The National Counter Terrorism Authority (NACTA forthwith) initiated training programs focused on advanced crime analytics and AI models to combat terrorism (NACTA, 2024), to equip analysts with the skills necessary to utilise AI effectively in identifying and countering extremist threats (UNODC, 2023). However, the implementation of AI-driven solutions was not without challenges. There was a major issue with technical limitations, e.g., the requirement of a robust data infrastructure, legal and ethical concerns (Montasari, 2024a) regarding surveillance and privacy, and financial constraints. These were the major factors that contributed towards the difficulties towards the effective adoption of AI for counterterrorism operations in the country (UN Counter-Terrorism Centre & UNICRI, 2020).

The focus of this paper, therefore, is to explore the utilisation of AI-driven predictive intelligence to boost Pakistan's struggle with counterterrorism. Further, it analyses various terrorism threats and challenges that the country is facing in its efforts to counter terrorism. The comparison with global practices and assessment of Pakistan's terrorism context helps the study to provide valuable insights into the effective harnessing of AI for national security and addressing ethical and operational perspectives.

Research Methodology

A qualitative methodology was adopted to analyse Pakistan's counterterrorism efforts with an incorporation of a multi-method approach for this study that included content analysis and case studies to provide a comprehensive understanding of the research area under consideration. The research design followed an exploratory and analytical investigation of AI integration into the country's counterterrorism strategies through diverse secondary data from open sources. It analysed reports from the NACTA, FATF, the United Nations Office on Drugs and Crime (UNODC), and UN Counter-Terrorism Centre & UNICRI, peer-reviewed journal articles and books on AI, predictive intelligence, and counterterrorism, and reports from credible news agencies to ensure no bias in findings.¹

¹ The views and opinions expressed or implied in this article are those of the author and should not be construed as carrying the official stance of the Pakistan Army, Air Force, Navy, or other agencies or departments of the government of Pakistan or their international equivalents.

The study also adopted a case study approach for a comparative analysis of global AI counterterrorism strategies. In this regard, the case studies of AI use in the United States, China, and Israel were examined to compare best practices. Moreover, Pakistan-specific case studies of instances of AI-driven counterterrorism operations in Pakistan were analysed to evaluate their effectiveness.

The Data was analysed through thematic analysis to identify recurring patterns and trends in AI-driven counterterrorism efforts. Findings from Pakistan were compared with global best practices to assess the gaps and opportunities. A SWOT² analysis was used to evaluate Pakistan's AI capabilities in counterterrorism. The study acknowledged the limitations of AI-based counterterrorism, particularly regarding privacy and human rights concerns. Some AI-driven counterterrorism initiatives in Pakistan may be classified, limiting access to detailed operational insights. Moreover, since AI adoption in Pakistan's counterterrorism is relatively recent, limited quantitative studies were found available. Also, counterterrorism policies are influenced by geopolitical considerations, making it challenging to assess AI applications in isolation from broader security dynamics. However, despite these limitations, this methodology ensured a holistic and evidence-based approach to analysing AI's role in counterterrorism in Pakistan, offering insights grounded in academic, policy, and operational perspectives.

Understanding Predictive Intelligence and AI in Counterterrorism:

AI-powered tools such as Facial Recognition, Machine Learning (ML) algorithms, and NLP have enabled security agencies to anticipate terrorist activities, identify extremist networks, and prevent attacks. By analysing vast datasets from communications, financial transactions, and social media, AI enhances intelligence efficiency and strategic decision-making. However, despite its potential, the implementation of AI in counterterrorism faces significant challenges, including technical limitations, ethical concerns, financial constraints, and geopolitical dependencies (Montasari, 2024a).

In the modern era, traditional counterterrorism strategies often struggle to keep pace with the dynamic and decentralised nature of terrorist networks (Wall, 2025). Predictive Intelligence is probably the greatest benefit of the use of AI for counterterrorism because security forces, with the help of algorithms, are now able to process vast amounts of data, identify patterns, and predict potential threats with greater accuracy (Wasil et al., 2024). The key components of predictive intelligence are 1) Data Collection & Integration, i.e. open-source intelligence (OSINT), classified government reports, social media monitoring, satellite imagery, and communication intercepts, 2) Data Processing & Machine Learning, i.e. patterns analyzed by AI-driven models in historical and real-time data to detect anomalies and predict threats, 3) Pattern Recognition & Anomaly Detection, i.e. identifying suspicious behavior, unusual transactions, or movements linked to potential terrorist activities and 4) Automated Decision Support Systems, i.e. seeking insights through AI tools allowing intelligence agencies proactive counterterrorism measures (Ganor, 2021; Khan et al., 2023; Maguire & Westbrook, 2025). Predictive intelligence reduces reaction

² Strengths, Weaknesses, Opportunities, and Threats

time, allowing law enforcement agencies to disrupt attacks before they occur rather than responding after an incident has already taken place (Wasil et al., 2024).

AI has transformed counterterrorism operations by enhancing the efficiency and accuracy of threat detection. Unlike traditional intelligence methods, AI can process enormous datasets in real-time, offering security forces an unparalleled advantage in identifying and neutralising threats (Wall, 2025). There are several AI-powered technologies used in counterterrorism. The *ML Algorithms* system is used to continuously learn from past terrorist attacks and intelligence reports to refine threat predictions (Mahesh, 2020). *NLP* is used to analyse extremist propaganda, detect radicalisation trends, and monitor online recruitment activities (Chowdhury, 2003; Nadkarni et al., 2011). *Facial Recognition & Biometrics* systems help track and identify terrorists across borders (Gates, 2006). *Predictive Policing* forecasts crime-prone areas and potential terrorist activities based on historical crime data (Mugari & Obioha, 2021; Agnew, 2016; Šaljić & Tomić, 2024). *The Cyber Threat Intelligence* system helps to enhance cybersecurity by detecting and preventing terrorist cyber-attacks on critical infrastructure (Lee, 2023). The U.S. National Security Agency (NSA) employs AI-driven predictive intelligence tools to analyse global communication networks and detect potential terrorist threats. Programs like PRISM and XKeyscore use AI algorithms to process vast amounts of metadata, allowing security agencies to identify suspicious activities before an attack occurs (Javed, 2023).

Pakistan has faced persistent threats from terrorist organisations such as the TTP, Al-Qaeda, ISIS-K, and Baloch separatist groups. In response, the government has begun integrating AI-driven predictive intelligence into its counterterrorism framework. One of the important AI systems used in Pakistan was launched by NACTA (NACTA, 2021). This AI-powered surveillance program helps to track extremist activities online and identify radicalisation trends. For border security, AI-enhanced surveillance drones and facial recognition systems are being deployed at sensitive border regions to detect militant infiltrations. Pakistani law enforcement agencies are using AI-driven cybersecurity measures to combat online terrorist recruitment and extremist propaganda. However, AI integration in Pakistan's counterterrorism efforts is still in its early stages, facing challenges such as limited technical expertise, inadequate infrastructure, and legal constraints on AI deployment in intelligence operations.

The implementation of AI in counterterrorism offers multiple advantages. It allows security forces to identify potential threats before they escalate into violent attacks. Real-time intelligence enables law enforcement agencies to act swiftly against terrorist cells (Tuteja & Marwaha, 2023). AI-driven analysis reduces Human Error and eliminates bias and fatigue, which can affect human intelligence officers. AI-powered surveillance improves the monitoring of cross-border terrorist movements, enhancing border security (Shahzad & Khan, 2024). Lastly, Combating Online Extremism has become possible through AI algorithms that help to track, flag, and remove terrorist content from social media platforms (Wall, 2025).

Despite its advantages, the use of AI in predictive intelligence also presents significant challenges and ethical dilemmas. AI-driven surveillance programs can infringe on civil liberties and privacy rights, leading to potential misuse by authoritarian regimes. The balance between national security and individual privacy remains a contentious issue. AI models may also exhibit bias due to flawed training data, leading to wrongful profiling of individuals or communities (Wasil et al., 2024). If not properly regulated, AI-based counterterrorism measures can disproportionately target certain ethnic or religious groups (Akilli, 2024). AI requires high-quality

data for accurate threat prediction. However, in developing countries like Pakistan, data collection is often fragmented and unreliable. Limited cyber infrastructure hampers the full deployment of AI-driven intelligence systems. Financial and technological constraints are the biggest challenge as AI implementation requires significant investment in infrastructure, expertise, and cybersecurity measures, which many developing nations struggle to afford. Pakistan faces budgetary constraints that always hinder large-scale AI adoption in counterterrorism operations.

The Terrorism Landscape in Pakistan:

Pakistan has long grappled with terrorism, facing threats from various militant groups operating both domestically and across its borders. The country's strategic location, historical conflicts, and socio-political dynamics have contributed to the proliferation of extremist organisations, many of which have global affiliations (Lodhi, 2024). Despite extensive counterterrorism efforts, Pakistan continues to face evolving security threats, necessitating the adoption of advanced intelligence solutions, including AI and predictive analytics.

Several militant organisations have been active in Pakistan, each with distinct objectives, ideological foundations, and operational strategies. The most prominent groups include the TTP, an umbrella organisation of various militant factions that emerged in 2007. It seeks to overthrow the Pakistani government and impose its version of Sharia law. The group has carried out high-profile attacks, including the 2014 Peshawar school massacre, which killed over 140 people, mostly children (Javed, 2023). In recent years, TTP has regained strength due to the Taliban's resurgence in Afghanistan, utilising cross-border sanctuaries for planning attacks in Pakistan (Junaidi, 2024; Ko & Jilani, 2025). Another organisation, The Islamic State – Khorasan Province (ISIS-K) is the regional affiliate of ISIS, active in Pakistan and Afghanistan. It primarily targets Pakistani security forces, religious minorities, and public spaces through suicide bombings and assassinations. ISIS-K has engaged in deadly rivalries with TTP and the Afghan Taliban, despite ideological similarities (Ko & Jilani, 2025; Giustozzi, 2022). The group poses an increasing cyber threat, using online radicalisation to recruit Pakistani youth (Javed, 2023). The Balochistan Liberation Army (BLA) is a separatist militant group advocating for an independent Balochistan. It has carried out attacks on Chinese interests, particularly targeting the China-Pakistan Economic Corridor (CPEC), as well as military installations (Abbas, 2021). BLA operates in small, well-coordinated cells, using guerrilla warfare tactics against security forces (Lodhi, 2024; Junaidi, 2024). Lashkar-e-Jhangvi (LeJ) is an extremist Sunni militant group responsible for sectarian violence, particularly against Pakistan's Shia Muslim population. Other groups, such as Sipah-e-Sahaba Pakistan (SSP) and Jundullah, also engage in sectarian attacks, increasing inter-communal tensions (Khan, 2024a; Khan, 2024b; Gul, 2023; Javed, 2023). These groups, though distinct in their goals, frequently overlap in networks, training, and financing, making counterterrorism efforts more complex.

Pakistan's security challenges are exacerbated by both external factors (cross-border terrorism) and internal radicalisation. The porous Afghanistan-Pakistan border (Durand Line) has historically served as a haven for militant groups. Following the U.S. withdrawal from Afghanistan in 2021, Pakistan has witnessed a rise in cross-border terrorist attacks, particularly from TTP and ISIS-K (Lodhi, 2024). The influence of Indian intelligence agencies, particularly through alleged

support for Baloch insurgents, has been a point of contention between Pakistan and India (Khan, 2024a; Khan, 2024b; Gul, 2023; Abbas, 2021). Madrassa networks and extremist propaganda continue to fuel radicalisation, particularly among youth in conflict-prone regions. The rise of online extremism has enabled groups like ISIS-K to recruit members through social media and encrypted messaging apps (Weimann, 2015). Economic instability and lack of education create an environment where extremist narratives easily take root (Mehdi, 2019).

Pakistan has implemented various counterterrorism strategies, including military operations and legislative measures. However, traditional methods face significant challenges. Pakistan has conducted major anti-terror operations, such as Zarb-e-Azb (in 2014) and Radd-ul-Fasaad (in 2017). While these operations successfully dismantled militant strongholds, groups like TTP have re-emerged in tribal regions (Javed, 2023). Pakistan's counterterrorism efforts involve multiple agencies (ISI, FIA, CTD, NACTA), but lack centralised intelligence-sharing. Delayed threat assessments often allow militants to evade capture (Shahzad & Khan, 2024). Weak prosecution and delayed trials result in low conviction rates for arrested terrorists. The Financial Action Task Force (FATF) has repeatedly flagged Pakistan for weaknesses in anti-money laundering measures related to terror financing (Lodhi, 2024). Political instability often affects counterterrorism efforts, as peace talks with militant groups (such as the 2022 TTP negotiations) have undermined military gains (Junaidi, 2024). Human rights concerns arise from extrajudicial killings and enforced disappearances, complicating Pakistan's global counterterrorism image (Ünver, 2024).

Given the evolving nature of terrorism, Pakistan must move beyond traditional counterterrorism tactics and invest in advanced intelligence solutions to anticipate and prevent attacks. AI can analyse big data from multiple sources, including social media, satellite imagery, and financial transactions, to detect terrorist activities before execution (Mir, 2018; Junaidi, 2024). Facial recognition and biometric tracking can improve counterterrorism surveillance (Giustozzi, 2022). AI-driven tools can detect and block extremist content online, preventing youth radicalisation (Weimann, 2015). Community-based de-radicalisation programs must be strengthened to rehabilitate former militants. Pakistan must develop a centralised counterterrorism database to improve real-time intelligence sharing among security agencies. International partnerships with China, the U.S., and Middle Eastern allies can provide technical assistance in intelligence gathering.

AI Applications in Pakistan's Counterterrorism Efforts:

The adoption of AI-powered surveillance technologies has transformed Pakistani security forces' monitoring capabilities. Authorities can perform real-time video stream analysis by combining AI with current Closed-Circuit Television (CCTV) networks, allowing them to quickly identify suspicious behaviors and individuals. Facial recognition technology, in particular, has been helpful in cross-referencing camera-captured faces with criminal databases, allowing offenders to be apprehended quickly. Furthermore, the introduction of AI-equipped drones has broadened surveillance coverage, particularly in distant or high-risk areas where traditional monitoring is difficult. These drones can collect high-resolution photos and videos, which AI algorithms may then analyze to identify strange patterns or motions that may indicate terrorist

activity. The use of biometric data improves the accuracy of these systems, ensuring that persons are appropriately identified and followed across several surveillance platforms (NACTA, 2023).

The massive volume of data created daily is both a burden and an opportunity for counterterrorism activities. AI-powered big data analytics enables the processing and analysis of enormous datasets to reveal hidden patterns and linkages that could indicate terrorist planning or operations (Tuteja & Marwaha, 2023). AI systems can detect networks and behaviors associated with extremist activities by analyzing communication records, financial transactions, and social media connections. For example, analyzing financial data can identify abnormal transactions that could point to financing sources for terrorist organizations. Similarly, monitoring social media platforms enables the discovery of radicalization tendencies and the identification of individuals who may be vulnerable to extremist views. These findings are invaluable for preemptive responses and disrupting possible dangers before they occur (Anwar et al., 2020; FATF, 2021).

Predictive modeling uses past data to estimate probable terrorist activity and identify geographical locations that are more likely to be attacked. AI algorithms use historical data, socioeconomic indices, and other pertinent variables to provide risk estimates for various places. This preemptive approach allows security organizations to better deploy resources, focusing on locations with higher threat levels. By anticipating future hotspots, law enforcement can take targeted steps such as increased patrols, community involvement initiatives, and fortification of susceptible areas. This method not only improves the efficiency of counterterrorism operations, but it also generates a sense of security among the population (McKendrick, 2019).

The spread of extremist content online demands effective procedures for monitoring and fighting radical narratives. NLP, a subset of AI, plays an important role in this sector by analyzing textual data to detect and evaluate extremist propaganda. NLP algorithms can search massive amounts of online content, such as social media posts, forums, and messaging platforms, for language patterns and keywords related with radicalization.

Once identified, this content can be flagged for further investigation or removed to prevent the spread of extremist ideologies. Moreover, NLP facilitates the development of counter-narratives by understanding the linguistic nuances of extremist propaganda, enabling the creation of targeted messages that resonate with at-risk individuals and communities.

The digital landscape has become a battleground for counterterrorism, with terrorist organisations exploiting cyberspace for recruitment, communication, and planning (Montasari, 2024b). AI-enhanced cybersecurity measures are essential to detect and neutralise these online threats. ML algorithms can identify anomalies in network traffic, signalling potential cyber-attacks or unauthorised access attempts by malicious entities (Weimann, 2015; Brundage et al., 2018).

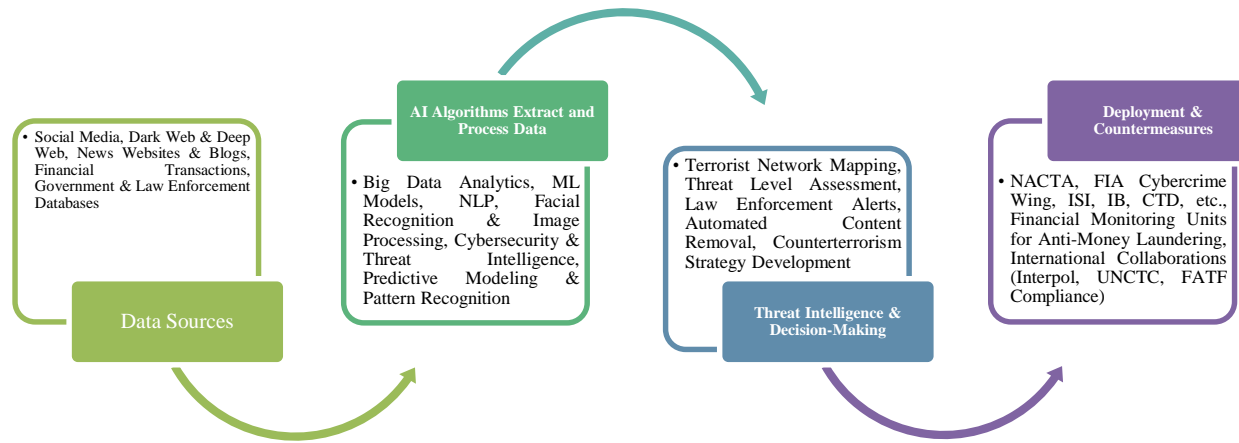
Figure 1: AI-generated figure for Pakistan's Use of AI for Analysing Data Available on the Internet



Furthermore, AI helps to trace terrorist networks' digital traces, disclose their online infrastructure, and disrupt their operations. By automating the examination of huge cybersecurity data, AI reduces response times and improves the precision of threat detection, thus defending key infrastructure and sensitive information from terrorist exploitation (Stanford University, 2024).

While AI offers significant advantages in counterterrorism, its implementation is not without challenges. Concerns regarding privacy infringement arise from extensive surveillance and data collection. Ensuring that AI systems operate within the bounds of legal and ethical standards is paramount to maintaining public trust and upholding civil liberties (Wall, 2025). Additionally, the effectiveness of AI applications depends on the quality and representativeness of the data they process. Biases in data can lead to inaccurate predictions and unjust outcomes, such as the misidentification of individuals or communities as security threats. Therefore, continuous evaluation and refinement of AI systems are necessary to mitigate these risks and enhance their reliability (Stanford University, 2024).

Figure 2: Framework of AI-Driven Internet Data Analysis for Counterterrorism in Pakistan
(Author’s courtesy)



Case Studies and Real-World Implementations:

NACTA has been at the forefront of Pakistan’s counterterrorism efforts, leveraging AI to enhance intelligence gathering and threat prediction. NACTA has worked on AI-driven predictive analytics, monitoring terrorist networks through big data analysis, cyber intelligence, and social media tracking (Baig, 2024). AI-assisted tools analyse online extremist rhetoric, helping security agencies track and prevent radicalisation. Furthermore, NACTA has initiated data-sharing protocols with law enforcement agencies, using ML models to identify high-risk individuals and locations (Rashid, 2023a). Such AI-powered threat assessment frameworks improve preemptive actions against terrorist threats.

Pakistan’s ISI and FIA play a critical role in integrating AI into counterterrorism operations. FIA’s Cyber Crime Wing (CCW) employs AI for digital forensics, monitoring suspicious financial transactions, and disrupting cyber threats (Bhatti & Shahrukh, 2023). AI-powered facial recognition systems have been deployed at airports and key security points, significantly enhancing border security and tracking wanted individuals (Baig, 2024). ISI, known for its covert intelligence operations, has expanded its capabilities using AI-driven signal intelligence (SIGINT) and NLP to detect online radicalisation and encrypted terrorist communications (Rashid, 2024; Shahzad & Khan, 2024). These systems process vast amounts of intercepted digital communication to identify potential threats before they materialise.

The National Security Agency (NSA) in the United States is one of the most advanced intelligence bodies utilising AI for predictive counterterrorism. NSA’s Artificial Intelligence and Data Analytics (AIDA) Division employs machine learning, neural networks, and automated surveillance to monitor global threats in real time (Rassler, 2021; Zegart, 2022). Through partnerships with the Department of Homeland Security (DHS) and the FBI, AI models analyse social media behaviour, biometric data, and communication patterns to preemptively thwart terrorist plots (Baig, 2024). The U.S. military’s Project Maven is another example of using computer vision and AI-powered drones to conduct precision strikes against terrorist groups in the Middle East and South Asia (Pellerin, 2017; Strout, 2022; Rosenberg, 2022). These AI applications

significantly reduce human error in identifying terrorist targets while ensuring efficient threat neutralisation.

China has integrated AI-powered facial recognition, biometric tracking, and predictive policing in the Xinjiang region to counter terrorism threats, particularly against Uyghur separatist movements (Stark, 2021; Zhao, 2022a). The Integrated Joint Operations Platform (IJOP) processes real-time data from surveillance cameras, mobile devices, and public transactions to detect “suspicious” activity (Wright et al., 2023a). While highly effective in crime prediction, China’s AI-based counterterrorism policies have also been criticised for mass surveillance and human rights concerns (Stark, 2021; Ünver, 2024). The extensive use of AI-driven social credit scoring and predictive law enforcement raises ethical debates about privacy infringement and over-policing (Mazzocco, 2022; Wall, 2025).

Israel has pioneered AI-driven intelligence through its Unit 8200, the Israel Defence Forces’ cyber-intelligence unit. Israeli AI models integrate geospatial intelligence (GEOINT), drone-based AI tracking, and deep learning algorithms to detect and neutralise terrorist threats. One of Israel’s notable AI systems is “Gospel”, a predictive intelligence framework that uses big data analytics and AI-driven behavioural analysis to anticipate terrorist attacks. Another AI initiative is “The Edge”, a deep learning-powered reconnaissance system that provides real-time counterterrorism intelligence to field operatives (Tunysová, 2022; Serhan, 2024; Davies & Abraham, 2025).

There can be several lessons for Pakistan from Global AI Counterterrorism Strategies. Pakistan can enhance inter-agency AI coordination similar to the NSA-DHS-FBI partnership in the U.S. Lessons from China’s IJOP can be applied with ethical safeguards to predict terrorist activities proactively. Adopting Israel’s AI-based military surveillance can improve Pakistan’s border security operations. ISI and FIA can replicate Unit 8200’s AI-based cyber operations to counter extremist propaganda online.

Challenges in AI Implementation for Counterterrorism in Pakistan:

The integration of AI in counterterrorism operations presents significant opportunities for Pakistan. However, several challenges hinder its effective deployment. These obstacles range from technological limitations and financial constraints to ethical dilemmas and legal ambiguities. This section explores the key challenges in AI implementation for counterterrorism in Pakistan and suggests potential solutions.

- i. **Limited AI Expertise and Research Capabilities:** Pakistan lacks a robust AI research and development ecosystem, making it difficult to implement cutting-edge AI-driven counterterrorism tools. Unlike developed nations, Pakistan has limited AI professionals, cybersecurity experts, and data scientists trained to develop and manage AI-based security systems (Baig, 2024; Shahzad & Khan, 2024). A notable instance highlighting these challenges is the 2023 incident involving the sophisticated use of AI-generated deepfake audio by cybercriminals, bypassing voice authentication systems in several banks. They successfully exploited AI to impersonate bank officials, leading to unauthorised transactions of approximately 450M PKR. (Hussain, 2025; Business Recorder, 2023; Stratheia, 2025; Pakistan Today, 2025; Jaleel, 2024; Ideal Solutions, 2023).

- ii. **Insufficient Computational Power and Data Centers:** Pakistan's technological infrastructure has limited AI-ready computing power, high-performance computing (HPC), cloud infrastructure, and advanced algorithms to process vast amounts of intelligence data (Rashid, 2023a), dedicated AI research labs and secure cloud storage systems which slows down real-time AI analysis, and prompt detection and counteract of terrorist threats (Bhatti & Shahrukh, 2023). While initiatives like the National Centre of Artificial Intelligence (NCAI) and the Sino-Pak Centre for Artificial Intelligence (SPCAI) have been established to promote AI research, their impact is constrained by limited resources and infrastructure. For instance, the SPCAI at PAF-IAST is developing a high-performance computing facility based on NVIDIA Tesla V100 GPU clusters. However, such facilities are exceptions rather than the norm, and many institutions lack the necessary infrastructure to support advanced AI research and applications. This disparity hinders the development and deployment of AI-driven counterterrorism tools across the country (Business Recorder, 2024, PAF-IAST, n. d.; NCAI, 2022).
- iii. **Poor Data Collection and Integration:** Pakistan suffers from fragmented and unstructured data collection mechanisms, leading to inconsistent intelligence sharing between agencies (Hassan et al., 2025), while effective AI-driven counterterrorism depends on accurate, real-time data from multiple sources.³ Also, the absence of centralised databases often results in missing terrorism threats and delays responses. The country established the National Intelligence Fusion and Threat Assessment Centre (NIFTAC forthwith) in May 2025 under NACTA to centralise intelligence data gathering and threat analysis through over 50 departments and agencies, federal and provincial. Six Provincial Intelligence Fusion and Threat Assessment Centres (PIFTACs) support NIFTAC for seamless information flow and operational consistency across the board. However, the effectiveness of NIFTAC is hindered because of bureaucratic inefficiencies resulting in a lack of fostering genuine inter-agency collaboration (NACTA, 2025; NIFTAC, 2025).
- iv. **High Costs of AI Implementation:** Pakistan's financial constraints and economic instability challenge the funding for AI-driven counterterrorism initiatives, such as substantial investment in hardware, software, training, and maintenance. The government prioritises conventional military and security spending over AI research and cybersecurity (Hussain, 2025; Abbas, 2021). Despite recognising the potential of AI, Pakistan's government has historically prioritised conventional military and security spending over AI research and cybersecurity initiatives. For instance, the National Artificial Intelligence Policy, unveiled in 2023, primarily relies on Public Sector Development Programme (PSDP) funding mechanisms, with IGNITE funding projected to absorb 30% of the budget. This approach restricts the policy's scope, compromising its capacity to shape the future of AI regulation, research, and management in Pakistan (Jahangir, 2023). Furthermore, Pakistan's AI research is underfunded and lacks institutional support. Unlike countries like China, which have invested heavily in AI research and university partnerships, most Pakistani universities have yet to introduce advanced AI curricula, limiting the talent pipeline (SDPI, 2024).
- v. **Dependence on Foreign Technology:** Without indigenous AI capabilities, Pakistan heavily relies on imported AI technologies and surveillance equipment from China, the US, and other countries (Baig, 2024), raising concerns about data security, cyber espionage, and operational sovereignty, making the country vulnerable to potential supply chain disruptions and foreign policy shifts affecting technology access. For example, the implementation of "Safe City" projects in Pakistan, particularly in Punjab, aimed at

³ e. g. biometric databases, financial transactions, social media, and surveillance footage.

- enhancing urban security, has incorporated Chinese surveillance technologies, including AI-driven facial recognition systems offering advanced security solutions, but raising concerns about data privacy and the potential for foreign entities to access sensitive information. There is always a threat that the integration of foreign systems into critical infrastructure makes the country vulnerable to cyber espionage risks and limits its control over national security operations (Baig, 2025; Ahmed, 2025; Editorial, 2024).
- vi. **Mass Surveillance and Privacy Issues:** In Pakistan, there is no clear legal framework governing AI use in counterterrorism, creating ambiguity about data protection and human rights (Haque et al., 2023). Pakistan's current legal landscape lacks robust data protection laws. The Personal Data Protection Bill, introduced in 2023, aims to regulate the collection, processing, and use of personal data. However, as of now, it remains unpassed, leaving a legislative void that fails to safeguard individuals' privacy rights effectively. This gap allows for unchecked surveillance and data misuse, as there are no clear guidelines or oversight mechanisms in place (Ahmad, 2024). Provincial governments have begun implementing AI technologies for surveillance purposes. For instance, the Punjab government has deployed an AI-based facial recognition system that captures images and compares them with a vast database, including records from driving licenses, crime records, and prison data. Similarly, the Sindh government has initiated AI technology at toll plazas to monitor and verify number plates and faces in real-time (Dawn News, 2025). The lack creates ambiguity about data protection and human rights and a risk that AI-powered mass surveillance systems could be misused by security agencies, leading to violations of citizens' rights. The broad and vague provisions in existing laws, such as the Prevention of Electronic Crimes Act (PECA) 2016, grant extensive surveillance powers to authorities without adequate oversight (Tech for Humanity Lab, 2025).
- vii. **Potential for Algorithmic Bias and Misuse:** Pakistan faces challenges of biases in data collection, which may be due to ethnic, religious, or socioeconomic factors, leading to the misidentification of individuals as threats. In counterterrorism, such biases have resulted in wrongful arrests, racial profiling, and increased distrust between communities and security forces (Abbasi, 2024). If Pakistan develops an AI-powered surveillance and predictive policing system that uses historical data to flag individuals as potential threats, and this system incorporates data from **past arrests, geographical location, religious affiliations, social media activity, tribal/family associations, etc.**, many individuals in areas like FATA,⁴ which were historically conflict zones, may be profiled or detained during counter-terrorism operations. This, like in the past, may result in false positives, violation of civil rights and erosion of trust (Scoop News, 2017; Abbasi, 2024).
- viii. **Lack of AI-Specific Legislation in Pakistan:** Pakistan does not have a dedicated AI governance policy for security and counterterrorism (Hassan et al., 2025). The Prevention of Electronic Crimes Act (PECA) 2016 covers cybercrimes but does not comprehensively address AI's role in law enforcement. Without regulatory clarity, AI implementation risks misuse, lack of accountability, and human rights violations (Ünver, 2024; Agnew, 2016). PECA 2016 was adopted to combat various types of cybercrime such as unauthorized access, electronic fraud, and online abuse. However, detractors claim that the law has confusing and broad clauses that are readily misconstrued and exploited. For example, Section 34 criminalizes "glorification of an offence or a person convicted of a crime," which is overbroad and might be used to target journalists, activists, and regular residents who express their opinions online. This rule encourages self-censorship and inhibits people from speaking out on issues of public importance, which violates free expression (Arab

⁴ now merged with Khyber Pakhtunkhwa

News Pakistan, 2024). Furthermore, the statute allows law enforcement considerable authority to investigate and prosecute electronic offenses with no oversight. As a result, individuals have allegedly been unfairly accused and punished, with PECA being abused to record false cases against political party personnel as a tactic for silencing opposition (Daily Times, 2023). In 2025, amendments to PECA were introduced, expanding the law's scope to include harsher penalties for what the government considers "fake news" and increasing state oversight of digital platforms. These changes have been met with criticism from political parties, journalist bodies, and human rights organisations, who view the legislation as a tool for suppressing dissent and silencing critical voices (Dawn, 2025). The amendments also led to the establishment of new regulatory bodies, such as the Social Media Protection and Regulatory Authority (SMPRA), tasked with monitoring social and digital media platforms. However, concerns have been raised about the potential for these bodies to infringe on citizens' liberties under the pretext of security (Wikipedia Contributors, 2024; APP, 2025).

- ix. **Threat of AI-Powered Cyber Attacks:** Pakistan's cyber defence infrastructure remains weak, making it susceptible to AI-driven cyber warfare (Hussain, 2025). For instance, in 2023, Pakistani banks reported multiple cases where AI-generated deepfake voices were used to bypass voice authentication systems for high-value transactions. These incidents led to unauthorised transfers worth Rs450 million before being flagged. Cybercriminals employed adversarial AI techniques to generate synthetic but realistic transaction patterns, evading anomaly detection algorithms. Additionally, deepfake-based social engineering was used to impersonate senior bank executives, authorising fraudulent fund transfers (Zhao, 2022b; Wright et al., 2023b; Ideal Solutions, 2023; Hussain, 2025).
- x. **Risk of Data Breaches and AI Exploitation:** AI-powered intelligence systems require vast amounts of sensitive data, including biometric records, financial transactions, and classified intelligence. A data breach or cyberattack on Pakistan's AI-driven intelligence networks could result in severe national security risks (Zegart, 2022). Without robust cybersecurity measures, encryption protocols, and AI-specific risk mitigation, Pakistan's AI-based counterterrorism infrastructure remains vulnerable. For instance, in 2021, Pakistan's National Database and Registration Authority (NADRA) reportedly faced an attempted cyberattack targeting its biometric data repositories. Although officials claimed the attack was thwarted, cybersecurity experts raised concerns about the agency's preparedness and the lack of end-to-end encryption on certain internal systems. If such a breach had succeeded, sensitive citizen data could have been compromised, potentially allowing terrorist organisations or hostile intelligence agencies to spoof identities, evade surveillance, or target specific individuals using AI-generated counterintelligence tactics (Khan, 2024; Zegart, 2022).
- xi. **Lack of Coordination between Security Agencies:** Pakistan's counterterrorism framework involves multiple agencies, including ISI, FIA, NACTA, and military intelligence units. However, bureaucratic inefficiencies and interagency rivalries hinder seamless AI-driven intelligence sharing. A lack of standardised AI protocols results in duplicated efforts and intelligence gaps, weakening counterterrorism effectiveness (Rashid, 2023). For instance, after the 2014 Army Public School (APS) attack in Peshawar, inquiries revealed that various agencies had received fragmented intelligence reports about a possible large-scale terrorist attack, but the failure to coordinate and share this information in real-time prevented timely action. NACTA was originally established to centralise counterterrorism coordination and data fusion, yet it has struggled to assert authority over other, more powerful institutions like the ISI or military intelligence. These coordination failures are further exacerbated in the context of AI, where seamless data

integration is essential for predictive threat modelling and early warning systems. Rashid, 2023b; NCTA, 2021; Dawn News, 2015).

- xii. **Political Resistance and Institutional Inertia:** For counterterrorism, Pakistan's traditional security institutions rely on conventional intelligence methods, and therefore, AI adoption faces resistance from them. Many policymakers and law enforcement officials lack awareness of AI's potential, slowing down its integration. Additionally, concerns about job displacement and AI replacing human intelligence officers create further resistance to AI adoption. For instance, while initiatives like the NIFTAC aim to centralise intelligence sharing and incorporate advanced technologies, the transition has been gradual due to institutional inertia and a preference for established practices. Additionally, concerns about job displacement and the potential of AI systems to undermine the roles of human intelligence officers contribute to the reluctance to embrace AI-driven solutions (Mugari, 2025; Gates, 2006; NCTA, n.d.).

Recommended Framework for Pakistan's Use of AI in Predictive Intelligence for Counterterrorism:

Pakistan must invest in developing AI research centres, collaborating with universities, and training security personnel, but for that purpose, there is a need to strengthen AI infrastructure, establish national databases and high-performance computing centres, and secure cloud networks for real-time counterterrorism operations. Moreover, AI-specific legal frameworks and governance laws are required to be formulated for mass surveillance, data protection, and accountability to protect human rights. Also, enhanced cybersecurity measures and AI-driven cybersecurity solutions, regular risk assessments, and encryption protocols must be developed and employed to safeguard intelligence data. An interagency AI collaboration may prove beneficial in establishing standardised AI data-sharing protocols between ISI, FIA, and NACTA. Moreover, public-private partnerships need to be encouraged with tech firms, AI startups, and international cybersecurity agencies to develop indigenous AI solutions for counterterrorism.

Possibly, a several-stage Strategic Framework can be devised and implemented in Pakistan. The very first stage is *Data Collection & Integration*, in which the country needs to establish a National AI-Driven Counterterrorism Data Hub for real-time intelligence sharing. The very first step will be to integrate structured (databases, criminal records) and unstructured (social media, surveillance footage, financial transactions) data sources and then implement cross-agency collaboration between NACTA, ISI, FIA, and law enforcement agencies.

The next stage, named *AI-Driven Threat Identification & Predictive Analytics*, would use Machine Learning (ML) models that would analyse behaviour patterns and detect anomalies to score any possible risk. After that, the NLP would be used to detect extremist narratives in digital communications. Once done, developed predictive models would assess the likelihood of terrorist attacks similar to past patterns.

Surveillance & Intelligence Automation may be the third stage of this framework, which will utilise computer vision and AI-powered facial recognition to identify high-risk individuals, then integrate drone-based AI surveillance for real-time monitoring of conflict zones, and finally, will leverage automated sentiment analysis to track radicalisation trends online.

Ethical & Legal Considerations may be the fourth stage to develop clear guidelines on AI usage, ensuring compliance with the legal framework and international human rights standards. The establishment of an *AI Ethics Oversight Board* for transparency and accountability will further ensure data privacy and protection, eliminating any possible misuse against non-threat individuals. To train law enforcement and counterterrorism agencies of Pakistan in AI-based intelligence systems and to foster public-private partnerships with universities and research institutions, the fifth stage, *Capacity Building & Technological Advancement*, will work. However, the country must invest in homegrown AI development to lessen reliance on foreign technologies.

The third level is Cybersecurity & AI Defence against Cyber-Terrorism, which includes AI-based threat detection to combat cyber-terrorism and enhanced digital forensics to trace down and dismantle online terrorist networks. Additionally, blockchain technology has the potential to protect data transmission in intelligence operations.

Table 1: Suggested Roadmap for the Framework for Pakistan’s Use of AI in Predictive Intelligence for Counterterrorism

S No.	Phases	Key Actions	Time Frame
1.	AI Policy & Legal Framework	Establish a national AI strategy for counterterrorism, and draft AI legal regulations.	6-12 months
2.	AI Infrastructure Development	Create a centralised AI-powered counterterrorism data hub and integrate national security databases.	1-2 years
3.	AI Deployment & Testing	Implement predictive intelligence models and launch AI-driven surveillance pilots.	2-3 years
4.	Nationwide Integration	Full-scale deployment across law enforcement and intelligence agencies.	3-5 years

Conclusion

The incorporation of artificial intelligence (AI) into counterterrorism activities has the potential to dramatically improve Pakistan's ability to combat emerging security challenges. Despite these advances, Pakistan faces significant obstacles in properly adopting AI-driven counterterrorism tactics. These include technology and infrastructure limits, financial restraints, ethical problems, cybersecurity flaws, and bureaucratic inefficiencies. The absence of AI-specific regulatory frameworks and interagency coordination complicates AI adoption in security operations. Nonetheless, with strategic investments in AI infrastructure, human resource development, and policy reforms, Pakistan can fully realize the potential of AI to improve national security while adhering to democratic ideals.

AI's capabilities go beyond reactive counterterrorism measures and into proactive threat reduction, making it a critical tool for future security frameworks. Several major areas show how AI has transformed Pakistan's counterterrorism efforts. If Pakistan efficiently implements and integrates AI-driven counterterrorism techniques, it will be able to greatly improve information collecting, security reaction times, and operational efficiency, therefore reducing terrorist risks.

While AI provides exceptional prospects for counterterrorism, its use must be calibrated with ethical considerations, civil liberties, and human rights protections. Mass surveillance, data privacy problems, algorithmic bias, and the possibility of misusing AI-driven intelligence present severe ethical quandaries. If artificial intelligence is not adequately regulated, it may result in

excessive government surveillance, false arrests, and infringement of private rights. To strike a balance between security and ethics, Pakistan must: 1) develop clear AI governance legislation to establish rigorous legal frameworks to oversee AI use in security while assuring data protection and transparency, 2) Implement AI oversight procedures by introducing independent monitoring bodies to avoid exploitation of AI-driven surveillance and hold security services accountable, 3) Ensure algorithmic fairness by training AI models on unbiased data to avoid racial, religious, or ethnic profiling in counterterrorism operations, 4) Increase public trust and openness by including civil society, legal experts, and human rights organizations to ensure AI is used responsibly and 5) Invest in AI education and awareness, which means training security professionals in ethical AI use and educating policymakers about AI's potential hazards and benefits.

AI has the ability to transform Pakistan's counterterrorism efforts by increasing intelligence skills, security infrastructure, and threat detection. To fully reap the benefits of AI, Pakistan must overcome financial, technological, legal, and ethical barriers through strategic reforms, investment in AI research, and interagency collaboration. The future of AI in Pakistan's counterterrorism operations depends on how well the government integrates AI-driven solutions while maintaining ethical standards. If properly applied, AI can be a strong force multiplier in Pakistan's fight against terrorism, assuring national security, stability, and long-term peace.

References

- Abbas, H. (2021). Extremism and Terrorism Trends in Pakistan: Changing Dynamics and New Challenges. *CTC Sentinel*, 14(2). 44-51. <https://ctc.westpoint.edu/wp-content/uploads/2021/02/CTC-SENTINEL-022021.pdf>
- Abbasi, S. (2024, October 22). Caught in the web: Surveillance, data protection and AI in Pakistan. *DAWN.COM*. <https://www.dawn.com/news/1864073>
- Agnew, R. (2016). A theory of crime resistance and susceptibility. *Criminology (Beverly Hills)* 54(2), 181–211. <https://doi.org/10.1111/1745-9125.12104>
- Ahmad, M. (2025, February 15). Pakistan's AI dependence. *The News International*. Retrieved from <https://www.thenews.com.pk/print/1282863-pakistan-s-ai-dependencethenews.com.pk>
- Ahmad, N. (2024, January 28). *Protecting rights: The case for a data protection law*. *The News International*. <https://www.thenews.com.pk/tns/detail/1244178-protecting-rights>
- Akilli, E. (2024). Artificial Intelligence in counterterrorism navigating the intersection of security, ethics, and privacy. *Seta Perspective*, 73, 1-5. <https://www.setav.org/en/assets/uploads/2024/04/P73En.pdf>
- Anwar, O., Malik, A., Aqil, A., & Iftikhar, N. F. (2020). The COVID-19 law and policy challenge: Cyber surveillance and big data - Pakistan's legal framework and the need for safeguards. *RSIL Law Review*, 4, 35-62. <https://www.rsillaw.review/wp-content/uploads/2023/01/RLR-V4-20-02.pdf>
- APP. (2025, January 30). PECA Law to combat digital crimes, fake news in Pakistan: Experts. *Associated Press of Pakistan*. <https://www.app.com.pk/domestic/peca-law-to-combat-digital-crimes-fake-news-in-pakistan-experts/>

- Baig, M. A. A. (2024). Artificial Intelligence, Emerging Technologies and National Security of Pakistan. *CISS Insight Journal*, 12(1), 90-114. <https://journal.ciss.org.pk/index.php/ciss-insight/article/view/363>
- Baig, M. A. A. (2025). Navigating Risks and Benefits of Pakistan's Tech Dependency on China. *Strafasia*. Retrieved from <https://strafasia.com/navigating-risks-and-benefits-of-pakistans-tech-dependency-on-china/strafasia.com>
- Bhatti, M., & Shahrukh, N. (2023). Navigating the Path towards Geo-economics: An Analysis of Opportunities and Challenges for Pakistan. *Margalla Papers*, 27(1), 1-12. <https://doi.org/10.54690/margallapapers.27.1.109>
- Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., Ó hÉigearthaigh, S., Beard, S., Belfield, H., Farquhar, S., Lyle, C., Crootof, R., Evans, O., Page, M., Bryson, J., Yampolskiy, R., & Amodei, D. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. arXiv. <https://arxiv.org/abs/1802.07228>
- Business Recorder. (2023, July 10). *10 urgent policy priorities for Pakistan towards AI-readiness*. <https://www.brecorder.com/news/40251832>
- Business Recorder. (2024, March 27). DeepSeek's AI 'disruption': insights for Pakistan in the global tech race. *Business Recorder*. <https://www.brecorder.com/news/40347725>
- Chowdhury, G. (2003). Natural language processing. *Annual Review of Information Science and Technology*, 37, 51-89. <https://pure.strath.ac.uk/ws/portalfiles/portal/131112/strathprints002611.pdf>
- Clarke, R. A., & Knake, R. K. (2019). *The fifth domain: Defending our country, our companies, and ourselves in the age of cyber threats*. Penguin Press.
- Davies, H., & Abraham, Y. (2025, March 6). *Revealed: Israeli military creating ChatGPT-like tool using the vast collection of Palestinian surveillance data*. The Guardian. <https://www.theguardian.com/world/2025/mar/06/israel-military-ai-surveillance>
- Dawn News. (2015, January 10). *Govt had prior information on the Peshawar attack: NACTA*. <https://www.dawn.com/news/1156082>
- Dawn News. (2025, March 20). *AI surveillance systems introduced in Punjab, Sindh to identify criminals, track vehicles*. Dawn. <https://www.dawn.com/news/1864073>
- Editorial. (2024, June 3). Dependence on foreign AI. *The Express Tribune*. Retrieved from <https://tribune.com.pk/story/2469485/dependence-on-foreign-ai-tribune.com.pk>
- FATF. (2021). *Opportunities and Challenges of New Technologies for AML/CFT*. <https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf>
- Ganor, B. (2021). Artificial or human: A new era of counterterrorism intelligence? *Studies in Conflict & Terrorism*, 44(7), 605-624. <https://doi.org/10.1080/1057610X.2019.1568815>
- Gates, K. (2006). Identifying the 9/11 'Faces of Terror': The Promise and Problem of Facial Recognition Technology. *Cultural Studies*, 20(4-5), 417-440. <https://doi.org/10.1080/09502380600708820>

- Giustozzi, A. (2022). *The Islamic State in Khorasan: Afghanistan, Pakistan, and the new Central Asian jihad*. Hurst Publishers.
- Gul, A. (2023, September 30). *Report: Surge in Terrorism Kills More Than 700 Pakistanis*. Voice of America; Voice of America (VOA News). <https://www.voanews.com/a/report-surge-in-terrorism-kills-more-than-700-pakistanis/7291609.html>
- Haque, E. U., Abbasi, W., Murugesan, S., Anwar, M. S., Khan, F., & Lee, Y. (2023). Cyber forensic investigation infrastructure of Pakistan: an analysis of the cyber threat landscape and readiness. *IEEE Access*, 11, 40049-40063. <https://doi.org/10.1109/ACCESS.2023.3268529>
- Hassan, B., Raza, M. O., Siddiqi, Y., Wasiq, M. F., & Siddiqui, R. A. (2025). CONNECT: An AI-powered solution for Student Authentication and Engagement in Cross-Cultural Digital Learning Environments. *Computers*, 14(3), 77. <https://doi.org/10.3390/computers14030077>
- Hussain, D. M. (2025, January 3). *Smart Wars: How AI Can Revolutionize Pakistan's Counterterrorism Strategies*. SVI - Strategic Vision Institute - Strategic Vision Institute; SVI - Strategic Vision Institute. <https://thesvi.org/smart-wars-how-ai-can-revolutionize-pakistans-counterterrorism-strategies/>
- Hussain, M. (2025). Cyber defence. *Pakistan Today*. <https://www.pakistantoday.com.pk/2025/03/14/cyber-defence/pakistantoday.com.pk>
- Ideal Solutions. (2023). *Top 23 Cybersecurity Vulnerabilities in Pakistani Banking Systems That Hackers Exploit*. <https://www.idealsols.com/cybersecurity-vulnerabilities-in-pakistani-banking-systems/idealsols.com>
- Jahangir, A. (2023, May-June). Policy Shortfalls. *Aurora*. <https://aurora.dawn.com/news/1144806/policy-shortfallsaurora.dawn.com>
- Jaleel, Z. (2024, August 7). *Digital Guardians: Cybersecurity Challenges in Pakistan's Modern Landscape*. Institute for International Cyber Research. <https://iicrpk.org/press-release/digital-guardians-cybersecurity-challenges-in-pakistans-modern-landscape/iicrpk.org>
- Javed, N. (2023). Combating online violent extremism through AI: avenues for Pakistan. *Pakistan Journal of Terrorism Research*, 5(2), 1-23. <https://nacta.gov.pk/wp-content/uploads/2024/01/Combating-Online-Violent-Extremism.pdf>
- Junaidi, I. (2024, December 31). 2024 was "deadliest year" for Pakistan's security forces. *DAWN.COM*. <https://www.dawn.com/news/amp/1882160>
- Khan, F. A., Li, G., Khan, A. N., Khan, Q. W., Hadjouni, M., & Elmannai, H. (2023). AI-driven counterterrorism: Enhancing global security through advanced predictive analytics. *IEEE Access*, 11, 135864-135879. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10328769>
- Khan, I. A. (2024, March 27). 2.7m citizens' data compromised over five years, probe finds. *Dawn*. <https://www.dawn.com/news/1824026efe.com+3dawn.com+3dawn.com+3>
- Khan, R. (2024a, December 31). *Pakistani security forces suffer deadliest year for a decade while fighting insurgency, report finds*. AP News. <https://apnews.com/article/pakistan-militants-attack-security-post-northwest-taliban-21fd9842de88b56b0ee28537f463e6f7>

- Khan, R. (2024b, November 20). *Suicide car bomb kills 12 troops at a security post in north-western Pakistan*. AP News. <https://apnews.com/article/pakistan-suicide-bombing-security-forces-killed-f17f4521de40a27e3ebf76ccf15d58ec>
- Ko, H., & Jilani, H. (2025, January 17). *Pakistan's bet on Taliban backfires as violence surges*. Financial Times. <https://www.ft.com/content/85935c21-6973-4956-af5e-282aacd05294>
- Lee, M. (2023). *Cyber threat intelligence*. John Wiley & Sons.
- Lodhi, M. (Ed.). (2024). *Pakistan: The Search for Stability*. Oxford University Press.
- Maguire, M., & Westbrook, D. A. (2025). Machine learning and artificial intelligence in counterterrorism: The “realities” of security practitioners and technologists. In M. Avis, D. Marciniak, & M. Sapijnoli (Eds.), *States of Surveillance: Ethnographies of New Technologies in Policing and Justice* (pp. 164–181). Routledge. <https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9781003412908-11/machine-learning-artificial-intelligence-counterterrorism-mark-maguire-david-westbrook>
- Mahesh, B. (2020). Machine learning algorithms-a review. *International Journal of Science and Research*, 9(1), 381-386. <http://dx.doi.org/10.21275/ART20203995>
- Mazzocco, I. (2022, July 27). The AI-Surveillance Symbiosis in China - Big Data China. *Big Data China*. <https://bigdatachina.csis.org/the-ai-surveillance-symbiosis-in-china/>
- McKendrick, M. (2019). Artificial Intelligence, Predictive Analytics, and Counterterrorism. *Chatham House*. <https://www.chathamhouse.org/2019/07/artificial-intelligence-predictive-analytics-and-counterterrorism>
- Mehdi, S. E. (2019). In their own words: Understanding Lashkar-e-Tayyaba: C. Christine Fair, Oxford University Press, New Delhi. *Strategic Analysis*, 44(1), 66–68. <https://doi.org/10.1080/09700161.2020.1699999>
- Mir, A. (2018). What explains counterterrorism effectiveness? Evidence from the US drone war in Pakistan. *International Security*, 43(2), 45-83. https://doi.org/10.1162/isec_a_00331
- Montasari, R. (2024a). Addressing Ethical, Legal, Technical, and Operational Challenges in Counterterrorism with Machine Learning: Recommendations and Strategies. In *Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution: Threats, Assessment and Responses* (pp. 199-226). Cham: Springer International Publishing. <https://link.springer.com/book/10.1007/978-3-031-50454-9>
- Montasari, R. (2024b). Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution. In *Advanced sciences and technologies for security applications*. Springer International Publishing. <https://doi.org/10.1007/978-3-031-50454-9>
- Mugari, I., & Obioha, E. E. (2021). Predictive policing and crime control in the United States of America and Europe: Trends in a decade of research and the future of predictive policing. *Social sciences*, 10(6), 234. <https://doi.org/10.3390/socsci10060234>
- Mugheri, S. H. (2025, March 18). *Eradicating terrorism through Artificial Intelligence*. Pakistan Today. Retrieved from <https://www.pakistantoday.com.pk/2025/03/18/eradicating-terrorism-through-artificial-intelligence/pakistantoday.com.pk>

- NACTA. (2021a). Big Data and Counter-Terrorism. *Pakistan Journal of Terrorism Research*, 4(1), 57-70. <https://nacta.gov.pk/wp-content/uploads/2021/09/Maryam-Baloch.pdf>
- NACTA. (2021b). *NACTA's role in counterterrorism coordination*. Government of Pakistan. <https://nacta.gov.pk/>
- NACTA. (2024). Counter-terrorism. *National Counter Terrorism Authority (NACTA)*. <https://nacta.gov.pk/functions/counter-terrorism-wing/counter-terrorism/>
- NACTA. (2025). *National Counter Terrorism Authority*. https://en.wikipedia.org/wiki/National_Counter_Terrorism_Authority
- NACTA. (n. d.). *National Intelligence Fusion and Threat Assessment Centre (NIFTAC)*. https://en.wikipedia.org/wiki/National_Counter_Terrorism_Authorityen.wikipedia.org
- Nadkarni, P. M., Ohno-Machado, L., & Chapman, W. W. (2011). Natural language processing: an introduction. *Journal of the American Medical Informatics Association*, 18(5), 544-551. <https://doi.org/10.1136/amiajnl-2011-000464>
- NCAI. (2022, August 23). *National Centre of Artificial Intelligence (NCAI) – A Leading Hub of Innovation and Scientific Research*. <https://ncai.pk/national-centre-of-artificial-intelligence-ncai-a-leading-hub-of-innovation-and-scientific-research/ncai.pk+1ncai.pk+1>
- NIFTAC. (2025). *National Intelligence Fusion and Threat Assessment Centre (NIFTAC)*. https://en.wikipedia.org/wiki/National_Intelligence_Fusion_and_Threat_Assessment_Centre
- PAF-IAST. (n.d.). *High-Performance Computing Cluster*. <https://paf-iaast.edu.pk/it-facility3cs/paf-iaast.edu.pk+1paf-iaast.edu.pk+1>
- Pakistan Today. (2025, March 18). *Eradicating terrorism through Artificial Intelligence*. <https://www.pakistantoday.com.pk/2025/03/18/eradicating-terrorism-through-artificial-intelligence/pakistantoday.com.pk>
- Pellerin, C. (2017, July 21). *Project Maven to Deploy Computer Algorithms to War Zone by Year's End*. U.S. Department of Defense. <https://www.defense.gov/News/News-Stories/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/>
- Rashid, A. (2023a). *The Challenges of Integrating AI into Pakistan's Security Apparatus*. Islamabad Policy Research Institute (IPRI). <https://ipripak.org/the-challenges-of-integrating-ai-into-pakistans-security-apparatus>
- Rashid, W. (2023b). Using Artificial Intelligence to Combat Extremism. *Pakistan Journal of Terrorism Research*, 5(2) 1-23. <https://nacta.gov.pk/wp-content/uploads/2024/01/Using-Artificial-Intelligence-to-Combat-Extremism.pdf>
- Rashid, W. (2024, June 23). Can AI help counter terrorism? *The News International*. <https://www.thenews.com.pk/print/1202886-can-ai-help-counter-terrorism>
- Rassler, D. (2021). Commentary: Data, AI, and the Future of US Counterterrorism: Building an Action Plan. *CTC Sentinel*, 31-40. <https://ctc.westpoint.edu/commentary-data-ai-and-the-future-of-u-s-counterterrorism-building-an-action-plan/>

- Rosenberg, P. (2022). Project Maven: The Pentagon's AI-driven counterterrorism revolution. *Defense & AI Studies*, 14(3), 77-94.
- Šaljić, E., & Tomić, D. (2024). The Use of Artificial Intelligence in investigating, combating and predicting crimes. *Pakistan Journal of Criminology*, 16(431).
- Scoop News. (2017). PAKISTAN: Racial profiling of Pakhtuns to be condemned. *Scoop.co.nz*. <https://www.scoop.co.nz/stories/WO1703/S00020/pakistan-racial-profiling-of-pakhtuns-to-be-condemned.htm>
- SDPI. (2024). DeepSeek's AI 'disruption': insights for Pakistan in the global tech race. *Sustainable Development Policy Institute*. https://sdpi.org/8933/news_detail
- Serhan, Y. (2024, December 18). How Israel Uses AI in Gaza—And What It Might Mean for the Future of Warfare. *Time*. <https://time.com/7202584/gaza-ukraine-ai-warfare/>
- Shahzad, S., & Khan, A. (2024). Adoption of AI in warfare: Comparative study of India and Pakistan. *International Journal of Academic Research for Humanities*, 4(2), 70-85. <https://jar.bwo-researches.com/index.php/jarh/article/view/434>
- Stanford University. (2024). *Artificial Intelligence Index Report 2023*. https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report_2023.pdf
- Stark, R. (2021). China's use of Artificial Intelligence in their War against Xinjiang. *Tulane Journal of International and Comparative Law*, 29, 153-173.
- Stratheia. (2025). *Smart Wars: How AI Can Revolutionize Pakistan's Counterterrorism Strategies*. <https://stratheia.com/smart-wars-how-ai-can-revolutionize-pakistans-counterterrorism-strategies/stratheia.com>
- Strout, N. (2022, April 28). Intelligence agency takes over Project Maven, the Pentagon's signature AI scheme. *C4ISRNet*. <https://www.c4isrnet.com/intel-geoint/2022/04/27/intelligence-agency-takes-over-project-maven-the-pentagons-signature-ai-scheme/>
- Tech for Humanity Lab. (2025, January 24). *Examining Pakistani digital surveillance and privacy rights*. <https://tech4humanitylab.org/blog/2025/1/24/examining-pakistani-digital-surveillance-and-privacy-rights>
- Tunysová, A. (2022). Predicting and Preventing Terrorism with Artificial Intelligence and Machine Learning: Implications for Security in Israel. Master's Thesis. Charles University, <https://dspace.cuni.cz/bitstream/handle/20.500.11956/174465/120416849.pdf?sequence=1>
- Tuteja, V., & Marwaha, S. S. (2023). Artificial intelligence: threat of terrorism and need for better counterterrorism efforts. *International Journal of Creative Computing*, 2(1), 87-100. <https://doi.org/10.1504/IJCRC.2023.133551>
- UN Counter-Terrorism Centre & UNICRI. (2020). *Countering terrorism online with artificial intelligence*. <https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/countering-terrorism-online-with-ai-uncct-unicri-report-web.pdf>
- UNODC. (2023, June 20). *Sustainable results against terrorism require sustainable responses, says UNODC Executive Director at United Nations Counter-Terrorism Week*. <https://www.unodc.org/unodc/frontpage/2023/June/sustainable-results-against-terrorism-require-sustainable-responses--says-unodc-executive-director-at-united-nations-counter-terrorism-week.html>

- Ünver, H. A. (2024). *Artificial intelligence (AI) and human rights: Using AI as a weapon of repression and its impact on human rights*. <https://data.europa.eu/doi/10.2861/52162>
- Wall, C. (2025). The Ghost in the Machine: Counterterrorism in the Age of Artificial Intelligence. *Studies in Conflict & Terrorism*, 1-27. <https://doi.org/10.1080/1057610X.2025.2475850>
- Wasil, A., Smith, E., Katzke, C., & Bullock, J. (2024). AI Emergency Preparedness: Examining the federal government's ability to detect and respond to AI-related national security threats. *ArXiv.org*. <https://doi.org/10.48550/arXiv.2407.17347>
- Weimann, G. (2015). *Terrorism in cyberspace: The next generation*. Columbia University Press.
- Wikipedia Contributors. (2024, December 24). National Cyber Crimes Investigation Agency. *Wikipedia*. https://en.wikipedia.org/wiki/National_Cyber_Crimes_Investigation_Agency
- Wright, J. & Weber, V. & Walton, G. F. (2023a). Identifying potential emerging human rights implications in Chinese smart cities via machine-learning-aided patent analysis. *Internet Policy Review*, 12(3), 1-26. <https://doi.org/10.14763/2023.3.1718>
- Wright, J., Patel, R., & Singh, A. (2023b). Artificial Intelligence in Cyber Warfare: Risks and Countermeasures. *International Journal of Security Studies*, 12(2), 101-118.
- Zegart, A. B. (2022). *Spies, lies, and algorithms: The history and future of American intelligence*. Princeton University Press.
- Zhao, W. (2022a). China's AI-enabled counterterrorism surveillance. *Journal of International Cybersecurity*, 12(1), 33-50.
- Zhao, Y. (2022b). AI and Cybersecurity: Emerging Threats and Defenses. *Cybersecurity Journal*, 15(3), 45-60.
- Zia, H. (2021). Information Revolution and Cyber Warfare: Role of Artificial Intelligence in Combatting Terrorist Propaganda. *Pakistan Journal of Terrorism Research*, 3(2), 133-157. <https://nacta.gov.pk/wp-content/uploads/2021/09/Information-Revolution-and-Cyber-Warfare-Role-of-Artificial-Intelligence-in-Combating-Terrorist-Propaganda.pdf>