

APPLICATIONS OF AI IN COUNTERING TERRORISM IN PAKISTAN: A WAY FORWARD

Harsa*

Musavir Hameed**

Abstract

Artificial Intelligence (AI) is a transformative technology to serve human interests. It can thus be leveraged to address complex issues like terrorism. This paper aims to determine how we can use AI to mitigate the rising threat of terrorism in the conflict zones of Pakistan, with a particular focus on the provinces of Khyber Pakhtunkhwa and Balochistan. The objectives of this research are to develop a framework for conflict zones in Pakistan to implement AI using the provided tools and strategies, which will help regulate efforts to combat terrorism and manage militancy. To balance AI's innovation and strategy, this paper examines the theoretical underpinnings of the Cyber Threat Intelligence (CTI) framework. It is being employed to determine the applications of AI in countering terrorism. In addition, the theoretical framework employs both the Intelligence Cycle and the Diamond Model of CTI to map the enemy's tactics and infrastructure, proactively prevent threats, and, in the event of an attack, manage them. Primary and secondary sources have been used in this research to provide a broader understanding of the topic. The methodology used a mixed-methods approach. Various case studies have been examined in this research to demonstrate and enhance security, stability, and counterterrorism in Pakistan. Findings of this study revolve around the following lines: Firstly, AI can be used for predictive analysis or as large language

* Assistant Research Fellow at Baluchistan Think Tank Network (BTTN), at BUIITEMS, Quetta.

** Research Officer at Baluchistan Think Tank Network (BTTN), at BUIITEMS, Quetta

models in surveillance. Secondly, AI has a huge role in monitoring social media content and tracking the financial activities of terrorist organizations. Furthermore, the study provides recommendations for applying AI tools in different domains of cybersecurity for Pakistan in countering increasing levels of terrorism and reducing the operational capacity of outlawed militant organizations.

Key Words: AI, Terrorism, Militancy, Extremism, Balochistan, Khyber Pakhtunkhwa, Pakistan.

Introduction

In the recent past, Pakistan has confronted several terrorist activities that have negatively affected Pakistan's National Security and Social Cohesion. Most of the attacks in Pakistan took place in the west of the Indus River, i-e, Balochistan and Khyber Pakhtunkhwa. Both of these provinces will be studied as conflict zones. Subsequently, a conflict zone is a geographical area undergoing sustained armed conflict, severe political crises, extremist violence, heightened military tensions, and militancy. Militant organizations operating in these areas have adopted sophisticated techniques to carry out their attacks. Along with the rising danger in these conflict zones and the increasing use of digital media by militant groups to obtain illegal funding for their operations and use technology to launch attacks against their enemies, there is a need for new forms of technology that may combat Terrorism using new technological tools. Artificial Intelligence (AI) is a tool of technology that could potentially create a paradigm shift in how Terrorism is fought in Pakistan. AI has many uses in fighting Terrorism in conflict zones, including predictive threat analysis and real-time surveillance using advanced large language models (LLMs), social media monitoring, and tracking the financial activities of terrorist

organizations. AI may help Pakistan shift from a reactive security model to a more data-driven, proactive, and strategic security model. Using AI, Pakistan can strengthen its resilience and stability in unstable regions of the country.

Balochistan, due to the historical presence of multiple militant organizations in the province since 1948, coupled with the province's limited economic development, social marginalization, and exploitation of resources, along with the continued threats posed by militant organizations, is viewed as a conflict-affected region. Due to the nature of the hybrid conflicts taking place in the province, the province is paying a high price in terms of human, economic, and infrastructure losses, including damage to strategic projects such as the China-Pakistan Economic Corridor (CPEC). The ongoing conflicts in the province have resulted in a significant loss of life, displacement, and socio-economic disruption, and demonstrate the need for sophisticated tools, such as AI, to enhance intelligence, surveillance, and humanitarian responses in the province of Balochistan.

Similarly, Khyber Pakhtunkhwa is posed as a conflict zone due to the persistent existence of militant organizations such as the TTP, which have had an active presence there. The TTP has been able to conduct increasingly sophisticated attacks against both military personnel and civilians because they have used the sanctuaries available to them in Afghanistan since the US withdrawal and the subsequent Taliban takeover. Intermittent violence between Sunni and Shia sects in areas such as Kurram further fuels sectarian tensions over issues of land and resources. It can be intertwined with the objectives of terrorist organizations, including ISKP. Both types of violence contribute to sieges, ambushes, and disruptions in supply lines that make daily life impossible. All of these factors are complicated by the complex

security environment within the province and weak diplomatic channels with the Taliban government in Afghanistan. These factors create long-term threats of increased Terrorism, humanitarian disasters, and regional instability that could have implications beyond Pakistan and Afghanistan.

The article further utilizes multiple global case studies from major international organizations and countries to illustrate how countries can use AI to fight violent extremism. Drawing on case studies from the UN, the US, Israel, and the EU, the authors demonstrate how AI-based analytical tools, surveillance systems, and ethical frameworks have been used to successfully reduce the incidence of terrorism and radicalization in their respective societies. While the case studies illustrate the successful utilization of AI in combating terrorism, they also emphasize the importance of international cooperation and the necessity of considering human rights when using AI to fight terrorism, and serve as lessons for Pakistan to develop and innovate its own counter-terrorism policies. Overall, the research's contribution is to produce a comprehensive review of how AI should be applied in a security environment relevant to Pakistan, and to establish policy recommendations for Pakistani authorities in conflict areas such as Balochistan and KPK. The study seeks to address the key question: whether AI is sufficiently capable of counteracting rising terrorist activity or managing its aftermath, and how AI's features, such as predictive analysis, LLM-based surveillance, social media monitoring, and financial tracking of terrorist outfits, can be used to combat terrorist activity. This study also provides information on the tools necessary for the above-mentioned AI features to function correctly in countering terrorism.

Theoretical Framework

This research has explored the Cyber Threat Intelligence (CTI) framework as a model to illustrate how AI can be used to combat terrorism in Pakistan's conflict zones, such as Balochistan and KPK. The two foundational models, i.e., the Intelligence Cycle and the Diamond Model in CTI, conceptualize counter threats using AI proactively. When combined with specific AI features and tools, this framework can be used to develop an innovative solution in Pakistan to counter terrorism systematically.

AI's features, like, predictive analysis, surveillance under Large Language Models, its social media monitoring and its tracking of financial support of terror outfits, if incorporated into the Intelligence Cycle (Identify, Collect, Process, Analyze, Disseminate, Evaluate) to help avoid biases in data and violations of individuals' privacy during the planning and direction stages of the cycle. This makes it easy to use AI to identify which areas of conflict require greater emphasis in the collection of intelligence; for example, AI can be used to identify areas of conflict in Pakistan, such as KPK and Balochistan, and the extremist groups operating there. Once these areas have been identified, CTI will utilize AI-enhanced tools to collect intelligence about these extremist groups from various sources, including but not limited to social media, financial transactions, video feeds from surveillance cameras, and field reports. The process and analysis phases of the Intelligence Cycle will also utilize AI algorithms to evaluate large quantities of disparate information to develop indicators and patterns related to the methods of funding, radicalization, and operations used by violent extremist organizations. The dissemination phase of the Intelligence Cycle will involve the timely distribution of intelligence to relevant governmental agencies, policymakers, and international partners so they may coordinate effectively in responding to the identified

threats after the dissemination phase of the Intelligence Cycle begins the evaluation/feedback phase, which will continue indefinitely, and will include continuous assessments and enhancements to both the input data and the analytical models to improve the reliability and performance of the system continually.

The Diamond Model is a framework to define and describe the "Adversary" (in this, "Infrastructure", "Capabilities", and "Victims" of violent extremist organizations. This study has applied AI to the predictive and preventative aspects of the Diamond Model, while ensuring compliance with all applicable laws and regulations. The Diamond Model describes the "Adversary" as the identification of violent extremist organizations and their organizational structures. The "Capabilities" portion of the Diamond Model describes the methods, weapons (e.g., IEDs), and operational tactics employed by the organizations. The "Infrastructure" portion of the Diamond Model identifies the logistics provided to organizations, i.e., smuggling routes and communication networks. The "Victim" in the Diamond Model is defined as the people of security and military agencies, the population targeted by the organizations, and the humanitarian consequences resulting from their activities.

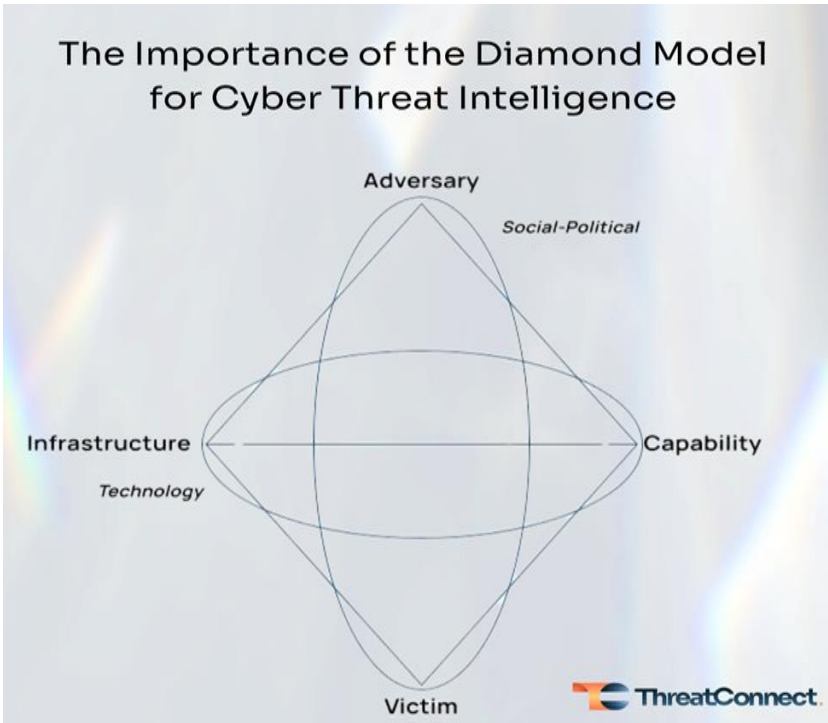


Figure 1: Sourced from Threat Connect (Bussa, 2023)

The framework proposed by CTI's Diamond Model and Intelligence cycle helps counter terrorism in conflict areas in Pakistan. Side by side, it can help in creating a Pakistan-focused CTI facility that balances innovation with strategy. Based on global experiences. Through this framework, global experiences on the same came to light. The framework encourages cooperation between countries and follows established norms such as the United Nations' Guiding Principles on Business and Human Rights, by identifying the ethical challenges related to AI, such as algorithmic bias and privacy breaches, and addressing them through regular audits and monitoring of organizations, including the National Counter Terrorism Authority (NACTA) (Javed, 2023). Overall, it will create an opportunity for AI to serve as a transformative solution to enhance security and resilience in Pakistan and combat the threat of terrorism.

Balochistan and KPK: Major Conflict Zones in Pakistan

Balochistan, Pakistan's largest province, comprising more than half of Pakistan's total landmass, if we count the sea as well, but is home to just 5 percent of Pakistan's total population. It is considered one of the conflict-prone areas of the country due to a persistent cycle of terrorism (Samad, 2015). This has kept the province in constant crisis and disrupted its socio-economic structure since the beginning (Ahmed et al., 2020).

The current surge in Terrorism, which started in 2004 after a period of quiet, is led by militant groups who are demanding either independence or are against the independent lives of the citizens (Bansal, 2008). Islamic Extremism has added to the violence caused by the separatist movement, with extremist religious militant groups, many of them targeting sectarian minority groups such as Shias (Siddiqui, 2025). The combination of ethno-nationalist militancy and jihadist terrorism has turned Balochistan into a hybrid conflict zone, where state-sponsored military operations create a cycle of retaliation. However, in recent times, Balochistan's conflict has increased, and has included more sophisticated insurgent tactics and spillover from other conflicts in the region. The involved militant groups have shifted from the traditional hit-and-run guerrilla warfare tactics to more high-profile operations, including suicide bombings, ambushing convoys, and sabotaging infrastructure. An example of how the conflict escalated occurred in early 2025 with the attack on the Jaffar Express train in March 2025 and then hijacking it in May, killing dozens of people and highlighting vulnerabilities in transportation networks (Hussain, 2025). On January 8, 2025, militants attempted to take control of the town of Zehri, showing that they were capable of holding territory temporarily and disrupting local government (Akhtar, 2024).

Cross-border dynamics have made things worse. In January 2024, tit-for-tat airstrikes between Pakistan and Iran targeted Baloch militants operating on both sides of the porous 900km border, with radical militant groups on both sides taking advantage of the division (Saifi & Mogul, 2024). The China-Pakistan Economic Corridor (CPEC), which includes Gwadar Port, has become a focal point, and insurgents view it as neo-colonial exploitation, resulting in attacks on Chinese workers and projects — over 20 such incidents since 2018, including a March 2024 suicide bombing in Gwadar that killed five Chinese engineers. Due to the province's rugged terrain and sparse population density (approximately 12 people/sq km), security operations are complex, creating a haven for non-state actors.

Khyber Pakhtunkhwa (KP), on the other hand, is a province located along the border of Pakistan and Afghanistan. Conflict in this region has been caused mainly by the province's geographical position, its history of being an area of long-standing insurgent activity and Terrorism; the roots of this conflict include military actions against militant groups and foreign fighters within the province dating back to the early 2000s, tribal and ethnic conflicts and the spill over of violence from the war in Afghanistan into the province. Terrorism in the region increased after Pakistan's military increased its operations against groups connected to al-Qaeda and the Taliban in the area. Militant organizations have been present in the conflict, with shifting alliances and rivalries.

In 2023 and 2024, Khyber Pakhtunkhwa saw an escalation in terrorist violence, with hundreds of deaths reported among civilians, militants, and members of security forces. The number of casualties included at least 12 security personnel in a suicide bombing attack in Bannu district in November 2024. Attacks of this type are typically claimed by factions of the militant groups

named after Taliban extremist groups, which continues to be the predominant militant organization in the region. A spike in terrorist violence was attributed to the weaknesses of government counter terrorism efforts and the breakdown of talks between the government and the militant groups.

Incidents of recent years also include targeted shootings and attacks against government officials and security forces, including an attempted assassination of the Deputy Commissioner of Kurram district in early 2025. These events demonstrate the continued threat that militants pose to the authority of the government and the ability of the security agencies to maintain order in KP.

Table 1: A detailed statistical analysis of the same is provided below.

Category	Balochistan	KPK
Overall Terrorism Trends in Pakistan	Terrorist attacks and fatalities increased by 17% in 2023 vs. 2022; Balochistan accounted for a significant portion due to separatist activities. (Source: PIPS Pakistan Security Report 2023)	In 2025 (Jan-Nov), KPK accounted for 62% of Pakistan's terrorist incidents and 68% of total fatalities nationwide, totaling around 1,188 violence incidents with 2,165 deaths. (Source: SATP report)
	Pakistan experienced over 50% more attacks and casualties nationwide in 2023 vs. 2022; Balochistan's	

	Terrorism contributed to at least 25% of incidents. (Source: US State Department Country Reports on Terrorism 2023)	
Incidents and Casualties	From 2023 to mid-2025, over 1,200 terrorism-related incidents occurred in Balochistan, resulting in ~1,500 deaths (800 security personnel, 400 civilians, 300 militants). (Source: South Asia Terrorism Portal)	In 2025 (up to Feb), 346 terrorism-related fatalities were reported (22 civilians, 63 security forces, 261 militants). (Source: SATP report)
	In 2024 alone, insurgent attacks surged by 40%, with 450 incidents claiming 600 lives. (Source: SATP)	In 2024, 1,363 fatalities (288 civilians, 421 SF personnel, 654 terrorists) occurred in 702 incidents. Nearly 300 terror attacks have been reported in KPK in 2025 up to mid-year. (Source: SATP Report)
	By August 2025, the militant group had conducted over 100 operations, including 15 suicide bombings.	

	(Source: US State Department Designation)	
Economic Impact	Conflict costs Balochistan \$5-7 billion annually in lost investment and infrastructure damage. (Source: World Bank Report)	The direct and indirect costs of terrorism in Pakistan have reached approximately Rs. 678 billion, badly affecting KP's socio-economic development. (Source: ISSI Report)
	CPEC projects (valued at \$62 billion) face delays due to security threats; over \$1 billion in damages from attacks since 2015. (Source: CPEC Reports)	Terrorism has caused economic losses such as infrastructure damage, halted development, unemployment, disrupted education, a decline in investment, and collapsed local industries like tourism and marble mining.
Extremism and Sectarian Violence	Balochistan hosts active religious extremist militant cells, responsible for 20% of Pakistan's jihadist attacks in 2024.	Sectarian violence in KP remains significant; e.g., in 2024-25, dozens were killed in sectarian attacks,

	(Source: GTI 2024)	notably in Kurram District, with over 130 fatalities and 186 injuries reported during sectarian clashes in late 2024.
	The Hazara community in Quetta has endured over 50 major bombings since 2001, killing >1,000 people. (Source: HRW/ UNHCR Reports)	Attacks often target the Shia community and have resulted in mosque damage and convoy attacks. (Source: SATP
	GTI 2024 ranks Pakistan 5th globally; Balochistan's share of deaths rose from 10% in 2020 to 25% in 2023. (Source: GTI 2024)	
Displacement and Humanitarian Toll	Over 100,000 people have been internally displaced (IDPs) since 2020 due to military operations and clashes. (Source: UNHCR 2022 report)	Military operations since the early 2000s have caused the massive displacement of hundreds of thousands from tribal areas to settled districts in KP. Up to 328,000 people were displaced in 2010 alone from Kurram and Orakzai. (Source:

		International Crisis Group Briefing)
--	--	---

The given statistics underscore the challenges orchestrated by terrorism led by militant outfits, further increasing the need for an innovative and AI-driven strategy to fight and counter these threats.

Applications of AI in Countering Terrorism in Pakistan

The figures mentioned above show the severity of the conflict in Balochistan. From terrorism related fatalities to terrorist activity, including suicide attacks, financial loss, damage to property, sectarian violence, and mass displacement resulting in poverty, which fuels extremism, the situation needs urgent intervention and resolution. The data also indicate the limits of conventional security methods, making AI necessary for developing proactive, data-driven solutions to terrorism in Balochistan.

AI is now a transformational tool for resolving conflicts, using fundamental techniques such as machine learning (ML), neural networks, natural language processing (NLP), and data analysis to evaluate large volumes of information, recognize patterns, and enable proactive decision-making. Ultimately, AI works through algorithms (Smith, 2020) that learn from data; supervised learning trains models with labeled datasets for classification/prediction, unsupervised learning finds unseen patterns in unlabeled datasets, and reinforcement learning maximizes action given feedback (Irfan et al., 2023). In conflict areas, these mechanics enable AI to shift from a reactive to a proactive approach to reduce terrorism, while minimizing ethical concerns about training data bias and surveillance privacy. Below are the sections that illustrate the potential uses of AI to support counter-conflict efforts in Pakistan, describing how AI's

computational speed and pattern recognition can assist such efforts.

a) Predictive Analysis

Predictive analysis in AI uses statistical algorithms and machine learning (ML) models to predict future events, using historical and real-time data to help prevent conflicts by anticipating terrorist activities or escalation. The methods employed for predictive analysis include algorithms such as regression models, decision trees, and deep learning neural networks (e.g., recurrent neural networks (RNNs) for time-series data) to analyze input data (such as geospatial data, communication intercepts, behavioral patterns) and produce threat-probability outputs (Khan et al., 2023).

In this context, “Regression” refers to a type of Supervised Learning (SL) in which we use input features to predict a continuous output feature rather than a categorical one. “Decision Tree,” however, is another type of SL that may be applied to both Classification and Regression problems; it has a hierarchical structure and functions as a flowchart that makes decisions one step at a time. Additionally, “Deep Learning Neural Networks” refer to sophisticated forms of AI that utilize multi-layered artificial neural networks, modeled on the human brain, to perform speech/image recognition and natural language processing when standard techniques cannot perform these tasks adequately.

Predictive analysis can fundamentally change how Pakistan identifies and prevents attacks. Using both historical data and current data sources (e.g., satellite images or troop movements), predictive AI can project areas at risk of ambushes or bombings. In regions like Balochistan and KP, where extremist groups take advantage of mountainous terrain, predictive AI can also

recognize patterns in previous attacks and anticipate where future attacks may occur, allowing security personnel to implement preemptive measures, transforming the traditional reactive approach to a proactive one, directly related to the evidence presented at the table of escalating violence outpacing human intelligence capabilities.

Specific tools for implementing predictive analysis include Palantir Gotham (Palantir Technologies Inc., n.d.), an operating system designed for government and defense organizations to aid mission-critical decision-making by integrating and analyzing data to support investigations and missions. US government agencies commonly use Palantir Gotham to support counterterrorism efforts. Another tool includes Recorded Future (Recorded Future, n.d.), operating system located in America that utilizes AI driven predictive analytics to forecast cyber and physical threats including patterns of extremism by processing and utilizing both Open Source Intelligence (OSINT) (Recorded Future, n.d.), the technique or process of gathering and analyzing publicly available information to assess threats, make decisions or answer specific questions in Cybersecurity and Dark Web Data for real-time alerting. For users who prefer open-source options, TensorFlow (Google Brain Team, n.d.), an end-to-end open source machine learning platform and PyTorch, a software-based open source deep learning framework for building neural networks, that combines the machine learning (ML) library of Torch with a Python-based high-level API can be customized to create bespoke models as was reported in recent UN reports on AI for early warning network (Chintala, n.d).

.

b) Surveillance under Large Language Models (LLM)

Surveillance is defined as the use of an advanced Generative AI system (e.g., transformer-based systems, such as GPT variants) to improve monitoring capabilities in conflict zones by processing and analyzing unstructured data, such as text, audio, or intercepted communications. The large language models are capable of producing insights through their self-attention mechanisms, which assign weights to different pieces of data, thereby enabling real-time intelligence and/or anomaly detection. Thus, these models can be used in conflict zones to analyze large volumes of surveillance feed data and identify potential threats, such as communication bias, which may indicate planning activity, enabling proactive intervention (Purohit & Bang, 2024).

Given the vast, rugged terrain in Balochistan and the complex security dynamics in KP, the use of surveillance technology that leverages large language models (LLMs) can be highly valuable. For example, the AI can process real-time sensor or camera data to identify anomalies, such as IED (bomb made and/or used by unofficial or unauthorized forces) placement or militant gatherings, thereby reducing the risk to security personnel. It can detect the use of any such hidden devices or equipment installed to attack or damage any area, and, in advance, inform the authorities to dispose of or disarm them. Furthermore, the AI can anonymize the data, which will help address some of the ethical issues associated with AI, such as privacy violations, and call for ethical governance. Additionally, the ability to use AI-enhanced monitoring to protect critical infrastructure (e.g., CPEC projects, which have cost Pakistan millions of dollars in damage) illustrates how AI can transform raw data into actionable intelligence; however, it requires robust governance to address risks in high-stakes environments.

For example, Anduril (a company developing AI technologies for military and civilian uses, including a surveillance tool called the Lattice Platform) uses LLMs combined with computer vision for AI-based surveillance in conflict zones. The Lattice platform processes drone feed data in real time to detect and classify threats for use in border monitoring by militaries. Additionally, HydroX AI (Hydrox AI, n.d.), an AI tool that provides a comprehensive AI solution platform, including AI Security, LLM Firewall, and AI Governance, ensuring safe AI deployment and compliance provides an LLM Firewall that defends against adversarial input for secure LLM deployment for surveillance applications, providing an additional layer of protection for sensitive data in high-risk environments. Finally, custom LLM tools developed using Meta's open-source model (Llama 3) can be customized for conflict-specific surveillance through Hugging Face. This company supports a large open-source community (referred to as Hugging Face) that develops machine learning tools.

c) AI-driven Social Media Monitoring

The use of AI to monitor social media for terrorist threats and radicalism employs natural language processing (NLP) and computer vision to scan social media for terrorist content, recruiting tactics, hate speech, and other forms of radical content, acting as a sentinel in the digital space where most conflicts begin. The core mechanics of AI include using convolutional neural networks (CNNs), which are types of deep learning models that are specifically designed to process grid-like data (such as images) to find patterns within this type of data, or transformer models which utilize word embeddings (vector representation of text) to determine if there are patterns such as "exact phrases" which are associated with terrorist propaganda. Agencies in South Asia and Southeast Asia have implemented AI

in their tools to aid in identifying and disrupting online terrorist networks, thereby enhancing the ability of national investigations to detect the presence of violent extremists automatically (Al-Ghamdi, 2021).

These tools can also be used to combat the radicalization in Balochistan, which amounts to a 62% share in Pakistan's total 73% rate of rising terrorism deaths, as of February 2025, and the killings of Shia minorities in KP. These tools can prevent the spread of ideologies that support terrorist groups, which recruit based on grievances like poverty and lack of resources.

Some key tools include Dataminr, an AI platform that monitors social media in real time to detect potential threats, enabling law enforcement to track terrorism-related posts and extremist trends in 2025 (Dataminr, 2025). Another tool is ZeroFox, a cloud-based software platform that helps companies expose and disrupt phishing and fraud campaigns; it uses machine learning to automate the removal of violent extremist content across multiple platforms, targeting counter-terrorism initiatives in South and Southeast Asia (ZeroFox, n.d.). For more advanced uses, the UNICRI-UNCCT (an all-encompassing framework and practical toolset developed to assist law enforcement, technology platforms, and policy makers in detecting, monitoring and combating terrorism and violent extremist content posted online by the United Nations) includes open-source AI, such as SpaCy (Honnibal, n.d.), an open-source NLP library for python used to classify and label terrorist propaganda, hate speech, or recruitment narratives, for NLP-based monitoring as documented in reports outlining methods to counteract online terrorism.

d) Financial Tracking of Terror Outfits

The use of AI to track and monitor illegal money transfers for terrorist organizations relies on Graph Neural Networks and

Anomaly Detection Algorithms to model large-scale, complex transaction networks across global financial networks. In practical terms, AI processing of both Structured Data (banking information) and Unstructured Data (intelligence reporting) will use Machine Learning (ML) methods, including Auto-Encoders, to identify outliers in financial data that may indicate terrorist financing. More broadly, AI has expanded Counter Terrorism's capabilities to assess how data quality affects overall effectiveness; however, terrorist actors are increasingly leveraging Generative AI to evade law enforcement and intelligence agencies. One of the greatest strengths of this system is its ability to process large amounts of data through scalable computing, making it possible to predict and disrupt funding sources. However, this requires high-quality, unbiased datasets to avoid false accusations and potential grievances. However, this requires high-quality, unbiased datasets to prevent false accusations and potential grievances. However, this requires high-quality, unbiased datasets to avoid false accusations and potential grievances. However, this requires high-quality, unbiased datasets to prevent false accusations and potential grievances in conflict areas (Sharma et al., 2024).

The considerable impact on the economy also demonstrates the prolonged nature of Terrorism, which is typically supported by either Hawala Networks (Informal Money Transfer Mechanisms that do not physically move money) or external funders. This is where AI can examine blockchain transactions and/or financial trends to break these money channels, thereby reducing the ability of insurgent organizations to receive funding. Through breaking down the money flow to these insurgent groups, the government will be able to ensure that no resources are being sent to those involved with planning and executing terrorist acts against a country's economic backbone, like CPEC. Similar

technologies have been used worldwide to severely damage Terrorist Networks, potentially in Balochistan and KP, to deny Militants the resources required to acquire weapons and conduct military campaigns.

Examples of these tools include TRM Labs (TRM Labs, n.d.), a blockchain intelligence firm that, in 2025, uses AI to track terrorist financing on crypto networks and support national security by linking transactions to designated sanctions entities. Verafin (Nasdaq Verafin, 2025), which was acquired by NASDAQ, provides Cloud-Based Financial Crime Management Technology Solutions for Fraud Detection, Anti-Money Laundering/Countering Financing of Terrorism Compliance, and high-risk customer Management, utilizes Machine Learning to automate the detection of terror-linked transactions with high accuracy in financial crime investigations. SymphonyAI (SymphonyAI, n.d.) is a US-based artificial intelligence firm that provides predictive models, demand forecasting, and fraud detection for financial institutions, offers a Financial Services suite that includes transaction-monitoring tools tailored to detect and prevent terrorist financing and uses AI to recognize patterns in complex datasets.

e) Provision of Humanitarian Aid under AI

AI has been used to support the humanitarian aspect of war by managing logistics and resource allocation through predictive modeling and optimization, using algorithms such as genetic algorithms and reinforcement learning. With data from satellites, sensors, and reporting, AI enables “anticipatory” humanitarian action (forecasting needs based on conflict trends to prevent crises rather than reacting to them). For example, AI platforms quickly process incoming information to enable timely decision-making in high-stakes emergencies and to convert reactive

humanitarian responses into proactive ones. In practice, this translates to creating machine learning models trained on historical disaster data to predict displacement and/or shortages of supplies, and to ensure that aid reaches the most vulnerable population while minimizing the risk of harm in a war zone. In addition to the operational benefits of AI, humanitarian organizations must also address the ethical implications of its use (i.e., protecting data and minimizing technological inequalities). (Khan et al., 2023)

Similarly, AI may also improve the delivery of humanitarian aid in Balochistan and KP to meet the needs of the large numbers of displaced individuals and a 71% poverty rate in Balochistan (Islamabad Policy Research Institute, 2023) and 40% in KP (Niaz, 2024) which have both contributed to the increase of extremist groups (Zaman & Bano, 2021). By utilizing predictive models to forecast humanitarian needs and to map safe routes to deliver humanitarian aid, humanitarian organizations will be able to assist those who need it the most and decrease the vulnerability that leads to recruitment. Therefore, the use of AI and a humanitarian strategy would help alleviate the conflict's humanitarian impact and stabilize a region that continues to experience increased displacement from military operations.

Some tools that can be used in Balochistan include Project Jetson (UNHCR Innovation Service, n.d.), an AI-based forecasting platform developed by the UN and other partners to project population displacement during conflicts and enable humanitarian agencies to plan and allocate aid proactively. Another tool is Dataminr's AI-based model, developed with Insecurity Insight, to analyze conflict data and generate early warnings for humanitarian response agencies, enabling them to focus their aid resources. Finally, commercial AI platforms (e.g., ChatGPT and Claude (AI assistants)) have been widely adopted.

They can be easily integrated via APIs to support logistics planning for humanitarian efforts, as indicated by recent humanitarian mapping reports.

f) AI-driven Safe City Projects

AI will significantly enhance Pakistan's capability to handle conflict-related issues, especially in unstable areas such as Balochistan and Khyber Pakhtunkhwa (Irfan et al., 2023). Utilizing AI's key features: ML, neural networks, NLP, and data analysis, which can analyze big data, identify significant patterns & and make informed decisions proactively. AI-driven cameras have successfully enhanced the Safe City Project in Balochistan through AI-powered camera systems & data analysis of critical patterns (Akhtar, 2024). In KP, however, the Safe City Project has now been revived after an 18-year delay. In this, the AI-camera system can record any unusual activity & send the images to official information centers instantly. The AI-camera system can also store all kinetic threat information & recognize members of all major terrorist groups upon entry into high-security areas in Quetta or Peshawar. However, AI-camera systems need to be placed at all strategic choke points in both major and minor towns in Balochistan and KPK, especially in the outskirts of cities contiguous to militant-prone areas.

In addition, the same AI-camera systems can feed data on all non-cleared Customs-Paid (NCP) vehicles moving into & out of both provinces 24/7. This can be achieved by feeding the data analytics of the NCP-identifier cameras with information on all cleared Customs-Paid cars in Pakistan. When an NCP vehicle is identified as entering a city or area & is engaging in unusual activity, the vehicle is recorded & sent to the appropriate authority before any extreme event occurs. Recently, the military has implemented a basic version of this technology in Quetta

Cantt, using cameras to monitor speed limits for all vehicles within the cantonment.

Global Case Studies from Entities to Counter Terrorism through AI

The application of AI by countries and organizations worldwide to address counterterrorism issues is increasing through various new technologies and methods, including predictive analytics, AI-powered surveillance systems, social media monitoring, tracking financial transaction flows, etc. These are,

The UN Counter Terrorism Efforts driven by AI

The United Nations (UN), through the Counter Terrorism Center and the UN Interregional Crime and Justice Research Institute (UNICRI), is developing AI-based frameworks and guiding law enforcement agencies in South and Southeast Asia to use AI to counter online terrorism. The UN emphasizes that, in developing AI-based counter-terrorism frameworks, it is essential to combine AI's analytic capabilities with respect for human rights and adherence to international law when identifying and disrupting online terrorist communications and/or actions.

US and the EU's usage of AI-based Technologies to Counter Terrorism and Extremism:

Similarly, the US government utilizes AI-based platforms such as Palantir Gotham to link large volumes of intelligence data, enabling real-time threat prediction, social media monitoring, and tracking/analyzing financial flows to and from terrorist organizations to disrupt funding for terrorist activities. Additionally, the US Terrorist Finance Tracking Program uses AI to detect suspicious financial transactions and identify connections between terrorist financiers and terrorist

organizations, thereby preventing funds from flowing to these organizations. Examples of how the US Government utilizes AI in fighting terrorism include; the utilization of AI-based predictive policing and surveillance systems by the Israeli Government to collect geospatial data, communication intercepts and social media data to identify potential terrorist threats and prepare for terrorist incidents and/or operations; the utilization of AI-enabled drones and sensor networks to monitor remote areas in real time to identify threats; and many EU countries are utilizing AI-based platforms to rapidly remove violent extremist content from social media to counter radicalization and terrorist recruitment. Similar to the US government's approach to using AI to fight terrorism, the EU countries are implementing AI-based platforms under strict ethical guidelines to ensure national security and protect individual civil liberties.

GIFCT's AI-based Efforts to Counter Terrorism:

In addition, the Global Internet Forum to Counter Terrorism (GIFCT), which comprises some of the world's largest technology companies, identifies emerging AI-based threats, such as terrorist use of Generative AI to create propaganda and design weapons, and points to the development of AI-based tools to counter these threats (International Centre for the Study of Radicalisation, 2021). The GIFCT also identifies the potential role AI could play in humanitarian contexts, specifically in aiding displaced populations affected by terrorism. As demonstrated globally, there are numerous applications of AI in addressing terrorism issues, including: intelligence gathering; surveillance; financial vetting; social media monitoring; logistical support to humanitarian aid operations; etc. Clearly, the success of these efforts demonstrates the need for access to quality data; culturally aware AI models; robust ethical governance structures; and

international cooperation to effectively utilize AI in the global fight against terrorism in Pakistan.

Conclusion

Pakistan can use artificial intelligence to fundamentally revolutionize the prevention and management of all types of conflict. As Pakistan experiences a growing number of terrorist attacks and remains at risk of terrorism and sectarianism, particularly in its provinces KPK and Balochistan, it needs to transition from traditional, reactive forms of security toward proactive and data-driven forms of security. Pakistan's security establishment can apply advanced AI capabilities for surveillance, social media monitoring, financial tracking, predictive analytics, and the optimization of humanitarian aid delivery to proactively anticipate, prevent, and mitigate the risks associated with various threats in unstable regions. Advanced AI can process vast amounts of data and information, Therefore, the security establishment will be able to identify new patterns in data that it is currently unaware of; predict when an attack is likely to occur; monitor the spread of extremist ideology through social media; interrupt the financing of terrorist organizations; and efficiently deliver humanitarian aid to individuals who are displaced or affected by conflict. Cyber threat intelligence is the theoretical basis for this research study. The research study utilizes two pre-existing theoretical models (The Intelligence Cycle and The Diamond Model) to demonstrate how AI can enhance intelligence, data collection, processing, and dissemination, and to provide conceptual frameworks for addressing ethical considerations related to bias and privacy.

The research study views AI as part of a broader strategy to incorporate innovation, ethics, and international cooperation to address emerging technological challenges. The research study

advocates the creation of a Pakistani-specific Cyber Threat Intelligence Organization, using AI to facilitate more cooperative and intelligence-led counterterrorism efforts. This paper provides examples of how similar concepts have been successfully implemented in other countries. Due to its significant geography and size, multiple and complex insurgent movements operate within it. Moreover, the hybrid nature of the ethno-nationalist and jihadist threats posed by different groups is another challenge. Balochistan is an area in need of AI-enabled systems to help alleviate the shortcomings of human intelligence in a challenging operational environment. The same goes for KPK's complex security environment. In addition, AI-based solutions can help mitigate the humanitarian consequences of conflict, including population displacement and poverty-induced radicalization, by enhancing the delivery of humanitarian assistance and developing early warning systems. The strategic application of AI in combination with strong ethical controls and collaborative mechanisms will significantly improve Pakistan's capacity to combat and defeat violent extremism and terrorism. Furthermore, AI can help resolve the root cause of conflict by creating a more stable and secure environment. This research study provides a practical framework for Pakistan to responsibly leverage the revolutionary potential of AI to create a safer, more resilient future for communities negatively impacted by conflict.

References

- “Academic and Practical Research Working Group White Paper: Extremism Research Horizons.” GIFCT. The International Centre for the Study of Radicalisation, King’s College London, June 2021. <https://gifct.org/wp-content/uploads/2021/07/GIFCT-APRWG-WhitePaper.pdf>.
- “Advanced Cyber Threat Intelligence.” Recorded Future. Accessed December 29, 2025. <https://www.recordedfuture.com/>.
- “AI-Powered Real-Time Event, Threat & Risk Intelligence.” Dataminr, October 21, 2025. <https://www.dataminr.com/>.
- Akhter, Saadullah. “Baloch Separatists Attack Remote Town in Pakistan’s Southwest, Security Forces Regain Control.” Arab News, January 9, 2025. <https://www.arabnews.com/node/2585754/pakistan>.
- Akhtar, Saadullah. “Safe City Project in Pakistan’s Quetta Helps Crack 140 Cases amid Persistent Security Concerns.” Arab News, August 25, 2024. <https://www.arabnews.com/node/2568724/pakistan>.
- Al-Ghamdi, Lina Muhammad. “Towards Adopting AI Techniques for Monitoring Social Media Activities.” Sustainable Engineering and Innovation 3, no. 1 (2021): 15–22.
- Ali, Fahad, Gang Li, Anam Nawaz Khan, Qazi Waqas Khan, Myriam Hadjouni, and Hela Elmannai. “AI-Driven Counter-Terrorism: Enhancing Global Security through Advanced Predictive Analytics.” IEEE Access 11 (2023): 135864–135879.
- “Balochistan’s Dismal Socioeconomic Indices.” Islamabad Policy Research Institute, April 29, 2023. <https://ipripak.org/balochistans-dismal-socioeconomic-indices/>.
- Bansal, Alok. “Factors Leading to Militancy in Balochistan.” Small Wars & Insurgencies 19, no. 2 (2008): 182–200.
- Bussa, Toby. “The Importance of the Diamond Model for Cyber Threat Intelligence.” ThreatConnect Blog, November 29, 2023. <https://threatconnect.com/blog/the-importance-of-the-diamond-model-for-cyber-threat-intelligence/>.
- “End-to-End Platform for Secure and Responsible AI.” Hydrox AI. Accessed December 29, 2025. <https://www.hydrox.ai/>.
- Hussain, Abid. “Deadly Pakistan Train Hijack: What Happened, Who Was Rescued, What’s Next?” Al Jazeera, March 13, 2025.

<https://www.aljazeera.com/news/2025/3/11/deadly-pakistan-train-hijack-what-happened-and-whats-next>.

“Introduction to TensorFlow.” TensorFlow. Google Brain Team. Accessed December 29, 2025. <https://www.tensorflow.org/>.

Irfan, Muhammad, Ziyad Abdulaziz Almeshal, and Muhammad Anwar. “Unleashing Transformative Potential of Artificial Intelligence (AI) in Countering Terrorism, Online Radicalisation, Extremism, and Possible Recruitment.” *Global Strategic & Security Studies Review* 8, no. 4 (2023): 1–15.

Javed, Nimra. “Combating Online Violent Extremism Through AI: Avenues for Pakistan.” *Pakistan Journal of Terrorism Research* 5, no. 2 (2023). <https://nacta.gov.pk/wp-content/uploads/2024/01/Combating-Online-Violent-Extremism.pdf>.

Khan, Sophia Saifi, and Rhea Mogul. “What’s Behind the Surge in Tensions Between Iran and Pakistan?” CNN, January 18, 2024. <https://www.cnn.com/2024/01/18/world/iran-pakistan-attacks-tensions-explainer-intl-hnk>.

“Learning PyTorch.” PyTorch. Soumith Chintala. Accessed December 29, 2025. <https://pytorch.org/>.

Niaz, Tahir. “Poverty Rate Increases in Pakistan from 38.6pc to 39.5pc in Five Years: PIDE.” *The Nation*, May 25, 2024. <https://www.nation.com.pk/25-May-2024/poverty-rate-increases-in-pakistan-from-38-6pc-to-39-5pc-in-five-years-pide>.

“OSINT Framework Explained.” Recorded Future. Accessed December 29, 2025. <https://www.recordedfuture.com/threat-intelligence-101/intelligence-sources-collection/osint-framework>.

“Project Jetson.” UNHCR Innovation Service. Accessed December 29, 2025. <https://www.unhcr.org/innovation/project-jetson/>.

Purohit, Rutuja, and Sanjay Bang. “SecurAI: Leveraging Edge Computing and Large Language Models for Intelligent Surveillance.” In *2024 IEEE 4th International Conference on ICT in Business Industry & Government (ICTBIG)*, 1–7. IEEE, 2024.

Samad, Yunas. “Understanding the Militancy in Balochistan.” In *State and Nation-Building in Pakistan*, 118–145. Routledge, 2015.

- Sharma, Malvika, Abhiranjan Dixit, and Poonam Rawat. "The Use of AI in Surveillance to Identify the Potential Threat of Terrorist Attacks." In 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC), 1–7. IEEE, 2024.
- Siddiqui, Khurram Shahzad. "Terrorist Alliance Formation: The Case of Islamic State and Lashkar-e-Jhangvi in Balochistan (Pakistan)." *Small Wars & Insurgencies* 36, no. 3 (2025): 552–575.
- Smith, Andrew. "Using Artificial Intelligence and Algorithms." Federal Trade Commission, April 8, 2020. <https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-algorithms>.
- "SPACY · Industrial-Strength Natural Language Processing in Python." Spacy. Matthew Honnibal. Accessed December 29, 2025. <https://spacy.io/>.
- "TRM Labs | Blockchain Intelligence Platform." TRM Labs. Accessed December 29, 2025. <https://www.trmlabs.com/>.
- "Verafin Inc." Nasdaq Verafin, November 4, 2025. <https://verafin.com/>.
- Zaman, Nadeem Uz, and Safia Bano. "Terrorism in Balochistan: Issues, Causes, Consequences and Cures." *Pakistan Journal of Terrorism Research* 3, no. 1 (2021): 1–23. <https://nacta.gov.pk/wp-content/uploads/2021/12/Terrorism-in-Balochistan-Issues-Causes-Consequences-and-Cures.pdf>.
- "ZeroFox: The Leader in Digital Risk Protection." ZeroFox. Accessed December 29, 2025. <https://www.zerofox.com/>.