AI-DRIVEN PREDICTIVE SYSTEMS: A TRANSFORMATIVE TOOL IN COUNTERING TERRORISM, WITH A SPECIFIC FOCUS ON INDIA, THE UK, AND THE USA

Modhurima Dalui, Swami Vivekananda University, Kolkata

ABSTRACT

Advancements in technology and global integration in societal governance has expanded the utilization of artificial intelligence and robotics, broadening the scope of societal oversight and administrative convenience. This progress has effectively improved and modified the different strata of societal advancements and progress. Amongst all such expanding horizons of developments, the incessant progress in the trans-boundary evolving research, developments and adaptations of Artificial Intelligence (AI) and Robotics have proved to lay the most effective strategies for defence mechanisms across the worldwide nations, aiding in the prevention of cross-border terrorist attacks. Particularly in defense, India, UK and other European countries has embraced AI to identify potential criminal preparations and intentions of terrorism. This paper focuses on the use of AI in predicting criminal activities, particularly in the context of terrorism. It explores AI's role in counterterrorism efforts in India and its impact on defence mechanisms. This paper also delves to thoroughly examine a comparative analysis of AI's utilization in defence strategies, in reference to the approaches taken in the UK, USA, and India. Additionally, the paper focuses to discuss about the various legal implications in the context of AI predictive system to counter terrorism.

Keywords: Artificial Intelligence, Predictive System, Criminal Profiling, Terrorism, Defence Strategies etc.

Introduction

The rampant instances of constantly growing terrorist activities and threats to cyber securities have throughout the ages targeted and undermined people's faith in the governmental mechanisms across the different democracies of the world. In countering such extremists threats of terrorism upon the governmental institutions and upon the societal framework, the ever evolving governmental tactics and developmental strategies have boosted the use of Artificial Technologies to combat such menaces. The evolving tactics of terrorism and extremist ideologies incorporate the use of digital media, social media forums, processes of coding and encryptions, multimedia exploitations and the use of dark web in dissemination of violent extremism throughout the cyberspace.[1]Recently, the terroristic activities have also crept into Block-chain based virtual assets, online banking forums and online crowd funding resources as their means to exploit the cyber space for executing terroristic activities.[2]

The adaptation and incorporation of the various facets of Artificial Intelligence (AI) have a profound impact on empowering the governments and the defence ministries across various nations in combating such terrorist activities through the use of the digital forums or the cyber space. In such regards the use of AI in developing the ISR System i.e the System of Intelligence, Surveillance and Reconnaissance have immensely contributed in data management and in the installation of counter-terrorism methods.[3]Through the governmental initiatives, the Intelligence agencies have used the means of AI in developing most advanced systems of automated data analytics to boost cyber security measures and developing systems of data visualizations. Further efforts have been laid to develop and use the AI in strengthening Predicting Systems in counterterrorism by ways of algorithms in categorizing Terrorist suspects, routinely reviewing data collected, stored and analysed to cure the potential threats of future terror attacks.

Several tools and mechanisms have been deployed by several nations to demonstrate the potential application of AI in countering terrorism mainly on the online platforms. Amongst the predictive usage of AI, the Generative AI system which is a part of the Artificial

[1]Dr.ObaidSalehAlmukhattin, 'Use of Artificial Intelligence Tools in Countering Terrorism' (Dec.2023) 5 Terrorism Issues, Islamic Counter Terrorism Coalition <https://imctc.org/en/eLibrary/TerrorismIssues/Documents/Terrorism%20Issues%20Issu%205%20EN.pdf> accessed 3 March 2024.
[2]*Ibid.*
[3] Government of India, Ministry of Defence, Artificial Intelligence in Defence: The New Age of Defence <https://www.ddpmod.gov.in/sites/default/files/ai.pdf> accessed3 March 2024.

Intelligence system is a more appropriate addition to the knowledge and implementation of newer technologies in countering terrorism. The Generative AI learns patterns from all the available data from various databases maintained and monitored by the agencies and governmental authorities and produce a profiling system helping to counter the technological advances used by the extremist groups.

With such wide range of effectiveness and applicability of AI based technologies, mechanisms and systems, this paper aims in analysing the roles of AI Predicting Systems in Countering Terrorism, analyses the steps and measures incorporated by India in implementation of such AI based systems in countering terrorism and having an in-depth comparative analysis of the advancement of such AI based technologies across the developed nations comprising of United Kingdom, The United States and America and finally forwarding a suggestive measures to lead this way forward towards further advancements in combating all terroristic activities of the future.

The Role of AI Predicting Systems in Counter-Terrorism

Terrorist attacks are violent acts aimed at instilling fear and advancing political, ideological, or religious goals. These attacks vary in methods from bombings to cyber-attacks and have profound impacts, including loss of life, injuries, economic damage, and social upheaval. Counter-terrorism efforts involve intelligence, law enforcement, international cooperation, and addressing root causes like poverty and extremism.[4]

AI is increasingly being used in counter-terrorism efforts for predictive analytics, identifying potential threats, and monitoring online activities for suspicious behaviour. It has the potential to detect various patterns and abnormalities and is also used to analyse large amounts of data that may indicate terrorist activities. AI prediction systems can be utilized in counter-terrorism for several purposes, including early threat detection, improved surveillance, cyber security, and countering propaganda.[5]In the context of border security, AI is currently implemented in various international borders to secure them such as counter terrorism and illegal immigrant migration. Two algorithms commonly used in these models are the neural network and

[4]Government of India Second Administrative Reforms Commission: Combatting Terrorism Protecting <https://darpg.gov.in/sites/default/files/combating_terrorism8.pdf> accessed 12 March 2024
[5]Kathleen McKendrick, *Artificial Intelligence Prediction and Counterterrorism*, 2019 International Security Department <https://www.chathamhouse.org/sites/default/files/2019-08-07-AICounterterrorism.pdf> accessed 11th March, 2024

AdaBoost. The AdaBoost algorithm helps in identifying and recognising different walking objects across the border, whereas the artificial neural network scans deeply and analyses each object in the image from a distance, and then makes proper predictions.[6]AI, with the help of automated data analytics, has the potential to enhance security services by analysing historical data and current trends. Several techniques related to machine learning have been utilized to predict and identify radicalization, the process by which individuals come to support terrorism and join terrorist groups.[7] Natural Language Processing (NLP) is also an AI branch employed for this purpose. NLP allows computers to comprehend and interpret human languages, facilitating more natural interactions between humans and machines which help in predicting radicalization.[8]In counter-terrorism, before an attack happens, intelligence and security services usually use investigative methods. They start by looking at partially discovered plots or known suspects to find other people involved or to find connections to larger terrorist groups.[9]Various Machine learning techniques and Natural Language Processing are used to analyse the text data such as social media posts or intercepted communications to identify potential threats or suspicious behaviour. The data mining layer is then applied to extract relevant information from large datasets, helping to uncover patterns or relationships that may indicate terrorist activities.[10]Network analysis is another important method to counter-terrorism, which is used to analyse the connections between individuals or groups, helping to identify the key players in terrorist networks. This network is often related to 'nodes' and 'ties. In network models, 'nodes helps in representing different groups, individuals or other collections of actors, such as states. Each node in a network is connected to other nodes through edges, which represent the relationships or interactions between the entities, also known as 'ties. 'Ties' refer to the relationships or connections between nodes in a network. These ties can represent various types of relationships, such as interactions, communications, dependencies, or associations, depending on the context of the network being studied.[11]AI predictive systems also use visualization tools to counter terrorism. These tools play a crucial

[6]Ige T, Kolade A, *Enhancing Border Security and Countering Terrorism through computer vision: A field of Artificial Intelligence*
2023<https://www.researchgate.net/publication/366834320_Enhancing_Border_Security_and_Countering_Terrorism_Through_Computer_Vision_A_Field_of_Artificial_Intelligence> accessed 11th March 2024
[7] Supra Note 4
[8] Countering Terrorism Online with Artificial Intelligence [2021] UNICRI and UNCCT
[9]V.S. Subrahmanian, *Handbook of computational approaches to counterterrorism* (Springer, 2012)
[10]Raj Bridgelall, *An application of Natural Language processing to classify what terrorists say they want*(2022) 11 JSS 23
[11]Steven T. Zech and Michael Gabby, *Social network analysis in the study of terrorism and insurgency: from organization to politics* (2016) 18 ISR 214

role in understanding and controlling terrorism by providing insights into complex data and networks. GIS tools, which are geospatial tools, are effective in monitoring and surveillingterrorist activities, aiming to predict key components including when and where attacks might occur, how they might be carried out, and who might be involved.[12]

There are various algorithms and techniques which are used in a wide range to combat terrorism which are Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs) etc. CNNs are utilized for surveillance, object detection, facial recognition, and analysing satellite images in counter-terrorism efforts. They excel at detecting weapons, explosives, and suspicious packages, identifying individuals in crowds, and tracking movements in remote areas. The CNN model is trained to comprehend the spatial properties of a terrorist dataset. It forecasts terrorist activity by taking into account a number of variables, including as the sort of attack, the success rate, the weaponry used, and the type of terrorists engaged.[13]On the other hand, RNNs are applied for text analysis, speech recognition, predictive analytics, network analysis, and anomaly detection in counter-terrorism. They play a crucial role in identifying threats by analysing communication patterns, propaganda, and extremist content. However, while these algorithms can be utilized to counter terrorism, they can also be maliciously employed by terrorist groups.[14]

The Global Terrorism Database extensively employs machine learning techniques and predictive analysis, achieving an accuracy rate of 79.24%.[15]Hence, AI predictive systems are playing a crucial role in modern counter-terrorism efforts. By leveraging machine learning and data analysis, these systems detect patterns and predict potential terrorist activities with accuracy. However, while AI can significantly enhance security measures, there is a need for responsible use to prevent exploitation of this technology by terrorist groups. Resolving the underlying causes of terrorism and promoting global collaboration continue to be crucial

[12]SalihHakan Can and Mark Leipnik, *Use of Geographic information systems in counter terrorism* 2010 <https://www.researchgate.net/publication/293671543_Use_of_Geographic_Information_Systems_in_Counterterrorism> accessed 11th March,2024

[13]F. Saidi, Z. trablesi A hybrid deep learning based framework for future terrorist activities modeling and prediction(2022) 23EIJ 215

[14]UNCCT, *Algorithms and Terrorism, The malicious use of Artificial Intelligence for terrorist purposes* [2021] UNCRI and UNCCT

[15]E.L.H Uriarte, Alicia Alva, *Machine Learning Techniques to visualize and predict terrorist attacks worldwide using the global terrorism database* (2020) <https://www.researchgate.net/publication/341153162_Machine_Learning_Techniques_to_Visualize_and_Predict_Terrorist_Attacks_Worldwide_using_the_Global_Terrorism_Database> accessed 12th March,2024

elements of successful counterterrorism tactics.

Counter-Terrorism using AI: The Indian Efforts

With a population of almost 1.4 billon people India[16] is affixed at using this huge resource of human intelligence to pave the path of unlocking its potentials in all spheres of development and especially in the rampant growth of research and development in the advancement of Artificial Intelligence and using it as the weapon to India's ever-evolving and most advanced defence mechanisms. India's efforts in boosting AI were witnessed in June 2018 when the first ever National Strategy for AI was launched when the AI Task force was convened to deliver defence specific recommendations to the government. In 2019 such was effectuated to form a High Level-Defence AI Council and a Defence AI Project Agency. Following such initiatives, in 2022 the Government of India published a total of 75 AI using projects to advance its defence system which primarily focused on simulation and autonomous system developments, cyber security enhancements, data processing and analysis, and developing robotics and drones systems.[17]

In the most recent Summit held at New Delhi on Artificial Intelligence in December 2023[18], it has been repeatedly emphasized that India is steadfast at developing the AI and incorporating AI in Counter Terrorism investigations and prosecutions. It was also emphasized that the need to develop an effective tracking system by AI such that the Terrorist agencies can be countered and prevented from misusing such technologies.

In the two-day Anti-Terrorism Conference organized by the National Investigation Agency (NIA)[19], among the elite dignitaries it was discussed and highlighted that the model Anti-Terrorism structure is ought to be established under the purview of the National Investigation Agency. The National Investigation Agency (NIA), the Automated Tooling System (ATS) and the Special Task Force (STF) must execute a combined effort in not limiting their stance to

[16]Finance and Development, International Monetary Fund, *Unlocking India's Potential With AI* (Nilekani&Bhojwani, 2023) <https://imf.org/en/Publications/fandd/issues/2023/12/POV-unlocking-india-potential-with-AI-Nilekani-Bhojwani> accessed 20 March 2024.

[17] Antoine Levesques, *Early StepsIin India's Use for AI for Defence", International Institute for Strategic Studies* (2024) <https://www.iiss.org/online-analysis/online-analysis/2024/01/early-steps-in-indias-use-of-ai-for-defence/#:~:text=Amit%20Shah%2C%20India's%20interior%20minister,AI%20technology%20by%20terrorist%20organisations.> accessed 21 March 2024

[18]*Ibid*.

[19] Government of India, Ministry of Home Affairs, Press Information Bureau, "Model Anti-Terrorism Structure" <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1964733>accessed 21 March 2024.

investigation but in incorporating more innovative measures to counter terrorism.[20] The agencies under the States and the Centre were directed to inculcate a Multidimensional and Artificial Intelligence based use of databases, to combat terrorism.

The recent records reveal that presently the ICJS or the Inter Operable Criminal Justice System of India an extensive network of CCTNS or Crime and Criminal Tracking Network and Systems[21] has been implemented in almost 16,733 police stations, The National Automated Fingerprint Identification System (NAFIS)[22] has till date recorded 90 lakhs fingerprint records, more than 17 lakhs data has been recorded via e-forensics, 22 thousand courts across the nation has been connected through the E-Courts systems, collecting data of over 3 crores of prisoners across India, even Nacro-Offenders have also been enlisted for a data over 5 lakhs by the effective measures of NIDAN or the National Integrated Database on Arrested Nacro-Offenders . The Crime Multi-Agency Centre (Cri-MAC) and the National Cyber Crime Reporting Portal (NCRP) have tracked over 14 lakhs alerts and 28 lakhs complains respectively, the NDHTO of the National Database of Human Trafficking Offenders has actively tracked the data of over 1 lakh trafficking cases. The Integrated Monitoring of Terrorism also called the i-MOT[23] has collected a data of 22 thousand terrorist activities in India. The biometric databases of prisoners and the comprehensive information about their visitors are also been monitored and kept records of and finally the databases tracking all the national terrorist activities by the NIA, this extensive resource of database management has laid the grounds for suing Artificial Intelligence through and completely automated system of monitoring and profiling terrorist activities to combat in advance all such threats of terrorist activities in the future.[24]

India has already paved the roadmap through the Defence AI Project Agency (DAIPA)[25] in developing AI enabled applications covering areas of Cyber Security, Online Data Surveillance, Training and Simulation, Multi-Sensor Data Management and Fusion system,predictive Management in curbing online terrorism. The various steps

[20]*Ibid*.
[21]Government of India, Ministry of Home Affairs, *Crime and Criminal Tracking Network and Systems*, Digital Police System <https://digitalpolice.gov.in/DigitalPolice/AboutUs> accessed 21 March 2024.
[22]Supra note 17.
[23]Supra note 19.
[24]Supra Note 17.
[25] Government of India, Ministry of Defence, *Enhancement of Capabilities of AI Technologies,* PIB Delhi (2022) <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1846937> accessed 22 March 2024.

alreadyincorporated in India in combating terrorism by the use of AI predictive mechanisms are as follows:[26]

1. **Project of Drone Feed Analysis**: This is a form of AI based Robotics Process Automation which is being applied to further the military intelligence in India through the ISTAR Missions (Intelligence Surveillance Target Acquisition and Recoinassanceand Live Monitoring of counter terrorism operations.

2. **Storm Drone Project, Automated Room Intervention Drone:** In countering terrorism intervention operations this form of AI enabled automated lethal and non-lethal payload drones are extensively used in building clearances, surveillances, military assistance and disaster managements in combating terroristic activities especially in GPS denied areas.

3. **Project Seeker:** This AI based Facial Recognition Monitoring System is an effective weapon of recognition, monitoring, surveillance, tracking and identification of threats for countering terrorism and terroristic alerts. This AI based system has become an integral part of state-of-the-art- of critical civilian and military establishments in combating Terrorism.

4. **Motion Detection and target Identification**: in physical forms the AI based systems and automated robotics engineering has developed the systems of counter insurgencies, counter terrorism by real time motion detection, identification and targeting, such real time feels on the line of control across the nation has been immensely successful in combating terroristic activities.

Thus the introduction of autonomy in the weapon system has become an indispensable asset preventing terroristic activities, preparing counter-terrorism measures, through the Intelligence, Surveillance, Reconnaissance i.e. the IRS Data Management System based data management systems.[27] All such efforts forming an integral part of the project of incorporating the tenets of AI in Military and Defence Forces to combat Terrorism in India has been more of

[26] Government of India, Ministry of Defence, *Artificial Intelligence in Defence: The New Age of Defence*<https://www.ddpmod.gov.in/sites/default/files/ai.pdf> accessed 20 March 2024.
[27] Supra note 24.

the main ideals of India becoming the face of development and progress through the expanses of 'Atmanirbhar Bharat'.

AI in Counterterrorism: UK & USA Focus

AI predicting system has been extensively used in counter terrorism efforts and also in predicting various criminal activities all over the world. The UK plays a significant role in the development and implementation of AI predictive systems, particularly in the context of counter-terrorism.[28]The UK is internationally recognized as a leading hub for AI and is ranked highly in 'AI-readiness'. The government of UK had brought the National AI Strategy in 2021which outlines the government's vision for AI in the UK and includes provisions for AI in defence and security. The three pillars of this program are investing in the long-term needs of the AI ecosystem, guaranteeing the benefits of AI across all industries and geographies, and efficiently regulating AI. This strategy emphasizes research and development of Artificial Intelligence in collaboration with other countries worldwide. It also underscores the importance of data access, where AI can be utilized to secure data and to analyse potentially threatening data. It also focuses on strategies where AI can identify intricate patterns, reveal new insights, and offer advice on optimizing system inputs to achieve defined objectives more effectively.[29] The AI predictive system in UK has also concentrated on utilizing 'behavioural biometrics' to recognize users by analysing distinct aspects of their digital behaviour, such as mouse movements or sentence composition in a document.[30] The UK has implemented AI systems for various aspects of counter-terrorism, such as threat detection, monitoring online activities, and analysing large datasets. These systems help security agencies in identifying and responding to potential threats more efficiently.[31] The four main pillars of the UK's counterterrorism strategy are Prepare, Protect, and Pursue Prevent. Within this framework, the UK has integrated AI predictive systems into its counter-terrorism endeavours, including efforts such as:

1) **The Joint Security and Resilience Centre (JSaRC): -**This centre focuses on the PROTECT duty which uses innovative technologies and machine learning techniques

[28]Government of UK, *National AI Strategy*<https://www.gov.uk/government/publications/national-ai-strategy> accessed 22nd March,2024
[29]Government of UK, National AI Strategy(2021) <https://assets.publishing.service.gov.uk/media/614db4d1e90e077a2cbdf3c4/National_AI_Strategy_-_PDF_version.pdf> accessed 22nd March, 2024
[30]A. Babuta, M.Oswald*, Artificial Intelligence and UK national security* <https://static.rusi.org/ai_national_security_final_web_version.pdf> accessed 23rd March,2024
[31] Supra Note 5

to support security growth and enhances UK's security. Its goal is to provide customized solutions and identify and shape government security requirements.[32]

2) **AI in identifying radicalisation: -**The UK government's PREVENT duty uses AI to identify individuals at risk of radicalization and intervene before they become involved in terrorism. The AI predicting system is used to predict groups or individuals supporting violence.[33]

3) **Counter Terrorism Operations Centre (CTOC):** -This centre is aligned with the UK's PURSUE strategy. It focuses on putting together the right personnel, information, and tools to more effectively locate, analyse, and dismantle terrorists. It uses AFR technology i.e. the Automated Facial Recognition Technology to identify individuals in public places. It also uses automated data analytics to analyse data and to detect potential terrorist activities or threats.[34]

4) **AI in Border Security:** -The UK is also focusing on digital borders as part of its efforts to enhance national security and counterterrorism. Digital borders refer to the use of technology, such as AI, biometrics, and advanced analytics, to strengthen border controls and identify potential threats. This includes monitoring and analysing digital footprints, such as online communications and travel patterns, to detect suspicious activities and individuals.[35]

In the United States, terrorist groups such as ISIS, al-Qaida, and Hizballah are actively plotting attacks against the country. The Department of State is working to gather global support to weaken and defeat these threats. Through diplomacy and aid, the Department is assisting foreign governments in enhancing their capacity to prevent, detect, and respond to terrorism. This effort includes bolstering law enforcement, improving border security, sharing information on a global scale, combating terrorist financing, enhancing crisis response, and countering violent extremism. The State Department is also encouraging countries to take more

[32]Government of UK, Joint Security and Resilience Centre <https://www.gov.uk/government/groups/joint-security-and-resilience-centre-jsarc>accessed 23rd March 2024
[33]Supra Note 6
[34]Government of UK, Counter terrorism Strategy2023 <https://www.gov.uk/government/publications/counter-terrorism-strategy-contest-2023/counter-terrorism-strategy-contest-2023-accessible> accessed 23rd March,2024
[35]Implementing digital Borders at UK: Lessons from the rest of the world <https://www.openaccessgovernment.org/implementing-digital-borders-uk-lessons-ai/156666/>accessed 23rd March,2024

responsibility for addressing terrorism and to enhance their own counterterrorism capabilities.[36] As the UK the US also focuses to use AI in countering terrorism, it is used in threat detection, enhancing security, surveillance etc. In the United States, NATO plays a crucial role in U.S. national security and defence strategy. As a founding member of NATO, the U.S. is deeply committed to the alliance's objectives, which include collective defence, crisis management, and cooperative security.[37]NATO employs technological advancements to minimize the impact of terrorist attacks, utilizing innovative or modified technologies and methodologies to detect, disrupt, and prevent asymmetric threats. These efforts encompass various areas, such as countering unmanned aircraft systems (C-UAS), utilizing biometrics, technical exploitation, and combating improvised explosive devices (C-IED).[38] The US uses AI in various ways to counter terrorism such as: -

1) **Joint Improvised Threat Defeat Organization (JIDO): -**Thisaims to enhance the U.S. Department of Defence's ability to respond tactically to improvised threats. It involves quickly getting resources to help combatant commands prepare for and handle unexpected events in counterterrorism, counter-insurgency, and related areas, like dealing with improvised explosive devices. The JIDO uses AI and machine learning to find and counter these devices used by terrorist groups.[39]

2) **Supporting Disaster Survivors: -** The Federal Emergency Management Agency (FEMA) leverages AI to swiftly evaluate damage to homes and buildings following disasters. AI-driven computer vision technology identifies damaged structures from aerial images, while human analysts verify the extent of the damage. This approach enables FEMA to process millions of images within days, completing thousands of assessments within a week after a disaster.[40]

3) **Defending Cyber Threats: -** The Cybersecurity and Infrastructure Security Agency (CISA) in the U.S. uses AI to improve its ability to detect and report cyber

[36]U.S. Department of State, Countering Terrorism <https://www.state.gov/policy-issues/countering-terrorism> accessed 23rd March,2024
[37]NATO, Countering terrorism <https://www.nato.int/cps/en/natohq/topics_77646.htm> accessed 23rd MArch,2024
[38]Ibid.
[39]U.S. Department of Defence, Improvised Threats Organization Becomes Part of Defense Threat Reduction Agency<https://www.defense.gov/News/News-Stories/Article/Article/961926/improvised-threats-organization-becomes-part-of-defense-threat-reduction-agency/> accessed 23rd March, 2024
[40]U.S. Homeland Security, Using AI to secure the Homeland <https://www.dhs.gov/ai/using-ai-to-secure-the-homeland> accessed 23rd March 2024

> vulnerabilities in critical infrastructure, including power plants, pipelines, and public transportation systems. CISA's Cybersecurity Division employs machine learning and natural language processing models to collect and categorize vulnerability data, which is subsequently reviewed by human analysts.[41]

Thus, the utilization of AI in counterterrorism represents a pivotal advancement in national security strategies, particularly evident in the innovative approaches adopted by the UK and USA. By harnessing the power of AI, these nations are significantly enhancing their capacity to detect, prevent, and respond to terrorist threats in a dynamic and evolving landscape. The focus of the UK and USA on AI in counterterrorism is not just strengthening their security systems but also establishing a model for other countries. By employing advanced AI algorithms and predictive analytics, these nations can analyse extensive datasets to detect patterns and anomalies, helping them stay proactive against potential threats. The collaboration with other nations is also enhancing their intelligence cooperation to identify and disrupt terrorist activities worldwide. They also engage in engage in joint military exercises and training programs with other nations to improve their collective ability to respond to security threats.

Legal Implications To Counter Terrorism

Terrorism imposes a major threat to a nation which poses risks to public peace and harmony in the society. To combat such menace several technological and digital developments and advancements are taking place through the advent and advancement in the technologies related to Artificial Technologies. Such advancements has its share of challenges and shortcomings in the socio-legal spectrum not only in the local levels but at the international forums also. Some of such areas in concern of facing legal shortcomings in the advent of AI usage in countering terrorism are primarily the human rights concerns.

The United Nations General Assembly, through its Resolution 68/167 on the Right to Privacy[42] emphasized that in this digital age, "the unlawful and arbitrary collection of personal data" is a highly intrusive act that can severely violate the right to privacy and freedom of expression, conflicting with the principles of a democratic nation. Deploying auto generated online

[41] Ibid.
[42] Resolution adopted by the United Nations General Assembly, Resolution 68/167 on "*The right to privacy in digital age"*, on 18th December 2013.

applications and designs to counter terroristic activities would directly target the freedom of thought by triggering actions based upon individuals expressions and activities also online which may generally qualify as only thoughts protected by democratic rights. This poses the risk of radicalization by the usage of AI based technologies in countering terrorism whereby for effective implication all large and small activities shall be captured and targeted including those which do not posses potential threats in reality. Therefore under such circumstances the Executive Directorate of United Nations Counter Terrorism Committee has called upon the policy makers across the nations to demarcate the illegal and not governmental activities which posses the threat to the nations safety and security in effectively countering terroristic activities and help the AI based technologies to efficient in distinguishing activities of people based on democratic rights from activities that pose the threat of terrorism.[43]

Also, the indiscriminate access to personal data and information by the AI applications for the smooth functioning to locate and eradicate threats of terrorism are also concerning towards the security of personal data and privacy. This is also a challenge that the national and the international forums have yet to look into and frame a mechanism accordingly. Therefore, the United Nations Office of Counter Terrorism and the International Crime Police Organization the laws establishing the automatic data collection and storage, the list of entities having access to the same and the purpose for such collection must be communicated to individuals for all their online activities.[44]

Further the other most challenge posed in the usage of the AI in generating effective measures to combat terrorism are the intricacies of the admissibility of such evidences in the court of law. For the legal framework to be applicable in true spirit and for the proper acceptance of the AI applications as legally just and fair mechanism not contradicting the statutory legal frame works of the nations, the legal admissibility determination of such evidences is mandated. Through the admissibility of digital evidence has become an integral part of the nation's justice delivery system, therefore the urge of preparing additional guidance to demarcate and determine the nature and extent of admissibility of AI evidences in countering terroristic activities have gained international recognition and importance. The United National Interregional Crime and Justice Research Institute have raised this issue for the earliest

[43] United Nations Office of Counter-Terrorism, *Countering Terrorism Online With Artificial Intelligence*, UNICRI<countering-terrorism-online-with-ai-uncct-unicri-report-web (1).pdf> accessed 22 March 2024.
[44] INTERPOL and UNOCT, *Using the Internet and Social Media for Counter Terrorism Investigation: Report of the United Nations High Commissioner for Human Rights* , A/HRC/39/29, dated August 3, 2018.

determination of admissibility of AI based and derived evidences in the courts of law which awaits national incorporation and implementation.[45]

The Concluding Note

The fight of all the nations trans-boundary, calls for the extensive collaborative efforts across the global level till the grassroots levels, involving active participation of the national agencies and the international co-operations to use all the evolving technological amenities, using all the artificial intelligence advances, to prepare a combat ground to counter terrorism worldwide. With the ubiquitous presence and usability of artificial intelligence, non-arguably the defence forces of every nation are mandated to develop further AI mechanism and systems as the quintessential technological emergence[46] to strengthen the defence mechanisms of the nations. Presently, the automated data analytics support the intelligence and security measures through digital visualization identification, analysing the various algorithms on terrorist suspects, collecting and routinely checking the information and data revealing patterns to counter possible terrorist attacks and also expose the networks used for probable terrorist activities and suspicious incidents. The major systems that have been playing a pivotal role in combating suspicious terrorist activities is through predictive analytics of AI.[47] The various law agencies and counter terrorism agencies across the nations have proved to use such analytics to expose trends and behaviours of future terrorists and have helped in successfully nullifying such efforts. Such analytics have also served to mis-information spreading and abusive tactics that the various terroristic activities undertake to victimise the public and governmental agencies. Thus overall, AI has proved to be the most adequate and adept mechanism to combat the modern day technologically driven terrorism activities across the globe. But still since it is ever evolving and ever developing have a strong hold over such technological advances become the new challenge since left to the wrong intents and without scrutinization can become a tool of destruction, putting at risk the public safety, security and a nation's integrity at large.

[45] INTERPOL and UNICRI, *Artificial Intelligence and Robotics for Law Enforcement* < https://unicri.it/artificial-intelligence-and-robotics-law-enforcement> accessed on August 7 2024.
[46]VenuTuteja&Anr., *Artificial Intelligence: Threat of Terrorism and need for better counter-terrorism efforts*, Vol.2 No.1 IJCC 87 [2023] <https://www.inderscience.com/info/inarticle.php?artid=133551> accessed 21 March, 2024.
[47] United Nations Office of Counter-Terrorism, *Countering Terrorism Online With Artificial Intelligence*, UNICRI<countering-terrorism-online-with-ai-uncct-unicri-report-web (1).pdf> accessed 22 March 2024.

The Way Forward

AI has proved to be the most effective mechanism to establish a predictive system in countering terrorism but it is also faced with several challenges. Amongst the several challenges the main challenge is sticking the balance between securing privacy to the public and collecting the personal data to analyse to predict the future terrorist activities. The second challenged posed is that the access to online platform cannot restricted amongst the masses and thus in spite of having several scrutinise, there always a chance remains that the extremist groups and agencies to hack systems and use the other means of Generative AI mechanisms to clone governmental sites and misuse the resources and thus still pose the threats of terrorism. Further the laws guiding the AI dynamics and mechanism are yet not developed across the world posing a challenge to the law enforcement mechanism to control and supervise all the procedures. Further the other major lacunae faced is the amount of data collected is huge and therefore surfing through such tons of data in analysing patterns and therefore forecasting terrorism threats are extremely difficult and challenging. Therefore, the several steps that are to be immediately implemented to possibly cure the defects are: -

1) To establish new legislations and policy frameworks to guide the access and use of AI by public.

2) AI based systems training amongst the security agencies have to be mandated

3) To enhance regular modes of scrutiny and surveillance

4) Regular scrutiny of the AI bases applications and tools that are developing and opened to the public for access are to be regulated

5) Categorization of the offences and the trends of possible offences are to be made to effectuate mechanisms accordingly;

6) Constant research and development have to be made to reach a desired goal in having the most effective tools using AI in countering Terrorism.