ARTIFICIAL INTELLIGENCE IN COUNTERTERRORISM

NAVIGATING THE INTERSECTION OF SECURITY, ETHICS, AND PRIVACY

ERMAN AKILLI

SETA | PERSPECTIVE

APRIL 2024 . NUMBER 73

- How can Artificial Intelligence (AI) technologies be used effectively for counterterrorism efforts?
- How does the quality of data affect the effectiveness of AI in counterterrorism?
- What are the ethical and privacy considerations in using AI for counterterrorism?

INTRODUCTION

On 22 March 2024, a terrorist attack occurred in Moscow, the capital of the Russian Federation. According to Russian authorities, gunmen clad in camouflage opened fire at Crocus City Hall, resulting in more than 60 fatalities and 145 injuries[1]. This tragic event reignited ongoing claims and suspicions surrounding such attacks, leaving a significant question lingering in the aftermath: Could it have been prevented?

Domestic terrorist attacks have consistently posed a complex dilemma, juxtaposing the need for national security against the preservation of individual rights. States find themselves periodically facing a fundamental challenge that resonates globally; balancing the imperative to protect citizens from internal security threats while upholding the individual rights and freedoms that form the bedrock of democratic societies[2].

This challenge extends beyond theoretical debate, touching upon policy, law enforcement, and civil liberties in tangible ways. In response to terrorist acts, governments are often compelled to intensify surveillance measures, fortify border security, and broaden the scope of law enforcement powers. Although aimed at public safety, these measures can inadvertently infringe on privacy rights, freedom of speech, and freedom of movement, sparking discussions among policymakers, security experts, and advocates for civil rights[3].

The terrorist attack in Moscow starkly illustrates this ongoing balancing act. As investigations unfold and the public demands answers, a broader dialogue persists on how societies can effectively counter terrorism without compromising the democratic values they hold dear. This incident highlights the urgent need for strategies that not only mitigate the threat of terrorism but also safeguard the fundamental rights and liberties that characterize open, democratic societies. In this context, it is imperative to explore whether emerging

[1] "Death toll from concert hall attack in Russia's Moscow region rises to 143," Anadolu Agency, (March 28, 2024), retrieved from https://www.aa.com.tr/en/asia-pacific/death-toll-from-concert-hall-attack-in-russia-s-moscow-region-rises-to-143/3177180.

[2] "Countering Terrorism Protecting Human Rights," OSCE, retrieved from https://www.osce.org/files/f/documents/d/6/29103.pdf.

[3] "The Delicate Balance Between Civil Liberties and National Security," retrieved from https://www.venice.coe.int/SACJF/2006_08_MOZ%20Maputo/Hamilton_delicate_balance.htm.

ERMAN AKILLI

Assoc. Prof. Dr. Erman Akıllı is currently serving as a faculty member in the Department of International Relations at Ankara Hacı Bayram Veli University. His areas of expertise include artificial intelligence in foreign policy, digital diplomacy, the Central Asia region, the Organization of Turkish States, soft power, and its sub-branches. Throughout his academic career, he has published articles in peer-reviewed journals indexed in SSCI and WOS; and has contributed as an author and editor to books published by prestigious publishing houses such as Routledge, Palgrave MacMillan, and Springer Nature. Additionally, he served as the chief editor at the OSCE Academy in Bishkek between 2023-2024 and continues his work as an assistant editor for the Insight Turkey journal published by SETA.

technologies, such as Artificial Intelligence (AI), could provide a viable means to address such threats. AI offers the potential to significantly enhance security infrastructure through advanced surveillance, data analysis, and predictive modeling. However, the integration of these technologies also prompts crucial considerations regarding privacy, ethics, and the risk of misuse. The exploration into the opportunities and challenges presented by AI in counterterrorism efforts compels a careful navigation of the delicate balance between embracing innovation and preserving individual liberties. This paper not only aims to assess the feasibility of leveraging AI in this domain but also to contemplate the broader implications for society and governance.

UTILIZING ARTIFICIAL INTELLIGENCE IN COUNTERTERRORISM EFFORTS

AI has captured global attention for its remarkable ability to process extensive datasets, revealing patterns and insights that remain invisible to human analysis.[4] This capability greatly enhances the efficiency and effectiveness of parsing complex information. As a multifaceted technology, the benefits of AI extend across numerous domains, including counterterrorism. In this field, AI's prowess in swiftly deciphering and interpreting intricate data is invaluable, pioneering innovative methods for detecting potential threats and formulating effective preventative strategies. The deployment of AI in counterterrorism not only demonstrates its substantial potential in security and defense tactics but also underscores its transformative influence across various sectors, emphasizing its critical role in contemporary analytical methodologies.[5]

First and foremost, it's vital to recognize AI technology's profound reliance on data[6]. While it's commonly said that data is the new oil, a more accurate analogy is that data resembles unrefined crude oil.[7] Just like the value of crude oil is determined by its volume, refinement, and organization, so is the value of data. Data acts as the fuel for AI, meaning the performance of an AI model is closely linked to the quality of the data it is trained on.[8] Therefore, without accurate and reliable data for training AI models, especially in counterterrorism, there is a significant risk of failing to fully leverage this groundbreaking technology to address our most pressing challenges.

Fundamentally, AI operates by scrutinizing large datasets to identify patterns and make predictions. Given the unique capabilities of AI systems, the essential task involves navigating through these vast reserves of data to extract actionable insights. In the current era, awash with data –from social media interactions and financial transactions to ride-sharing services like Uber and Bolt, as well as surveillance footage in public spaces– a tremendous amount of data is continuously gathered. This explosion of 'Big Data' presents a dual-edged sword: the opportunity and challenge of harnessing it effectively. At this critical juncture, specific AI technologies such as image processing, facial recognition, anomaly detection, predictive analytics, and social media monitoring stand out as essential tools for bolstering security measures and averting potential threats, playing pivotal roles in threat identification.

Image Processing and Facial Recognition

"Image Processing and Facial Recognition" technology can significantly enhance security measures by identifying known or suspected terrorists in real-time across various settings, such as airports, train stations, and public events. Essentially, this technology scans faces in crowds to match them with databases

[4] Patrick Amponsah and Amos Atianashie, "Navigating the New Frontier: A Comprehensive Review of AI in Journalism," Advances in Journalism and Communication, Vol. 12, (2024), pp. 1-17.

[5] Kathleen McKendrick, Artificial Intelligence Prediction and Counterterrorism, (Chatham House, 2019).

[6] Willem Sundbladeurope, "Data Is The Foundation For Artificial Intelligence And Machine Learning," Forbes, retrieved from https://www.forbes.com/sites/willemsundbladeurope/2018/10/18/data-is-the-foundation-for-artificial-intelligence-and-machine-learning/?sh=5bd023c451b4.

[7] Nisha Talagala, "Data as The New Oil Is Not Enough: Four Principles For Avoiding Data Fires," Forbes, (2022), retrieved from https://www.forbes.com/sites/nishatalagala/2022/03/02/data-as-the-new-oil-is-not-enough-four-principles-for-avoiding-data-fires/?sh=6863a34cc208.

[8] "National Artificial Intelligence Research And Development Strategic Plan 2023," retrieved from https://www.whitehouse.gov/wp-content/uploads/2023/05/National-Artificial-Intelligence-Research-and-Development-Strategic-Plan-2023-Update.pdf.

of known individuals. Furthermore, recent developments in the technology industry have made it common to see AI-powered cameras capable of detecting even weapons.[9]

By leveraging existing camera networks in large-scale environments like schools, airports, or corporate campuses, algorithms can detect guns or shotguns. Initially, the system marks the firearm in orange as suspicious before quickly escalating to a red alert within seconds. A security officer receives a notification on their cell phone; subsequently, the software provides a still image that details the firearm and identifies the suspect. This facilitates the decision-making process on whether to deploy first responders or to dismiss the alert as a false alarm. For example, the AI can distinguish between a gun and a sprinkler head.[10] Nonetheless, as mentioned above, this technology heavily relies on vast amounts of data to be refined. As it continues to gather video data and fine-tune algorithms and models for better object recognition, we can expect the accuracy to steadily improve over time. However, Image Processing and Facial Recognition's implementation raises concerns regarding privacy, potential bias, and the accuracy of identifying individuals across different demographics.[11]

Anomaly Detection Systems

AI-powered anomaly detection systems play a pivotal role in counterterrorism efforts by identifying deviations from usual patterns and behaviors. These systems excel in uncovering suspicious activities across financial transactions, travel patterns, and online communications, serving as proactive tools in the early detection of potential threats. Their effectiveness in preemptive threat identification helps prevent attacks before they occur, with a focus on reducing false positives and maintaining privacy.

In the realm of Suspicious Activity Reporting[12] (SAR), AI-enhanced anomaly detection is particularly critical. SARs, essential for detecting and countering financial crimes such as money laundering and terrorist financing, have traditionally been challenging due to the need to filter through vast amounts of transactional data. AI simplifies this process, merging speed, accuracy, and efficiency to enable financial institutions to pinpoint anomalies more effectively. By employing advanced machine learning and pattern recognition, AI improves the SAR process, providing real-time monitoring capabilities that greatly diminish the opportunity for financial crimes to go undetected. Nonetheless, incorporating AI into SAR compliance presents challenges, including ethical considerations and data privacy, alongside the necessity to keep pace with changing regulations. Despite these obstacles, the critical role of human judgment remains, especially for evaluating intricate or uncertain situations highlighted by AI.[13]

Predictive Analytics

Predictive analytics employ historical data and AI algorithms to forecast future events[14], including potential terrorist threats. By analyzing vast amounts of data, including communications, transactions, and movements, predictive models can suggest when and where a terrorist act might occur. While promising, the ethical considerations regarding surveillance and the risk of profiling need careful management. Additionally, the reliability of predictions and the potential for overreliance on automated systems are critical concerns.

[9] "Threat Awareness System with Advanced AI," Iterate.ai, retrieved from https://www.iterate.ai/solutions/threat-awareness-system.

[10] David Louie, "New artificial intelligence feature to detect guns through surveillance video," ABC 7 News, (2020), retrieved from https://abc7news.com/gun-safety-artificial-intelligence-omnilert-security-cameras/7431778/.

[11] "Cameras Everywhere: Examining The Conflict Between Technology and Human Rights," SWE, retrieved from https://alltogether.swe.org/2020/01/cameras-everywhere-examining-the-conflict-between-technology-and-human-rights/.

[12] "What is a suspicious activity report?", Thomson Reuters, retrieved from https://legal.thomsonreuters.com/en/insights/articles/what-is-a-suspicious-activity-report

[13] Joseph Ibitola, "Leveraging AI in Suspicious Activity Reporting," Flagright, (2023), retrieved from https://www.flagright.com/post/leveraging-ai-in-suspicious-activity-reporting

[14] "What is predictive analytics?," IBM, retrieved from https://www.ibm.com/topics/predictive-analytics

Implementing such technology faces challenges, especially due to data limitations. Terrorist attacks, with varied motives and methods, produce unique digital traces influenced by factors like beliefs or mental health, participant numbers, and communication modes (possibly encrypted). Spotting patterns is difficult within a single dataset but improves with cross-dataset analysis, which requires detailed scrutiny and increases the dataset's 'dimensionality'. Machine learning algorithms for mass surveillance must be trained on diverse datasets to detect patterns effectively. This introduces the 'curse of dimensionality' in big data, where more complex datasets hinder statistical analysis, reducing algorithm accuracy and performance. More detailed information per suspect enhances accuracy but requires larger datasets, making the scarce documented terrorist attacks insufficient for thorough training.[15]

On the other hand, Deep Neural Networks (DNNs)[16], known for their precision, significantly boost the predictive analytics framework. Excelling in complex pattern recognition within large datasets, DNNs are particularly suited for predictive tasks. They model high-dimensional data intricately, enhancing forecast accuracy. Through extensive learning from historical and current data, DNNs achieve higher prediction accuracy than many statistical methods. Their multi-layer processing provides a nuanced data understanding essential for accurate outcome prediction across various contexts. DNNs also refine decision-making by offering visualizations and scores, thus enabling more precise and informed decisions. DNNs can mitigate some issues posed by the curse of dimensionality by progressively reducing data dimensionality. Although DNNs do not entirely eliminate the curse of dimensionality, they provide a robust framework for effectively managing and analyzing high-dimensional data. This makes them a valuable tool in predictive analytics and other fields that require complex dataset analysis.

Social Media Monitoring

The significant increase in the volume of data related to individuals' online behaviors, notably on social media platforms, has garnered substantial interest in recent years. Researchers and security agencies are diligently exploring the use of social media data to predict terrorist activities. This exploration is rooted in the belief that patterns in social media usage and interactions can reveal vital insights into an individual's intentions, affiliations, and potential plans, making it a critical asset in preemptively addressing threats. It is indeed accurate that terrorist groups frequently exploit social media for propaganda, recruitment, and communication. Utilizing AI to monitor these platforms assists in identifying and disrupting such activities. AI technologies, such as Language Learning Models (LLMs) and Convolutional Neural Networks (CNNs), are adept at analyzing text, images, and videos for extremist content, flagging them for subsequent human review. The effectiveness of these AI tools relies on their ability to comprehend context and nuances, thereby reducing the likelihood of mistakenly censoring legitimate content while accurately identifying genuine threats. Maintaining a balance between security and freedom of speech presents a significant challenge in this area.[17]

As Vladimir Voronkov, the first-ever Under-Secretary-General for the UN Counter-Terrorism Office, claims that by leveraging quantum computing in conjunction with AI, accelerated information processing can enable effective terrorist tracing in social media. He explained, *"The Internet content of terrorists is detected and deleted faster than ever…fifteen to twenty minutes*

[15] H.M. Verhelst, A.W. Stannat, & G. Mecacci, "Machine Learning Against Terrorism: How Big Data Collection and Analysis Influences the Privacy-Security Dilemma," Sci Eng Ethics, Vol. 26, (2020), pp. 2975–2984.

[16] M. Irfan Uddin, et al., "Prediction of Future Terrorist Activities Using Deep Neural Networks," Complexity, Vol. 2020, retrieved from https://doi.org/10.1155/2020/1373087

[17] "Countering Terrorism Online With Artificial Intelligence: An Overview For Law Enforcement And Counter-Terrorism Agencies In South Asia And South-East ASIA," UN Office of Counterterrorism, retrieved from https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/countering-terrorism-online-with-ai-uncct-unicri-report-web.pdf.

is enough to detect and remove such content thanks to machine algorithms".[18]

CONCLUSION: 'CHALLENGES YET TO BE ANSWERED'

In September 2017, Russian President Vladimir Putin made a historic statement, saying, *"Artificial intelligence is the future, not only for Russia but for all humankind. It comes with colossal opportunities but also threats that are difficult to predict. Whoever becomes the leader in this sphere will become the ruler of the world."* [19] For many[20], this statement brought AI from cutting-edge technology laboratories to the attention of the international public. Henceforth, it is essential to comprehend the significance and reasons behind AI's potential impact on national security, whether its effects are revolutionary or simply incremental.

The effectiveness of AI significantly depends on the quality of its data inputs, highlighting the need for a cohesive data strategy that seamlessly integrates AI into existing technological frameworks.[21] The efficacy of AI in processing data is not solely determined by the volume of data but also by its representativeness and lack of bias, crucial for interpreting complex human behaviors accurately.

AI plays a pivotal role in enhancing counterterrorism efforts by efficiently processing and analyzing large datasets. It supports the identification of patterns and connections within terrorism-related data, such as incident reports and counterterrorism activities, thereby aiding in the prediction and prevention of terrorist threats. Leveraging machine learning technologies like image processing, facial recognition, anomaly detection, predictive analytics, and social media monitoring is vital for advancing counterterrorism measures.

These technologies utilize data uniquely; for instance, image processing and facial recognition help identify individuals from visual data, while anomaly detection spots unusual patterns that may signal security threats. Predictive analytics uses historical data to forecast future events, and social media monitoring proactively detects threatening communications. However, these technologies are often viewed skeptically, seen as potentially dystopian and invasive, raising concerns about privacy invasion, discrimination, and accidental harm. There's a pressing need to establish clear norms for AI usage in security. Effective deployment of AI in counterterrorism requires not just data collection but also ethical data management, prioritizing privacy, and data security to ensure technological advancements benefit society while respecting individual rights. Balancing security enhancements with the protection of freedoms presents a significant challenge, demanding a nuanced approach to the use of AI in counterterrorism, considering ethical dilemmas, technical reliability, and the risk of errors. Transparent, regulated, and ethical application of AI tools is essential for preventing terrorism while safeguarding individual liberties and rights. The integration of AI into counterterrorism strategies represents a significant step forward in enhancing security measures and predictive capabilities. Nevertheless, navigating the ethical considerations and technical challenges associated with its use remains an ongoing endeavor, with the most profound impacts and solutions yet to come.

[18] "New technologies, artificial intelligence aid fight against global terrorism," United Nations, retrieved from https://news.un.org/en/story/2019/09/1045562.

[19] "'Whoever leads in AI will rule the world': Putin to Russian children on Knowledge Day," RT, (September 1, 2017), retrieved from https://www.rt.com/news/401731-ai-rule-world-putin/. .

[20] Michael C. Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," retrieved from https://tnsr.org/2018/05/artificial-intelligence-international-competition-and-the-balance-of-power/

[21] "National Artificial Intelligence Research and Development Strategic Plan 2023," retrieved from https://www.whitehouse.gov/wp-content/uploads/202

The conclusions and recommendations of any SETA Foundation publication are solely those of its author(s), and do not reflect the views of the Institution, its management, or its other scholars.