Chapter 5
The Role of Artificial Intelligence in Combating Terrorism:
Exploring Capabilities and Challenges in the Dark and Deep Web

Abderrahim Khoumich
University Ibn Tofail, Morocco

Mohamed Mliless
https://orcid.org/0000-0003-4153-2524
School of Arts and Huminaities, University Moulay Ismail, Morocco

Mohamed Achamrah
University Sultan Moulay Sliman, Morocco

ABSTRACT

Technology is evolving rapidly, leading to increasingly sophisticated terrorist threats that challenge global security. Efforts by states to mitigate these risks often fall short, as terrorists adapt their techniques, especially through new technologies like artificial intelligence (AI). Research in cybersecurity is essential for awareness and protection. Counterterrorism strategies must evolve to address advancements in technology and the complexities of the dark web, where terrorist activities proliferate. Effective monitoring and legislative measures are crucial for enhancing security and combating these emerging threats.

DOI: 10.4018/979-8-3373-0245-4.ch005

INTRODUCTION

Artificial intelligence offers potential and difficulties in the fight against terrorism, especially when it comes to the deep and dark web. New threats from organised and self-organised individuals or groups are joining the classic risks as terrorism activities move more and more into the internet. Therefore, improving knowledge of the new ways terrorists communicate is essential to counterterrorism initiatives (Ebner et al., 2022). The possibility of terrorists abusing AI is threatening. The way that terrorists exploit the Internet and cutting-edge technologies has created a new dynamic environment that counterterrorism will need to adjust to in order to defeat their tactics. The encrypted nature of social network conversations, for instance, makes intelligence collection extremely difficult. There are possible advantages to integrating artificial intelligence with counterterrorism initiatives, though.

Some progress has been achieved by integrating behavioural cues and language processing (Thorley and Saltman, 2023). Although socio-semantic network analysis has shown promise in identifying individuals who inspire violence in radical networks (Bérubé et al., 2023), it is not always possible to derive a social network for study. As we will explore, evaluating anonymous and dispersed communications platforms requires linguistic research exclusively, as there are no social network structures to examine.

However, before pursuing any action, Leveraging AI's potential requires understanding both terrorism and AI's function. Understanding the roots of terrorism may orient Intelligence services to effectively use AI in surveillance and monitoring systems, predictive analytics and threat assessment, and data analysis and pattern recognition. Through social networks, forums, and markets on the dark web, these capabilities could prominently improve the battle against terrorism.

By analysing citizen big data, artificial intelligence techniques are essential for anticipating terrorist attacks (Kathleen, August 2019). However, they also present human rights issues and practical application challenges that raise concerns about the limitations of their predictive uses in counterterrorism and the implications of opportunities and risks (Kathleen, August 2019).

Notwithstanding its potential, applying AI to counterterrorism presents many difficulties. Significant challenges include privacy and security hazards, legal and ethical issues, adversarial attacks, and false information (McKendrick, 2019). To make matters even more complicated, terrorist operations find refuge on the deep and dark web. AI solutions for monitoring the dark and deep web include web scraping and crawling technologies, natural language processing for text analysis, as well as image and video recognition for content detection. However, challenges in monitoring the dark and deep web, such as anonymity and encryption technologies, volume and velocity of data, and deception and disinformation tactics, must be addressed.