Utilizing Artificial Intelligence in Combating Terrorism
Monitoring, Analysis and Prediction Technologies as a Model

Dr. Imran Awan

Expert on counter-terrorism and Professor of Criminology at Birmingham City University, UK

Artificial Intelligence (AI) is characterized by its sophistication and profound influence on several aspects of our daily lives. It is marked by a tremendous number of features that gives it a competitive edge over several entities according to their purposes or how they are leveraged. It can be abused by terrorists to serve their interests and achieve their criminal goals. It is also used by security and law enforcement agencies, such as the police, to predict and preemptively foil potential terrorist attacks.

Several companies, including Microsoft, Google, Yahoo, Amazon, banks, and credit card issuers, are now using AI for developing their own security systems. AI is also utilized to improve performance and decision-making in many organizations, as AI's predictive technologies aid in the fight against terrorist threats. They can be used to determine patterns, monitor them, and make predictions that can be utilized to design effective counter-strategies .

AI has created a virtual model where people engage via various state-of-the-art means of communication. Such a convergence contributed to the emergence of heightened security threats on a daily basis, which emphasizes the need to seek intelligent solutions to better understand complex societal issues. Perhaps AI can be regarded as a subsidiary means to decipher the linguistic communication between those individuals.

Modern technology can be used to intercept terrorist communications by recording, analysing, and framing them using «speech recognition» programmes. Despite the fact that Nuance Communications has collected millions of «speech» samples to be used swiftly by such apps, the ability to effectively reproduce such messages and communications using AI is a hurdle. However, there are certain advantages, such as the ability to pick single words or phrases in word command programmes .

As terrorists will attempt to leverage such technologies too, AI has posed a major risk threatening the safety and security of society throughout history. A recent study found that some terrorist organizations have found what they seek in modern technologies and AI tools. They use them either for establishing secure and fast communications among their members or with potential recruits, for camouflage and getting away from security tracking, for the polarization and recruitment of new followers and arms acquisition, or for facilitating their criminal operations by relying on technology virtually or on the ground .

Terrorist Threats

Emerging terrorist threats relying on AI have been changing rapidly as Sheldon and Wright put it in their Policing and Technology; "cyber-security has become a national security issue" that needs to be addressed. This necessitates incorporating AI in the fight against terrorist threats .

Modern technologies of all kinds have a major role in combating terrorist organizations and exposing their operatives. At the same time, privacy and human rights must be protected, which also require addressing them. Prosecutions should not be a random chaos among all people, as technology may be a double-edged weapon.

One cannot argue that any security system is entirely invulnerable to cyberattacks, not least when a terrorist organization manages to install malware to remotely control hacked computers and connect them later creating botnet networks. Terrorist organizations also recruit individuals willing to commit any atrocities that serve their criminal agendas. They use different patterns and methods, utilizing AI technologies to amplify the impact of their propaganda and polarize and recruit vulnerable individuals, turning them into extremists .

Highly accurate and sophisticated information analysis using AI technology online must be used effectively by the respective authorities to integrate all types of available data, ranging from online conversations on social networking sites to police records of suspected terrorists and biometric databases (recognition systems that automatically identify people). As a result, it is important that multiple agencies work together to stop and arrest terrorists using AI technologies. To combat the global terrorist network, international collaboration and laws must be strengthened .

It is also necessary to enhance technologies designed to coordinate preemptive domestic and global responses. Partnerships between the public and private sectors

are a potential model for using AI in countering terrorist threats. Private organizations will pay for internet surveillance and "raw" data analysis, while people will pay for the arrest and prosecution of terrorists who use their services .

Fight and Prevention

There are several preemptive tactics that can be used to fight terrorism using AI apps in covert counter-terrorism operations, as terrorists pose a serious threat given how increasingly advanced they are in using the internet and modern technologies as evident in the manner of their activities .

Contemporary tools for knowledge management in organizations offer diverse practical strategies to address the growing potential threats posed by terrorism through the application of artificial intelligence (AI). Effectively combating terrorism with these modern technologies necessitates a comprehensive grasp of the data cycle, information gathering, and distribution methods, alongside maintaining open communication with societies at every level. Relevant authorities should collaborate to deploy advanced knowledge-management systems and strengthen partnerships for the exchange of logistical information. Additionally, it is essential to recognize that the use of AI applications in countering terrorism can bolster collective security decision-making, thereby thwarting terrorist groups through collaborative and proactive measures.

The European Police Union, Europol, and Interpol are prime examples of intelligence exchange via AI. The organizational structures of security agencies specialized in combating terrorists work coherently, highlighting the importance of interconnected systems to gather data, analyze information and use AI effectively .

Investigations entailing lengthy formal procedures are likely to fail. Thus, European police services managed to develop new strategies to combat terrorist threats utilizing AI, thanks to information technology. This comprises community policing, an uncompromising policing, an intelligence-led policing (ILP), and a problem-oriented policing (POP) .

Many governments have invested heavily in Infrastructure in Information and Communication Technologies (ICT), recognizing the threat posed by cyber-terrorism. Currently, a more holistic approach is needed to develop laws, protocols and strategies to approach the huge development of technology in the context of addressing the challenges associated with artificial intelligence and terrorism, as well as to introduce

agreed definitions to replace the ambiguous language used in the current European agreements.

In addressing AI and terrorism, the idea of interacting with local communities to provide information and data to be applied at multiple levels must be reaffirmed. This approach focuses on the citizen as well as on using knowledge management and intelligence policing to their maximum potential to meet the demands of society in the fight against terrorism.

Mutual Cooperation

The development of ICT and AI highlights the relevance of joint cooperation between several agencies to employ these technologies to combat the spectre of terrorism. It is necessary to develop effective counter-terrorism programs and to start exchanging information—correct, real-time information—between security and law enforcement agencies and military bodies via AI programs. Moreover, the root causes of this issue should be addressed through proactive counter-terrorism strategies. Thus, enhancing security cooperation and community cohesion is essential for counter-strategies to effectively dissuade terrorists from committing these heinous crimes. Inter-agency communications are also urgent at large so that security services work together in a coordinated and effective manner within or outside national borders.

AI-powered virtual networks are capable of enhancing social interaction, building relationships, and providing support systems to transform into a community that leverages social capital. But in order to understand terrorism-related AI, governments need to develop practical strategies to counter such an imminent threat, with coordinated, comprehensive, flexible and rapid action that addresses preventive responses on local and global levels. There are existing policing and analytical models that may be useful when applied within recognized and approved frameworks that can counter terrorist organizations using AI .

Without a doubt, artificial intelligence (AI) combines the will and capacity to share information and intelligence across multiple agencies that must collaborate in a positive and successful security alliance to end terrorism and apprehend terrorists. In order to tackle this criminal behaviour, more international collaboration and legislation are urgently needed. In the context of «globalisation» and the current era of network systems, this is especially true given the mounting risks from terrorists, criminal gangs, hackers, and hostile countries who aim to damage critical infrastructure and internet

services. This is on top of the dangers presented by AI-powered terrorism, which has the potential to further inflame prejudice and alienate some cultures.

Conclusion

Artificial Intelligence paves the way for terrorist groups to carry out their diabolical plans. With the increasing spread of AI applications and the unprecedented development of innovative technologies, it is likely that these groups will look for further ways to employ and exploit new technologies in their terrorist agendas. Therefore, it is necessary to address such a phenomenon through modern policing methods, help counter terrorist threats, and harness the available modern technologies to thwart emerging threats .

As David Lyon argues in his Surveillance Studies, "Questions of risk and trust of security and opportunity are central". Thus, it is important to leverage new technologies to stay ahead of terrorists. There should also be a global agreement on what data is to be collected via AI, when it should be shared, and with whom, not only to fight terrorism, but also to protect our personal freedoms and identities.