RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 124 – 26 August 2024

The Use of AI in Terrorism

By Asha Hemrajani

SYNOPSIS

Artificial Intelligence (AI) is changing the way intelligence is gathered and used, affecting geopolitical tensions and terrorism. It has been reported that terrorist and violent extremist actors are leveraging AI to enhance their operations in three ways: boosting information operations, recruitment and financing. The potential for AI to be weaponised and misused in terrorism is rapidly becoming realised. Proactive policies and multistakeholder initiatives will be needed to monitor and counter these AI-enhanced terrorist operations.

COMMENTARY

In a speech to the Australian National Press Club in April, Mike Burgess, Director-General of the Australian Security Intelligence Organisation (ASIO), warned that "AI is likely to make radicalisation easier and faster". His assessment is shared by other Intelligence chiefs who are similarly concerned about "terrorists exploiting the enormous potential of the technology [AI]".

The key driver for this is that the barriers to leveraging AI tools, such as cost, training, and coding skills, have been reduced as they become more widely accessible and do not require significant resources or technical skills. Terrorist groups will likely incorporate more AI into their operations.

AI can potentially change terrorism operations in three fundamental ways: (a) boosting Information Operations (IO), (b) recruitment, and (c) financing.

Information Operations

AI platforms can play a clear role in shaping and enhancing IO. Last year, *Tech Against Terrorism*, an initiative launched by the United Nations to work on terrorism

threat intelligence and policy, reported that terrorist and violent extremist actors (TVEs) have already started using Generative AI tools to enhance their existing methods of producing and spreading propaganda, distorting narratives and influencing public opinion, as part of their IO.

Deepfakes are one type of synthetic media output from Generative AI tools. They can resemble certain persons, objects or events and appear genuine. Deepfakes are becoming more widespread and difficult to tell apart from genuine content, thus facilitating unlawful and dangerous activities. For example, a media organisation associated with Al-Qaeda had been disseminating misinformation and propaganda that appeared to have been produced using deepfakes.

These images have been made into posters overlaid with propaganda messages. The analysts believed it was likely that the images were generated with free tools to avoid the risks of identification associated with paid tools. It is also likely the images were originally generated without the propaganda messages overlaid, thereby avoiding violations of content moderation rules.

In February 2024, another study examined 286 pieces of AI-generated/enhanced content created or shared by pro-Islamic State (IS) accounts across four major social media platforms. The most common imagery in the AI-generated material were IS flags and guns. AI allowed the supporters to generate creatively and efficiently and even bypass filters on Instagram and Facebook by blurring the IS flag or placing a sticker on top.

The above examples suggest that TVE operatives have become adept at circumventing content creation restrictions in AI-enabled image generation tools. They have also developed a high level of skill in bypassing content moderation controls on social media platforms. This strongly suggests that the current guardrails on both AI-enabled image generation tools as well as social media platforms need to be strengthened.

Recruitment

Terrorists could use AI-based tools to profile candidates and identify potential recruits who meet their criteria. Subsequently, generative AI tools could be used to personalise and tailor messaging and media content for potential recruits. A UN study reported that concerns have been raised about OpenAI's tools in terms of their capabilities in "micro-profiling and micro-targeting, generating automatic text for recruitment purposes".

The same study found that AI might be used in the data mining process to identify individuals susceptible to radicalisation, enabling the precise dissemination of terrorist information or messaging. For example, they may send tailored messages to potential recruits, such as those who often seek "violent content online or streamed films portraying alienated and angry antiheroes" via AI-powered chatbots. This was demonstrated in an experiment when the UK's terrorism legislation reviewer was "recruited" by a chatbot.

Financing

Countering Financing of Terrorism (CFT) mechanisms trace how finance flows from the source, legally or illegally, to terrorists. These involve multiple stakeholders and include programmes against money laundering. Know Your Customer (KYC) is one standard technique financial institutions deploy to combat money laundering, especially when a bank account is opened online.

Some banks require the account holder to be present during a live video call where his "liveness" is verified. It is possible to spoof these KYC processes with deepfake videos, allowing terrorists to open fake accounts to facilitate funding for their activities.

The use of deepfakes in biometric KYC verification is particularly worrying. A report by *sensity.ai*, a fraud detection company, studied the most popular biometric verification vendors and found that "the vast majority were severely vulnerable to deepfake attacks". Terrorists can, therefore, leverage AI-generated deepfakes to bypass security checks inherent in KYC platforms, evade CFT mechanisms and thus illegally transfer funds.

Just as audio deepfakes have been used for commercial fraud, they can also be leveraged by terrorists to transfer funds illegally. These recordings can deceive people into parting with money or sensitive information as certain banks utilise voice authorisation checks for security purposes. Audio deepfakes could be used to bypass KYC checks and illegally transfer funds by synthesising a voice that closely resembles that of the authorised user.

Cryptocurrencies are another source of terrorist financing. In 2022, Bloomberg reported that a UN counter-terrorism legal expert had opined that "more cases of crypto use in terror-financing are being detected amid stepped-up scrutiny of such practices".

Cryptocurrencies were suspected to have been used in financing the 2015 Paris and 2019 Sri Lankan bombings. Following the 7 October attack on Israel, the US Treasury Department imposed sanctions on a virtual currency exchange in Gaza suspected of facilitating the Hamas attack. In February 2024, the crypto exchange Binance, whose CEO is a Singaporean, was sued by the families of the victims of the attack for allegedly "facilitating terrorism".

AI can potentially enable terrorists to take further advantage of cryptocurrencies in two ways: trading and theft.

AI-powered cryptocurrency bots can detect patterns and price trends to "offer predictions on target and breakout prices, alongside confidence levels, thus significantly enhancing decision-making processes", which is especially useful for markets with high volatility. Terrorists can leverage this ability to make more lucrative cryptocurrency trades, increasing their profits.

The second way is the outright theft of cryptocurrencies. Global cryptocurrency thefts have surged more than 100 per cent in the first half of 2024 as compared to 2023, partly caused by major attacks. This includes a US$308 million loss at a Japanese

crypto exchange due to a cybersecurity vulnerability. Given the growing trend of using AI to craft and launch cyberattacks, it is foreseeable that terrorists will use AI to "facilitate the theft of cryptocurrencies from 'hot wallets'" as reported by the UN.

Conclusion

The potential for AI to be weaponised and misused in terrorist activities is fast being realised. It is becoming another tool in the terrorism toolbox to run their IO, recruitment, and financing operations.

Policymakers, lawmakers, law enforcement agencies, and civil society must collaborate closely to develop robust strategies to counter terrorist entities' misuse of AI.

Greater vigilance and an array of mechanisms such as multistakeholder initiatives, legislation, policies such as better guardrails on social media platforms and AI-enabled content generation tools as well as the use of automated detection tools will be needed to monitor and contain these AI-enhanced terrorist operations.

Asha Hemrajani is a Senior Fellow at the Centre of Excellence for National Security (CENS) at S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
T: +65 6790 6982 | E: rsispublications@ntu.edu.sg | W: www.rsis.edu.sg