ID 003

Islamic State Exploitation of Emerging Web3 and Generative AI Technologies

RMTGP Rathnayaka[1#]

[1]Sri Lanka Army

[#]wadogayan@gmail.com

Islamic State, being a nefarious global terrorist organization, has showcased its exploitation and adaptability of various online technologies throughout the history. This research investigates its evolving Web3 and Generative AI exploitation tactics by using exploratory qualitative content analysis of discussions on IS friendly communication platforms, websites and online whistle-blowers then triangulated with recognized secondary resources. Pro-IS online entities demonstrate a concerning ability and interest to adapt and exploit emerging technologies like Web3 technologies (including decentralized communication, hosting, finance, and Metaverse) and Artificial Intelligence (including AI-generated videos, voice cloning, AI images and chatbots) for experimenting new tactics for propaganda, recruitment, and fundraising by evading extreme counter terrorism content moderation and detection mechanisms. It was observed that decentralized chat platforms and cryptocurrency are widely used by pro-IS entities while exploitation of decentralized web and virtual platforms were also susceptible for exploitation. There is a wide use of AI generated images, and textual contents. Exploiting AI audio-visuals and AI chatbots are still on experimental phase but possess an alarming threat. The global threat implied by these exploitations cannot be negated hence early counter terrorism actions must be taken to mitigate this emerging threats. These findings highlight the urgent need for a multi-stakeholder approach to counter this threat. Collaboration between tech companies, governments, counterterrorism agencies and international organizations is crucial to keep emerging online technologies to be safe from terrorist exploitations.

Keywords: *Web3, Generative AI, Islamic State*