Tanja MILOSHEVSKA

UDK: 343.341:004.8(100)
Review article

THE POTENTIAL EXPLOITATION OF GENERATIVE ARTIFICAL INTELLIGENCE BY TERRORISTS AND VIOLENT EXTREMISTS

Abstract:

This paper will analyze how and to what extent terrorists and violent extremists have interacted with generative artificial intelligence so far and identify potential ways in which they could misuse generative AI in the future. It is therefore necessary to question assumptions that terrorist and violent extremist actors will quickly adopt generative AI solely based on an assessment of the capabilities it may offer. Although research has shown that technological capability and availability are key drivers of terrorist innovation, terrorist and violent extremist actors also assess any new technology on its compatibility (with both their modus operandi and ideology), relative complexity, cost, and the context in which they are operating. Understanding these factors, both in isolation and in relation to one another, will be a key aspect in monitoring the extent to which terrorists and violent extremists adopt generative AI tools. In doing so, the paper will seek to identify a likely trajectory for the abuse of this technology by terrorist actors as well as conclude with some initial recommendations for policymakers.

Keywords: *generative artificial intelligence, terrorists, violent extremists, propaganda.*

Introduction

With the arrival and rapid adoption of sophisticated deep-learning models such as ChatGPT, there is growing concern that terrorists and violent extremists could use these tools to enhance their operations online and in the real world. Large language models have the potential to enable terrorists to learn, plan, and propagate their activities with greater efficiency, accuracy, and impact than ever before. As such, there is a significant need to research the security implications of these deep-learning models. Findings from this research will prove integral to the development of effective countermeasures to prevent and detect the misuse and abuse of these platforms by terrorists and violent extremists. Specifically, is analyzed the potential implications of commands that can be input into these systems that effectively 'jailbreak' the model, allowing it to remove many of its standards and policies that prevent the base model from providing extremist, illegal, or unethical content. Using multiple accounts, the paper explored the different ways that extremists could potentially utilize different large language models to support their efforts in training, conducting operational planning, and developing propaganda. The article discusses the potential implications and suggests recommendations for policymakers to address these issues.

Terminology

Generative AI (GenAI) is a type of Artificial Intelligence (AI) that can create a wide variety of data, such as images, videos, audio, text, and 3D models." (generativeai.net). It does this by learning patterns from existing data, then uses this knowledge to generate new and unique outputs: "GenAI can produce highly realistic and complex content that mimics human creativity, making it a valuable tool for many industries such as gaming, entertainment, and product design." (Goaltide, 2023).

The GenAI industry is developing rapidly, and foundation models (such as Large Language Models, or LLMs) are being adopted across nearly all industries. Text Generation involves using generative AI learning models to generate new text based on patterns learned from existing text data. One of these new applications is ChatGPT. ChatGPT is a text-generating chatbot developed by OpenAI and released in November 2022.

This remarkable application can be used for malicious purposes, too, for example, by terrorists and violent extremists.

The **metaverse** presents an immersion of the physical and virtual worlds in the digital sphere, using 3D technologies and online communication devices like computers and smartphones, allowing people to have real-time interactions and experiences across long distances.

The phrase **violent extremism** is used in contexts when extremist worldviews are accompanied by the justification and use of extreme violence (such as

atrocity crimes) against those who do not share the same belief or ideology. Violent extremism may be expressed by individuals or groups through speeches or media posts, by carrying out isolated acts of violence in the name of extremist ideologies, or by physically joining violent groups (Aroua, 2018).

Terrorism definitions vary across different national jurisdictions, and there is no universally agreed definition of terrorism. For the purposes of this paper, is chosen to use the shortened version of Schmid's (2011) academic consensus definition, where terrorism is defined as:

"1. Terrorism refers, on the one hand, to a doctrine about the presumed effectiveness of a special form or tactic of fear-generating, coercive political violence and, on the other hand, to a conspiratorial practice of calculated, demonstrative, direct violent action without legal or moral restraints, targeting mainly civilians and non-combatants, performed for its propagandistic and psychological effects on various audiences and conflict parties;

2. Terrorism as a tactic is employed in three main contexts:

(i) illegal state repression;

(ii) propagandistic agitation by non-state actors in times of peace or outside zones of conflict; and

(iii) as an illicit tactic of irregular warfare employed by state- and non-state actors."

Potential misuse of generative AI platforms

The potential exploitation of generative AI by terrorists and violent extremists has attracted its own share of warnings, including that chatbots could be used to groom or radicalize young people (Taher, 2023) or increase the risk of bioterrorism (Sandbrink, 2023).

Already in 2020, Kris McGuffie and Alex Newhouse (2020) highlighted the potential for abuse of generative language models by assessing GPT-3. Experimenting with prompts representative of different types of extremist contents, they revealed significant risk for large-scale online radicalization and recruitment. In April 2023, the EUROPOL Innovation Lab issued a report that presented some of the ways in which LLMs such as ChatGPT can be used to commit or facilitate crime, including impersonation, social engineering attacks, and the production of malicious code that can be used in cybercrime. LLMs like ChatGPT have the potential to significantly improve the performance of chatbots, moving them away from pre-scripted, rules-based responses and increasing their human-like qualities. This has led to discussion regarding the potential for the creation of a "terrorist GPT," a customized chatbot that could encourage individuals down the pathway to radicalization.

Governmental bodies have also raised concerns about the potential misuses of generative AI platforms, with an Australian eSafety Commissioner report published in August 2023 noting the many ways that terrorists or other

violent extremists could leverage this technology (eSafety Commissioner, 2023). In that report, they raised concerns that terrorists "could potentially use these models for financing terrorism and to commit fraud and cyber crime;" additionally, these models could allow "extremists to create targeted propaganda, radicalise and target specific individuals for recruitment, and to incite violence." (eSafety Commissioner, 2023).

In early November 2023, a report by Tech Against Terrorism, an initiative backed by the United Nations'Counter-Terrorism Committee Executive Directorate (CTED), concluded that there was relatively little evidence of generative AI being systematically exploited by terrorist and violent extremists, defining their engagement with the technology as "in its experimental phase." Despite the fairly small data set, the examples in the report are illustrative of the most obvious use of generative AI for terrorists and violent extremists — the production of propaganda. They include AI-generated posters produced by an al-Qaeda-aligned media entity, AI-generated images and memes on a far-right Telegram channel, and the transcription of an Islamic State propaganda message from Arabic speech into Arabic, Indonesian, and English text by an ISIS supporter.

Terrorists and violent extremists have proven to be remarkably adaptable in leveraging online platforms to further their goals (Weimann, 2005, 2015). From the advent of extremist websites in the late 1990s, to new social media platforms such as Facebook, YouTube, Twitter, Instagram, and TikTok, these groups have quickly adopted and exploited new developments in cyberspace. More recently, they have also begun embracing encrypted messaging apps, such as Telegram, TikTok, and TamTam. They utilize anonymous cloud storage platforms, and even the Dark Net, highlighting their continued attempts to leverage the most recent advancements and evolutions in the digital world. "For their part, many terrorists have changed their mode of operations, adopting these new technologies and implementing various operational security measures designed to avoid or defeat sophisticated intelligence collection operations." (Wagner, 2007). For terrorists, these technologies offer the ability to communicate and coordinate worldwide operations with reasonable expectations of privacy and security. AI has been able to exploit newer technologies for individuals and groups, making the threat of cyberattacks and espionage more pervasive than ever before (Esmailzadeh, 2023). It has the potential to be both a tool and a threat in the context of terrorist and extremist groups.

The notion of AI and terrorism has mostly focused on the potential uses of AI for counterterrorism or countering violent extremism (McKendrick, 2019). In 2021, the United Nations Office of Counter-Terrorism (2021) released a special report reviewing prospects offered by AI to fight online terrorism. Indeed, several studies have focused on the use of AI in counterterrorism (Verhelst, at all, 2020). Yet, very little attention has been devoted to exploring the other side: how terrorists and violent extremists can use AI-based technologies to spread hate, propaganda, and influence vulnerable individuals toward their ideologies.

Recently, the Global Internet Forum to Counter Terrorism (GIFCT) released a report about the threats posed by extremist/terrorist use of GenAI (GIFCT Red Team Working Group, 2023). The potential uses of AI by extremist groups include:

- ✓ Propaganda: AI can be used to generate and distribute propaganda content faster and more efficiently than ever before. This can be used for recruitment purposes or to spread hate speech and radical ideologies. AI-powered bots can also amplify this content, making it harder to detect and respond to.
- ✓ Interactive recruitment: AI-powered chatbots can interact with potential recruits by providing them with tailored information based on their interests and beliefs, thereby making the extremist group's messages seem more relevant to them.
- ✓ Automated attacks: Terrorists can use AI to carry out attacks more efficiently and effectively—for example, by using drones or other autonomous vehicles.
- ✓ Social media exploitation: AI can also be used to manipulate social media and other digital platforms to spread propaganda and recruit followers.
- ✓ Cyber-attacks: AI can be used by extremist groups to enhance their ability to launch cyber-attacks against targets, potentially causing significant damage.

Indoctrination and Recruitment

Online recruitment and engagement are trademarks of modern extremism. The metaverse risks expanding this capability by making it easier for individuals to socialise and congregate (Elson at all, 2022).

Much of the analysis so far has focused on how generative AI could assist in the creation and dissemination of terrorist and violent extremist propaganda. Most notably, generative AI allows for the creation of new images or the adaptation of existing ones on a scale and at a speed that was not previously possible. Similarly, actors can now use such tools to generate synthetic video and audio, including deepfakes of known or notable individuals. Although the reliability and quality of video production has typically been inconsistent, the February 2024 launch of OpenAI's Sora which can generate videos based on text prompts, points to the rapid speed at which this technology is developing (Montgomery, 2024).

Finally, a variety of ever-improving LLMs can create text using different styles, formats, and, most relevantly, languages. Previously, terrorist groups had to rely on manual (and often relatively poor) translations of propaganda material, and this process was heavily reliant on the skills of a handful of individuals. Generative AI can theoretically be used to create and transcribe video

and audio propaganda, or generate text-based propaganda, near-instantaneously and in multiple languages.

In combination, these developments create the potential for an increase in the volume and quality of terrorist or violent extremist propaganda material.

Currently, tech companies can share the "digital fingerprint" or "hash" of terrorist content with each other, enabling its timely removal and/or preventing it from being uploaded at the source (GIFCT's Hash-Sharing Database, 2023). The use of generative AI to manipulate imagery could change this digital hash without substantively altering the file, effectively "destroying hash-sharing as a solution." (Gilbert, 2023). Although major platforms can identify and remove terrorist content in other ways — including the use of Natural Language Processing to identify new content that is similar, but not identical to, existing terrorist content (United Nations Office of Counter-Terrorism and United Nations Interregional Crime and Justice Research Institute, 2021)—hash-sharing has been central to cross-platform efforts to counter terrorist content since 2016 (Meta, 2016). Its potential degrading as a solution has been described as a "massive risk." (Gilbert, 2023).

It is important to emphasize that creating terrorist content is just the first part of a process. Terrorist actors also need to find a way to reliably store and share content online. Thanks to a combination of regulation, disruptive action, and public-private partnerships, this is currently difficult to do across most major platforms, with terrorist actors instead relying on a patchwork of smaller, less regulated options (Wells, 2022). Crucially however, generative AI offers terrorist actors the potential ability to optimize their evasion of major platform counter-measures, in particular the use of so-called hash-sharing.

How can the metaverse be exploited by violent extremists and violent extremist organizations?

The metaverse may become a new territory for terrorist activity, a promising platform to improve and advance their online activities, including radicalisation, recruitment, training, fundraising and the coordination of attacks (Debuire, 2022).

Combining artificial intelligence with augmented reality within the metaverse will allow extremist leaders to convene and meet with their supporters, develop and sustain virtual idealistic societies, and increase their spheres of influence. Because of the extreme emotional environment made possible by the metaverse, it may be challenging for some individuals to differentiate between real life and virtual reality (Council of the European Union, 2022). Some users may consider that what takes place in the metaverse is not factual even if it has real consequences for their lives. By blending artificial intelligence and augmented reality in the metaverse, online recruiters for terrorist or violent extremist groups will be able to meet in a virtual room with potential followers and entice them with visions of the future.

First, the metaverse will provide extremists with a unique environment to recruit new members as they can create their own private servers, reach a wider audience, and simulate in-person recruitment networks. These servers will be onerous to moderate, and the current regulatory guidelines and technological mechanisms do not sufficiently prevent the production of nefarious content and behaviors. As a result, the metaverse will serve as an ideal incubator for extremist recruitment.

Second, the metaverse will simplify fundraising and cybercrime for violent extremists. Through the usage of cryptocurrency, cybercrime, and money laundering, the metaverse will provide added layers of anonymity and prevent potential detection from law enforcement and financial institutions.

Third, the metaverse affords extremists the ability to do the majority of their pre-attack planning and intelligence gathering virtually. By limiting the number of times they must visit a potential target and minimizing the time spent online conducting open-source intelligence, violent extremists will be able to operate discreetly while still maintaining a high level of efficiency. Additionally, should they gain access to the servers used by law enforcement to conduct their own virtual trainings, violent extremists will have the opportunity to develop more effective attack and contingency plans.

Finally, as metaverse technology becomes more realistic, extremists can practice creating and handling explosives, weapons, and conducting attack simulations with a variety of potential disruptions or variable changes and establish methods of best practice to still achieve their key objectives (Levin, 2024).

Virtual Training-Pre-Attack Planning

One aspect violent extremist may utilize the metaverse for is expanding their pre-attack planning capabilities. Under our traditional understanding of pre-attack activities, individuals planning to commit acts of violent extremism develop a variety of different behaviors to plan their attacks. In a report published by the Office of the Director of National Intelligence's Joint Counterterrorism Assessment Team, their researchers identified a recurrent attack planning cycle. According to the report, violent extremists generally plan attacks in observable stages, although specific details, sequencing, and timing can vary greatly and change over time. In addition, they noted that certain activities are easier to spot than others. Pre-attack surveillance, training, and rehearsals are often observable and can offer opportunities to identify plots and prevent attacks (ODNI, 2020). However, one major concern with the metaverse is that it may remove the need for violent extremists to conduct the majority of their pre-attack intelligence gathering in person. For example, should violent extremists become able to combine metaverse technology with other modern technologies such as CCTV, personal cameras, social media posts, and other livestream capabilities, they may never have to go in public to collect the intelligence they need to carry out attacks on specific targets or locations.

Another area of concern regarding violent extremist groups' pre-attack planning is their ability to use roleplay metaverse games and training tools already available for law enforcement and armed forces to counter potential issues during their attacks.

An example of the tools that are already available and could be modified for illicit purposes is AUGGMED (Automated Serious Game Scenario Generator for Mixed Reality Training). The aim of AUGGMED was to develop a serious game platform to enable single- and team-based training of end-users with different levels of expertise from different organizations responding to terrorist and organized crime threats. The platform automatically generates non-linear scenarios tailored to suit the needs of individual trainees with learning outcomes that improve the acquisition of emotional management, analytical thinking, problem solving and decision making skills. The game scenarios include advanced simulations of operational environments, agents, telecommunications and threats, and can be delivered through virtual reality and mixed reality environments with multimodal interfaces. In addition, the AUGGMED platform will include tools for trainers enabling them to set learning objectives, define scenarios, monitor training sessions, modify scenarios and provide feedback in real-time, as well as evaluate trainee performance and set training curricula for individual personnel in the post-training session phase (European Commission, 2022). Plus, once these virtual scenarios were created and ran without any technical issues, the cost of replicating and sharing the software with other agencies is minimal. This enables reusability and iteration at low cost (Herath & Jarnecki, 2022).

Extremists either join the service in order to gain combat and logistical training, or are recruited once their service ends by radical groups preying on the combination of trauma, loss of purpose and community that often affects veterans (Ware, 2023). In sum, access to former law enforcement, armed forces personnel, and their response protocol information would elevate the success of violent extremist pre-attack planning in the metaverse and their operational capabilities.

The final area of concern when it comes to violent extremists using the metaverse for pre-attack planning can already be demonstrated by online games such as Minecraft, Roblox, and Sandbox. Based on publicly available plans and layouts, online information and imagery, and other mapping technologies, users have been able to create a plethora of virtual recreations of real-life infrastructure within these platforms. As a result, violent extremists will likely have the ability to gather intelligence simply by creating, downloading, or interacting with these virtual recreations to record notes and identify any points of vulnerability in which they could exploit during an attack. This will be especially worrisome for government buildings, critical energy infrastructure, public venues, university campuses, sports stadiums, and any other locations that may become potential targets for violent extremism.

Attack Simulation

The final activity that is alarming and requires immediate attention is the enhanced ability for violent extremists to simulate attacks. As mentioned above, the military has harnessed the powers of virtual and augmented reality simulation for decades. Although the technological affordances of high-quality metaverse graphics are still in development, software companies are trying to create programs that are considered so realistic they will suspend one's disbelief that it's a simulation and trick their minds into thinking they are physically somewhere else. This will translate to software programs that will allow users to manipulate the complexities of life such as varying amounts of civilians, differing infrastructure and traffic patterns, altering terrain, and various weather conditions. An example of how this has already manifested within the American armed forces is the Synthetic Training Environment (STE), which was developed by the software company Bohemia Interactive Simulations, that creates high-fidelity simulations for soldiers to train anywhere in the world. This version of the metaverse is called One World Terrain and the software combines three-dimensional data collected from satellites, sensors or scanners and combines it with additional information to render high-fidelity terrain simulations. Furthermore, STE's digital world can be manipulated by artificial intelligence and machine learning to achieve specific training exercises and results (Easley, 2022).

Should violent extremists be able to gain access to these software programs, there is an infinite amount of plausible scenarios in which they manipulate the algorithms to the exact specifications of an upcoming attack and simulate their activities under hefty layers of anonymity.

The second key component of attack simulation within the metaverse that poses a heightened threat to public safety is their ability to practice with virtual weaponry and explosives. There is now an emerging alternative option where users would have access to similar levels of anonymity, only now it will be far more immersive than the Tor Network. Within metaverse servers, organized crime such as arms trafficking could take place with relative ease under the current lack of technological understanding, regulation, or oversight (INTERPOL, 2022). As it pertains to firearms testing and purchasing specifically, there are companies that have already built firearm-emulating controllers that pair with virtual reality headsets that are shockingly realistic. With this technology, metaverse users and violent extremists alike will be able to simulate the usage of any number of different firearms, test its efficiency in a number of simulated situations, and arrive at a decision in which one they prefer to use in real life.

The final activity and a critically important area of concern is how the Metaverse will enable violent extremists to rehearse their attacks. Once they have completed their pre-attack planning, gathered all the materials needed, the next step in the attack planning cycle is rehearsal. Violent extremists often rehearse the attack scenario to confirm planning assumptions, enhance tactics,

and practice escape routes. They may also trigger an incident at the target site to test the reaction of security personnel and first responders. While assessing the efficacy of their plans prior to the attack, violent extremists also seek to determine the conditions which favor the highest rate of success and lowest risk. Factors they commonly consider include the element of surprise, choice of time and place, use of diversionary tactics, and ways to impede response measures. Unless the violent extremist is planning a suicide attack, escape routes and contingency plans are also carefully planned (ODNI, 2020). Until recently these activities were most frequently carried out in person. However, with the addition of metaverse technology, violent extremists could have unparalleled rehearsal opportunities (Elson et al., 2022). For example, violent extremists can simulate a variety of potential disruptions or variable changes and establish methods of best practice to still achieve their key objectives. This will enable violent extremists to replicate law enforcement and civilian responses, learn viable and efficient paths, coordinate alternative routes if some become blocked, and establish multiple contingency plans should disruptions occur.

Conclusion

Terrorist and violent extremist groups and individuals have shown that they can adapt very well and have evolved considerably over the decades. They have demonstrated the potential to innovate, for instance, in their organizational structure, becoming decentralized, franchised and global.

The implications of this article indicate that the metaverse resembles Pandora's box; the emerging technology is far more complex than our current systems can handle, and the consequences could be devastating. The evolution of the adoption of AI by terrorist groups and individuals should be monitored.

Increased cooperation between the private and public sectors, between the academia, high-tech, and the security community, would increase awareness of the potential abuse of AI-based platforms by violent extremists, fostering the development of more sophisticated protections and countermeasures. The use of AI and related emerging technologies to counter AI-enabled terrorist threats should be explored, in particular to counter terrorist radicalization and spread positive narratives.

BIBLIOGRAPHY:

- All Things Generative AI," generativeai.net, n.d.
- Aroua, A. (2018). *Addressing Extremism and Violence. The Importance of Terminology*. Geneva: The Cordoba Foundation of Geneva. Available at: https://www.cordoue.ch/images/pdf/Papers/CFG_ConflictTransformationPerspective.pdf [Accessed 16 April 2022].
- "Considerations of the Impacts of Generative AI on Online Terrorism and Extremism. (2023). GIFCT Red Team Working Group.
- "GIFCT's Hash-Sharing Database," (2023). Global Internet Forum to Counter Terrorism. Available at: https://gifct.org/hsdb/.[Accessed 10 May 2024].
- ChatGPT. (2023). The impact of Large Language Models on Law Enforcement. The Hague: EUROPOL Innovation Lab.
- Council of the European Union. (2022). "The Metaverse in the Context of the Fight Against Terrorism", Special Report. Available at:https://data.consilium.europa .eu/ doc/document/ST-9292-2022-INIT/en/pdf. [Accessed 3 March 2024].
- Countering Terrorism Online With Artificial Intelligence: An Overview for Law Enforcement and Counter-Terrorism Agencies in South Asia and South-East Asia," United Nations Office of Counter-Terrorism and United Nations Interregional Crime and Justice Research Institute. (2021). Available at: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/countering-terrorism-online-with-ai-uncct-unicri-report-web.pdf. [Accessed 12 April 2024].
- Debuire, D. (2022) "Terror-ist use of the Metaverse: new opportunities and new challenges", *The Security Distillery*. Available at: https://thesecuritydistillery.org/all-articles/terrorism-and-the-metaverse-new-opportunities-and-new-challenges. [Accessed 5 April 2024].
- Early terrorist experimentation with generative artificial intelligence services. (2023). Tech Against Terrorism. Available at: https://techagainstterrorism.org/hubfs /Tech % 20Against%20Terrorism%20Briefing%20-%20 Early%20terrorist% 20 experi mentation%20with %20generative% 20artificial% 20intelligence%20services.pdf. [Accessed 5 April 2024].
- Easley, M. (2022). "How Interconnected, Simulated Worlds Could Transform Military Training." *NDIA Business & Technology Magazine*. Available at: www.nationaldefensemagazine.org/articles/2022/11/23/how-interconnected-simulated-worlds-could-transform-military-training. [Accessed 5 May 2024].

- Elson, J at all. (2022). "The metaverse offers a future full of potential – for terrorists and extremists", *The Conversation*. Available at: https://theconversation.com/the-metaverse-offers-a-future-full-of-potential-for-terrorists-and-extremists-too-173622. [Accessed 5 April 2024].
- Esmailzadeh, Y. (2023). "Potential Risks of ChatGPT: Implications for Counterterrorism and International Security," *International Journal of Multicultural and Multireligious Understanding* 10:4.
- European Commission. (2022). "Automated Serious Game Scenario Generator for Mixed Reality Training." *CORDIS*. Available at: https://cordis.europa.eu /project/ id /653590. [Accessed 5 April 2024].
- Gilbert, D (2023). "Here's How Violent Extremists Are Exploiting Generative AI Tools," *Wired*. Available at: https://www.wired.com/story/generative-ai-terrorism-content/[Accessed 5 April 2024].
- Herath, C., Jarnecki, J. (2022). "Securing Future Realities: What Can We Expect from the Metaverse?" *RUSI,* Available at:https://rusi.org/explore-our-research/ publications /commentary/securing-future-realities-what-can-we-expect-metaverse. [Accessed 5 April 2024].
- INTERPOL. (2022). "INTERPOL launches first global police Metaverse.". Available at: https://www.interpol.int/en/News-and-Events/News/2022 / INTERPOL-launches-first-global-police-Metaverse. [Accessed 10 May 2024].
- Levin, J. (2024). Violent Extremists in the Metaverse*, Global Affairs Review*, The Center for Global Affairs, New York University. Available at: https:// wp.nyu.edu /schoolofprofessionalstudies-ga_review/violent-extremists-in-the-metaverse/. [Accessed 15 April 2024].
- McGuffie, K., Newhouse, A. (2020). "The Radicalization Risks of GPT-3 and Advanced Neural Language Models," available via Arxiv.
- McKendrick, K. (2019). "Artificial Intelligence Prediction and Counterterrorism," International Security Department, *Royal Institute of International Affairs*.
- Montgomery, B. (2024). "Sora: OpenAI launches tool that instantly creates video from text," *The Guardian*. Available at:https://www.theguardian.com /technology /2024 /feb/15/openai-sora-ai-model-video. [Accessed 19 April 2024].
- Partnering to Help Curb Spread of Terrorist Content," (2016). Meta. Available at: https://about.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content/.[Accessed 12 April 2024].
- Sandbrink. J. (2023). "ChatGPT could make bioterrorism horrifyingly easy," *Vox.* Available at: https://www.vox.com/future-perfect/23820331/

chatgpt-bioterrorism-bioweapons-artificial-inteligence-openai-terrorism. [Accessed 2 April 2024].

- Schmid, A (Ed.) (2011). *The Routledge Handbook of Terrorism Research*. London and New York: Routledge.
- Taher, A. (2023). "AI chatbots could be 'easily be programmed' to groom young men into launching terror attacks, warns top lawyer," *Daily Mail*. Available at: https://www.dailymail.co.uk/sciencetech/article-11952997/amp/AI-chatbots-easily-programmed-groom-young-men-terror-attacks-warns-lawyer.html?s=03 [Accessed 5 February 2024].
- Tech Trends Position Statement – Generative AI. (2023). eSafety Commissioner.
- US Office of the Director of National Intelligence (ODNI). (2020) "Counter-terrorism Guide for Public Safety Personnel." *JCAT*. Available at: https://www.dni.gov/nctc/jcat/index.html. [Accessed 5 April 2024].
- Verhelst, H.M. at all. (2020). "Machine Learning against Terrorism: How Big Data Collection and Analysis Influences the Privacy-Security Dilemma," *Science and Engineering Ethics* 26.
- Wagner, A. (2007). "Intelligence for Counter-Terrorism: Technology and Methods," *Journal of International Affairs* 2:2 (2007): pp. 48-61.
- Ware, J. (2023). "The Violent Far-Right Terrorist Threat to the U.S. Military." *Council on Foreign Relations*. Available at: https://www.cfr.org/blog/violent-far-right-terrorist-threat-us-military. [Accessed 5 April 2024].
- Weimann, G. (2005). *Terror on the Internet, The New Arena, the New Challenges*, Washington, D.C.: United States Institute of Peace Press.
- Weimann, G. (2015). *Terror in Cyberspace: The Next Generation*, New York: Columbia University Press.
- Wells, D. (2022). "Why outsourcing counter-terrorism online won't work in future," Lowy Institute. Available at: https://www.lowyinstitute.org/the-interpreter/why-outsourcing-counter-terrorism-online-won-t-work-future. [Accessed 5 April 2024].
- What is Generative AI?" Goaltide, February 21, 2023