KATARZYNA CZORNIK

AI AND GENAI AS TOOLS IN THE HANDS OF ISLAMIC TERRORIST ORGANISATIONS

Katarzyna Czornik
University of Silesia in Katowice, Faculty of Social Science, Institute of Political Science, Katowice, Poland
Email: katarzyna.czornik@us.edu.pl

Abstract: The paper demonstrates that AI, and currently GenAI, enable Islamic terrorist (jihadist) organisations to feel increasingly confident in the world of modern information and communication technologies. AI and GenAI have become highly effective tools in the hands of jihadist organisations, and their ease of use, wide and nearly unlimited availability combined with weak safeguards make them what can be described as intensifiers and catalysts of jihadism. GenAI provides a space for an almost revolutionary transformation of jihadist operations in terms of speed, efficiency and scale, while also allowing them to wage an effective "hallucinatory war". The use of AI and GenAI by jihadist organisations focuses on three main areas: 1) personalised propaganda and disinformation; 2) interactive, selective recruitment and radicalisation; 3) combat applications and use on the battlefield (autonomous vehicles and drones). In this context, the religious and philosophical perspective is crucial. A challenging and problematic issue is AI's alignment with societal values and Islamic teachings, and its potential use by jihadists.

Key words: Artificial Intelligence, generative Artificial Intelligence, new technologies, terrorism, jihadism, Islamic terrorist organisations, selective propaganda, "hallucinatory war".

1. Introduction. Methodological assumptions

Artificial intelligence (AI), and in particular generative artificial intelligence (GenAI), represents one of the most recent and innovative developments in information and communication technologies, enabling humanity to access a wide range of functions and services in a fast, convenient and efficient manner.

Broadly understood artificial intelligence cannot be viewed in binary terms. As a relatively new phenomenon, it has two dimensions. On the one hand, AI brings numerous benefits – it increases operational efficiency, automates tasks, supports decision-making and forecasting, enables the analysis of large data sets, and, in the case of GenAI, can even create reality. On the other hand, however, improper use of AI, or its exploitation by bad actors (such as terrorist organisations), can lead to serious disruptions in the functioning of societies and states, and thus to significant challenges to international security. These may include erroneous or manipulated individual and even group decisions, violations of privacy through data leaks, large-scale international fraud, as well as the coordination and facilitation of planning and carrying out terrorist attacks, the strengthening and expansion of cyberterrorism, the increased reach and effectiveness of cyber wars, or easier conversion to Islam and religious radicalisation through the creation of a distorted image of reality. In this context, the religious and philosophical perspective is crucial, as it examines AI's alignment with societal values and Islamic teachings. Certain Islamic principles may raise concerns when considering the current trajectory of AI development. These include issues related to autonomy and free will, privacy, bias and fairness, preservation of life, economic disparity, and transhumanism.

Nowadays, radical Islamic terrorist organisations, e.g., Al-Qaeda, the Islamic State, or Hezbollah, increasingly utilise new technological solutions across various aspects of their activities, particularly those based on artificial and generative intelligence. AI and generative AI are employed by these groups for internal communication, recruitment processes, as well as for planning, organising and ultimately carrying out terrorist attacks. AI can be and is used by Islamic terrorist organisations to create deepfakes (false videos and recordings), conduct targeted propaganda campaigns (e.g. based on age or gender), and engage in other forms of disinformation, which can lead to manipulation of public opinion, reputational damage, and even disruption of democratic processes. The emergence and use of broadly defined artificial intelligence thus represent a significant opportunity for terrorist organisations not only to expand the scope of their operations and increase the efficiency of achieving their

objectives, but also to infiltrate areas and domains which were previously inaccessible to them.

The research objective of this paper is therefore to demonstrate the various forms of use of AI and generative artificial intelligence by selected radical Islamic terrorist organisations, as well as to identify the dangers posed by these terrorist groups' utilisation of new technologies in the form of AI and generative AI. This article focuses on the complex and nuanced relationship between AI and Islamic ethics. It is important because the Muslim world is not just a passive observer but an active participant in the realm of AI and GenAI development and regulation. The Muslim world is actively involved in AI and GenAI development and regulation, contributing Islamic ethical and philosophical perspectives to global discourse. This involvement is multifaceted, encompassing the development of a moral framework, policy advocacy, and practical applications that align with Islamic values.

The research problem centres on the question of how (through which instruments) radical Islamic terrorist organisations utilise AI and generative AI in their activities, as well as how and to what extent these technologies facilitate their operations.

The research hypothesis states as follows: rapid democratisation of artificial intelligence and generative artificial intelligence enables Islamic terrorist organisations to exploit these technologies, increasingly implementing advanced, innovative and novel applications in their terrorist tactics. By utilising AI and generative AI across various aspects of their operations, Islamic terrorist organisations are becoming more and more active, effective and dangerous – especially from the Western perspective – non-state actors on the international stage. Artificial intelligence, and especially generative artificial intelligence, have emerged as some of the key determinants, instruments and tools used to intensify and expand the scope of hybrid threats, including radicalisation, jihadism (*qital*) and cyber-jihadism (Pratt 2006, 438-456).

The resolution of the above-mentioned research problem and the verification of the research hypothesis will be carried out using the following research methods: 1) factor analysis, aimed at identifying the areas (spheres/fields) of influence of the use of artificial intelligence and generative artificial intelligence in hybrid operations on international security; 2) causal analysis, intended to identify the reasons behind the increasingly intensive and expansive adoption of AI and generative AI tools by Islamic terrorist organisations, as well as to indicate the consequences of their use; 3) case study analysis of specific instances of AI utilisation by Islamic terrorist organisations; 4) content analysis involving the examination of available literature on the subject within the field under discussion.

The paper is divided into five parts. The introduction covers the background of the subject matter, highlighting the importance of the

phenomenon under study, as well as the methodological assumptions. Next, a theoretical approach is applied, as the second part presents the origins and definitional challenges of key scientific terms central to the text, such as artificial intelligence and generative artificial intelligence. The third part is dedicated to outlining specific areas (spheres) of AI and generative AI's influence on the intensification of the hybrid threat posed by jihadism. The penultimate section presents case studies of the use of artificial intelligence and generative artificial intelligence by radical Islamic terrorist organisations to promote ideology and conduct jihadist activities. The final, fifth part contains the conclusions drawn from the conducted research.

2. What is AI and Generative AI – Theoretical Approach

Artificial intelligence, as a scientific term, was coined by John McCarthy, an American computer scientist, who first employed it in 1956 during the Dartmouth AI Conference, in reference to intelligent machines designed in such a way that the outcomes of their operations would reflect the results of human thought processes (Sheikh and Prins and Schrijvers 2023, 15-41).

Since then, over the course of nearly seven decades, the concept of AI has undergone substantial evolution, shaped primarily by rapid scientific and technological progress (particularly in the fields of computer and engineering science) as well as by revolutionary developments in media and communication (Haenlein 2019, 1-9). In the scholarly literature, AI is therefore presented both as a domain of knowledge and as its artefacts, such as bots, including chatterbots, search bots, shopping bots, databots, updatebots and infobots, as well as various types of robots, including humanoid robots (Gaikwad 2018, 2305-2306).

The very term AI is exceptionally difficult to define, as it may be considered from multiple dimensions and at various levels. To date, no single, universally accepted definition has been established, and it can be assumed that the creation of such a definition is impossible, given the scientific breadth and complexity of the term.

Over the span of nearly seven decades since the term's first use, several hundred different definitions of the concept have emerged, applied depending on the context of AI usage, the level of technological advancement and the sophistication of new media (Meacham 2021, 1-2). For example, as early as the 1970s, Richard Ernest Bellman described artificial intelligence as the process of automation of certain activities such as decision-making and learning, which reflect human intelligence (Bellman 1978, 12). Almost two decades later, Robert J. Schalkoff characterised AI as a sphere of study aiming to clarify and simulate intelligent behaviour through computational processes (Schalkoff 1990, 35). Paul

Thagard, focusing on the scientific aspect of AI, defined it as a discipline encompassing issues such as neural networks, algorithms, artificial life, fuzzy logic, robotics and evolutionary computation. He emphasised that AI is a part of computer science concerned with studying the rules governing smart human behaviours, creating models of these behaviours and consequently developing computer programmes that simulate them (Thagard 1993, 11). In the 21st century, Peter Menzel and Faith D'Aluisio pointed out that artificial intelligence is a method of programming that enables computers to operate autonomously, including learning, reasoning, adapting to their environment, correcting and improving their performance (Menzel and D'Aluisio, 2001, 82). Around the same period, Stuart Russell and Peter Norvig simply defined AI as systems that act and think like humans – that is, they think and behave rationally (Russell 2003, 16). Missy Cummings viewed AI as the possibilities of computers to perform tasks that require human intelligence, such as image processing, speech recognition, and decision-making (Cummings 2018, 7). Michael C. Horowitz simply defined AI as the use of computers in ways that simulate intelligent human behaviour (Horowitz 2018, 40). Finally, Max Tegmark described artificial intelligence in very simple terms as non-biological intelligence (Tegmark 2019, 58).

Artificial intelligence is thus understood in two ways. On the one hand, there is an anthropocentric approach, which is characterised by seeking similarities between artificial and human intelligence (Bostrom 2016, 55). This perspective highlights a range of shared traits and numerous similarities between what characterises human and artificial intelligence. On the other hand, however, this way of defining AI faces extensive criticism, and a non-anthropocentric or even anti-anthropocentric approach has become dominant. In this latter case, it is emphasised primarily that computers cannot think like humans because they simulate thinking rather than duplicate it. Moreover, supporters of the non- or anti-anthropocentric view stress that artificial intelligence is simply a concrete algorithm designed to achieve a defined goal or solve a specific problem. AI is thus software whose code contains algorithms that make decisions based on processed data in order to enable machines to perform tasks consciously (Primož 2024, 31-50). Therefore, artificial intelligence does not need to think in a manner corresponding to human intelligence, nor does it need to resemble the functioning of the human brain. Furthermore, decisions made by algorithms processing vast amounts of data often exceed the scope of human knowledge and interpretative capabilities (Bostrom 2016, 55).

To summarise the theoretical considerations on artificial intelligence, it should be noted that the English-language literature classifies AI among the emerging threats – factors arising as a result of technological development that may contribute to significant threats to the functioning of actors in international relations (Emerging 2025).

Generative AI, in turn, is a specific type or branch of artificial intelligence that, unlike traditional AI, possesses creative power – it can generate new, original content such as texts, images, sounds, videos, games (including generating successive game levels), as well as product visualisations or prototypes. Its development and initial successes date back to the 2020s and are associated with advancements in deep neural networks based on transformers, especially large language models (Ashraf 2024, 716-725). The foundation of GenAI lies in deep learning, a form of machine learning that mimics the human brain's data processing and decision-making patterns. Artificial neural networks, composed of many interconnected layers, process and transmit information by emulating neurons in the human brain (Alalaq 2025, 1-15).

Looking at the origins of GenAI, it should be noted that one of the first cases of its widespread use occurred only in the spring of 2020, when in March an anonymous researcher from the Massachusetts Institute of Technology released a free online application, 15.ai, capable of generating realistic voices of characters using minimal training data. The success of GenAI proved extraordinary and spread at a revolutionary pace (Generative 2025). Almost immediately, it found broad applications across numerous sectors, including computer science, robotics, software development and the design of virtual assistants that generate human-like responses, as well as in business, marketing, finance, customer service sectors, advertising, medicine, healthcare, scientific research and the broadly understood entertainment industry – including pop culture – as well as in art, literature and even fashion (Marr 2024). For nearly five years, the following have remained in widespread use: 1) text-based chatbots or programmes designed to simulate conversations with humans, including ChatGPT, Copilot, Google Gemini, Llama 2, DeepSeek and Claude; 2) AI-based image generation systems that transform text into images or videos, such as Stable Diffusion, Midjourney, Bing Image Creator and DALL-E 3; and 3) voice generators that convert available text into speech, such as Microsoft VALL-E, or into video, such as Sora. Tech giants such as Microsoft, Google, Bing Chat, Baidu, OpenAI and Anthropic have developed their own generative artificial intelligence models, which are widely available in various versions and levels of advancement (Wood 2024).

To summarise the theoretical issues related to AI and GenAI, it should be noted that GenAI utilises advanced machine learning models to analyse data and generate new, unique outputs that mimic human creativity. Thus, it can be stated that while the task of AI is to analyse existing data, categorise it and forecast certain scenarios, the task of GenAI is to create an entirely new reality (new data). Generative AI is therefore perceived as a kind of virtual expert that supports human ingenuity, innovativeness, efficiency, resourcefulness and unconventional thinking.

The third decade of the 21st century can thus be described as the decade of GenAI. The success of this tool is indeed extraordinary. Like AI,

GenAI possesses a wide range of advantages and shows excellent prospects for the future in developing even more advanced instruments (Raiskin 2019, 53-60). However, in the case of GenAI, concerns about its potential misuse arise to an even greater extent than with AI, especially by non-state actors, including terrorist organisations. GenAI indicates not only remarkable technological progress that contributes to facilitating human life and the functioning of the world, but also entails increased risks related to cyberterrorism, cybercrime, the easy generation of fake news, the creation of false or distorted images of reality, mass production of deepfakes, manipulation and control of individual or mass audiences of the disseminated content, and on a broad scale, the threat of information warfare (Verma and Goyal 2024). The ethical aspects of GenAI usage – particularly regarding human rights issues, the use of biometric systems, improper control of migration, as well as the authenticity and integrity of generated texts, the dissemination of false information or deliberate fraud – raise numerous concerns and require appropriate legal regulations. The legislation concerning GenAI currently represents an urgent and significant challenge for political decision-makers at both national and international levels (Kajjo 2024).

The Islamic world doesn't exempt itself from the challenges associated with AI and GenAI. The most significant challenges are related to Islamic doctrine and the ethical aspects of Islam in the context of using AI. Muslim states take different initiatives to become active global actors in the AI sphere. They participate in the development of AI and GenAI, which nowadays shape a crucial part of human life. The Islamic world has to find a balance between technological progress in the AI sphere and adherence to Islamic ethics. Discussions focus on the interactions between AI and Islamic doctrine. The Muslim scientists emphasize the need for a nuanced approach that respects Islamic teachings while embracing the benefits of AI. They encourage taking initiatives to develop AI systems that adhere to ethical guidelines informed by Islamic principles. They emphasize that the initiatives must promote fairness, transparency, and accountability in decision-making processes, as well as in AI algorithms and new human-centered design. The connection between AI and Islam must reflect the integration of Islamic doctrine with technological advancements. The active involvement of the Muslim world in AI development and regulation demonstrates a commitment to ensuring that AI advances in the Islamic states in a manner compatible with the Islamic doctrine (Ali 2024).

3. AI and GenAI as Intensifiers of Jihadism – theory and practice

Attempting to identify how, through which tools and in what areas AI – especially GenAI – become actual and potential intensifiers and propagators of jihadism utilised by Islamic terrorist organisations, it is nece-

ssary to consider at least some of the most active dimensions (spheres) of their use and operations, namely: 1) personalised propaganda (Whittaker 2022, 71-79) and disinformation (Terrorist, 2024); 2) interactive, selective recruitment (Esmailzadeh 2023, 535-543) and radicalisation (Early 2023); 3) combat applications and use on the battlefield (Snyman 2024).

In reference to the spheres outlined above, in which AI – and particularly GenAI – may become an effective instrument in the hands of radical Islamist terrorist organisations, thereby serving as a propagator and intensifier of jihadism, it is worth presenting specific instances of such activities that have occurred in recent months and years. It must be stressed that the primary objective of Islamist terrorist organisations employing GenAI is hallucinatory propaganda aimed at broad audiences, deliberately distorting the perception of reality so as to evoke predetermined emotions and behaviours among recipients. This means that, at first glance and without thorough examination of an image or text, the transmitted information may appear coherent. However, upon closer, in-depth analysis, it proves to be unreliable, internally contradictory, devoid of logical sense and therefore false. In light of this, it can be concluded that GenAI has the potential to enhance the capacity of Islamist terrorist organisations to influence the behaviour of ordinary individuals and create difficulties in distinguishing between genuine and fabricated online content. Bots, for example, can flood forums and social media platforms on a massive scale, manufacturing a false dynamic of discussion and fuelling social tensions, including those along racial or religious lines. This constitutes an exceptionally dangerous phenomenon that has already become an integral part of the reality surrounding human existence – on a global scale (Neifakh 2024).

Citing several examples of the use of AI and GenAI by radical Islamist terrorist organisations in the realm of personalised propaganda, disinformation and interactive – often selective – recruitment and radicalisation, it is worth referring to the latest stage of the conflict in the Gaza Strip. This is undeniably a conflict in which, due to its complexity, multidimensional nature and the profound emotional charge, as well as political and social controversy surrounding it, terrorists exploit GenAI to publish online images and videos aimed at escalating violence, disseminating disinformation, conducting a "hallucinatory war" and portraying themselves as victims. For this purpose, they employ certain images of children and young people who have been injured or killed as a result of Israeli attacks (the disproportionate attacks by Israel and the policy of violence pursued by the Israeli authorities under Prime Minister Benjamin Netanyahu must be unequivocally condemned!). These images are deliberately selected rather than chosen at random, aiming to evoke the strongest possible emotional responses and to escalate chaos, as well as to trigger heated discussion, particularly online, between supporters and

opponents of Israel's brutal military campaign in the Gaza Strip (Siegel 2024).

Another example of "hallucinatory war" involves images and videos depicting IDF soldiers wearing diapers, which surfaced on social media. These materials appeared to have been generated by a group linked to Hamas through the use of GenAI, with the aim of undermining the authority of the Israeli army. The images spread rapidly across the Internet, escalating disinformation about the reality on the ground in the Gaza Strip (Siegel 2024).

Some Islamist terrorist organisations have also published guidelines on the use of AI and GenAI for producing propaganda and spreading disinformation. Examples of such activities include: 1) a technical manual on the safe use of GenAI tools published by IS in the summer of 2023; 2) a guide to memetic warfare in which jihadist groups (including those affiliated with al-Qaeda and IS) provided instructions on how to employ AI- and GenAI-based image-generation tools to create extremist memes (Criezis 2024); 3) the use of GenAI by IS and IS-affiliated organisations to translate propaganda speeches and communiqués into Arabic, Indonesian and English – a practice that has become widespread in order to expand their reach (Minniti 2025); 4) the use of GenAI by al-Qaeda-affiliated organisations to produce propaganda materials and posters (Criezis 2024).

Thanks to GenAI, Islamist extremist groups are able to scale both the quality and quantity of their propaganda more easily. Admittedly, in order to identify vulnerabilities in GenAI systems, practitioners attempt to bypass GenAI model safeguards by simulating the ways terrorists might try to circumvent protections, and technology companies implement "red teaming" activities, in which they actively engage experts to reveal potential security gaps. However, this does not guarantee success or complete protection against terrorist activities. Moreover, a black market dedicated to the so-called jailbreaks – methods of circumventing the ethical safeguards embedded in AI models – has already emerged. GenAI may be capable of providing instructions on how to bypass security systems, as well as how to construct weapons or organise the structures of terrorist cells. This is particularly attractive to lone-actor attackers (Weiman 2024, 17-24).

When analysing cases of GenAI use by terrorist groups, it is also important to highlight its potential application in manipulating and circumventing content moderation of materials that promote violence and extremism, which these groups disseminate online both synchronously and asynchronously. This implies that GenAI can be easily employed to conceal and evade detection, for instance on social media platforms, of both the sources of such manipulations and the very moderation processes. A striking example of such practices is the superimposition of cartoon characters onto live-streamed video materials of terrorist attacks. This occurred during the Christchurch attack in 2019,

when the characters from the Minions animated films were overlaid onto victims in order to evade detection of the terrorists and to make the attack itself more attractive (Saltman and Gilmour 2025).

GenAI can also significantly enhance the capabilities of Islamic terrorist organisations to personalise their recruitment activities, particularly given the importance that groups such as Al-Qaeda and IS attach to tailored and targeted strategies. Recruitment chatbots can be employed by terrorists on social media platforms and in online gaming environments in an increasingly efficient way, simulating everyday conversations and encouraging users to familiarise themselves with more extreme content. A notable case from the United Kingdom involved the planning of a terrorist attack with the participation of a chatbot. Jaswant Singh Chail planned an attack on Queen Elizabeth II using a crossbow, acting under the influence of his "AI-girlfriend" (Mathur and Boekaert and Clark 2024).

Propaganda and disinformation using GenAI tools have become tailored to specific contexts, personalised and easier to produce. Their activities also include deepfakes of fictional or real online personalities, as well as audio or video recreations, aimed at creating more engaging content for audiences. As an example, one can point to the appearance on the Internet of deepfakes concerning the Bali bombings carried out by the Jemaah Islamiyah group linked to Al-Qaeda, which brought the terrorists back to life, and these revived figures encouraged viewers to carry out attacks and incited violence (Saltman and Gilmour 2025). More sophisticated GenAI-generated images are now visible in official publications associated with ISIS.

The aforementioned activities also extend to the modification of existing online games by Islamic terrorist groups or the creation of their own online gaming environments. A report by Tech Against Terrorism from January 2023 highlights trends related to terrorism and extremist ideology online, noting that gaming platforms constitute a part of a broader problem. Gaming networks (multiplayer games and their platforms) are used by radical groups not only to disseminate extremist content that is removed from major social media platforms and is available only on the dark web, but also to establish contacts and build networks (Report 2023). Online games can be used to embed symbolic content, thereby normalising its reception. For example, one such game is *Quest for Bush*, released in 2006 by the Global Islamic Media Front, in which players completed six missions fighting against American soldiers resembling presidents, and in the final, seventh mission, directly confronting the president in a desert setting. Throughout the game, jihadist songs are played in the background. ISIS, in turn, modified the popular game *Grand Theft Auto*, allowing players to assume the role of ISIS fighters killing police officers and attacking military vehicles carrying explosives. In *Assassin's Creed*, ISIS inserted flags supporting its cause. Hezbollah developed the *Special Force* and *Special Force 2* series, which simulated military missions

against the IDF. All of these games are available online in multiple languages to reach a global audience (Lamphere-Englund 2024). According to the same report, one gaming platform contained 40 versions of real terrorist attacks. Users could, for example, simulate the roles of terrorists in Christchurch in 2019, Buffalo in 2022, Utøya in 2011 or at the Bataclan theatre in Paris in 2015 (Report 2023).

GenAI tools can also facilitate innovative methods for planning and executing terrorist attacks themselves by providing access to critical information. There are also concerns regarding the use of chatbots and cybercriminal tactics to raise funds through cryptocurrencies (Voronkov and De Meo 2021).

Increasing attention is being paid to the spreading of information on bomb-making, 3D-printed firearms and the potential future development of chemical and biological weapons. For example, in the United States, there is an online movement called "3D2A", which links 3D printing with Second Amendment rights, providing instructions to terrorist organisations on how to use GenAI to facilitate the partial or complete 3D printing of assault weapons (Saltman and Gilmour 2025).

Finally, GenAI could also prove to be an especially dangerous tool in the hands of Islamic terrorist organisations on the battlefield. Its potential military applications could be considerable. For instance, there is a risk of extensive use of autonomous vehicles as explosives (a capability that was already partially exploited by ISIS in Syria and Iraq). GenAI could significantly enhance the operational capabilities of such vehicles, enabling them to autonomously navigate to a designated target and detonate explosives (Archambault and Veilleux-Lepage 2020). The key technology here is that used for autonomous driving: AI, by analysing and processing data from various sensors such as cameras and radars, allows vehicles to perceive their environment, identify obstacles and predict traffic flow, thereby ensuring autonomy and functionality in their surroundings. The development of this type of technology could consequently reduce the need for human operatives (not entirely predictable in their behaviour) in the role of suicide attackers, replacing them with machines – in this case, with autonomous vehicles controlled by AI (Hall 2024). It is also worth noting that following the explosion of a Tesla Cybertruck near the Trump hotel in Las Vegas in January 2025, concerns about the use of autonomous vehicles for terrorist attacks have increased, especially given ISIS's growing use of delivery vans and passenger cars in attacks on crowded areas (Chasan 2025).

There is also concern that extremist Islamic terrorist groups will increasingly use AI- and GenAI-assisted drones to carry out attacks. The use of drones by Islamic organisations dates back to the second decade of the 21st century. For example, in 2017, ISIS announced the creation of a division called the Mujahideen Unmanned Aerial Vehicles, whose primary goal was to employ the unmanned aircraft as part of a long-term strategy

to develop drone technology and adapt it for use as a weapon. In East Africa, it has been documented that Al Shabaab used drones for reconnaissance and to record propaganda materials. Terrorist organisations employ drones to gather information on the location of military forces, types of weaponry and potential troop movements. The possession of advanced GenAI technologies increasingly allows terrorists to engage in combat on equal terms. A new reality dominated by GenAI on the battlefield implies that drones equipped with, or even controlled by, artificial intelligence are becoming a fundamental tool for these groups on the battlefield (Hope 2025).

5. Conclusions

Nowadays, there are many links between the Muslim world and research into artificial intelligence and GenAI. Muslim scientists are involved in global research on artificial intelligence, which stems from the concern and, at the same time, the necessity to reconcile this technological tool with Islamic doctrine and ethics. Islamic countries remain active in this field and are not just passive observers of how the West operates in the sphere of AI. Muslim countries are primarily seeking a platform for integration, including reconciling Islamic principles with technological innovations related to AI. On the one hand, these activities contribute to the development of artificial intelligence in the Muslim world. On the other hand, they ensure that technological development in the AI sector is consistent with Islamic doctrine and the ethical and cultural values of Muslim societies.

A vital research initiative is the analysis of artificial intelligence ethics from an Islamic perspective. Research focuses on pluralistic ethical benchmarking for artificial intelligence and Islamic philosophy. Arab countries, particularly those in the Arab League, are attempting to develop a common strategy for the use and development of artificial intelligence. The aim is to address the challenges that AI poses to the traditional approach to religion and ethics. AI initiatives in Arab countries include educational programmes dedicated to AI, research centres, and efforts to develop an ethical framework for GenAI. These initiatives demonstrate a proactive approach to leveraging technological advances while adhering to Islamic principles.

The Islamic scholars emphasise that AI's potential to understand the Qur'an is significant. AI can assist in the philosophical and linguistic analysis of the Qur'an. Advanced algorithms can analyse classical Arabic, helping to interpret the text and provide context for revelations. This can be particularly beneficial for non-Arabic speakers seeking. Cooperation between Muslim scientists, scholars, and tech companies on AI ethics and Islamic doctrine is evident in ethical and philosophical research, the use of

Islamic prayer bots, conferences that consider the relationship between Islam and AI, and efforts to raise and promote rational awareness about the responsible use of AI in Muslim societies.

The rapid transformation of the modern world and the development of new technologies present significant opportunities for growth as well as new security threats. The emergence of advanced technologies such as AI and GenAI has raised considerable concerns regarding their potential use by Islamic (jihadist) terrorist organisations. While these groups have been using new technologies for a long time to achieve their objectives – including radicalisation, the expansion of jihadist ideology, and ultimately the execution of terrorist attacks – the progress in AI and GenAI has almost revolutionised the operational capabilities of jihadist groups, making them even more dangerous and unpredictable non-state actors on the international stage.

The above analysis demonstrates that the use of GenAI by Islamic terrorist groups undoubtedly represents a concerning new trend in the evolving landscape of global security. These organisations are increasingly turning to advanced technologies based on broadly defined AI to achieve their objectives. The consequences of their use of AI and GenAI are extensive and encompass activities across three main fields: 1) the dissemination of personalised propaganda tailored to the age and gender of the audience, the creation of sophisticated disinformation campaigns, including the conduct of a "hallucinatory war" aimed at producing false media content to incite violence, spread fear and generate chaos; 2) interactive, selective (also based on age and gender criteria) recruitment and radicalisation through enhancing the appeal of violent content disseminated online, the personalisation of conversations via chatbots acting as recruiters for terrorist organisations, the use of online games embedding jihadist ideology and the expansion of deepfakes; 3) the enhancement of jihadist organisations' technological capabilities on the battlefield through the deployment of far more complex technologies and the widespread use of GenAI-controlled drones and autonomous combat vehicles to carry out terrorist attacks.

In summary, the above analysis indicates that while GenAI possesses many valuable features and offers significant potential for progress, its misuse by entities such as Islamic terrorist organisations carries substantial risks. GenAI creates the potential for an almost revolutionary transformation in jihadist operations, both in terms of speed and scale. It enables the conduct of a highly effective "hallucinatory war", the exertion of specific influence over individuals (deliberately and selectively targeted chat-recruitment victims), and can thus be used for the rapid radicalisation of selected individuals or social groups, the expansion of jihadist ideology and the effective execution of *qital* (Mostfa 2021, 1-17).

AI and GenAI thus enable Islamic terrorist organisations to feel increasingly confident in the realm of new information and communi-

cation technologies. AI and GenAI have become highly effective tools in the hands of jihadist groups, and their ease of use, widespread and nearly unlimited availability, combined with weak safeguards, make them what can be described as intensifiers and catalysts of jihadism. In light of this emerging trend, political decision-makers at the global level should closely cooperate to develop unified strategies to counter the misuse of GenAI by terrorist organisations. By taking appropriate international measures to reduce the risks associated with GenAI use by jihadist groups, it is possible to create a secure environment where "hallucinatory war" has no place. At the current stage of GenAI development, this appears both feasible and necessary, as although a "terrorist chatbot" does not yet exist, the technological infrastructure, deep social vulnerability and even greater determination on the part of jihadist organisations are already in place.

References:

Ali, Muhammad Mumtaz. 2024. "AI and Islam: Navigating the Path Between Progress and Ethics." https://www.islamicity.org/92680/ai-and-islam-navigating-the-path-between-progress-and-ethics/

Archambault, Emil and Veilleux-Lepage, Yannick. 2020. "Drone imagery in Islamic State propaganda: flying like a state." *International Affairs* 96(4): 955–973.

Bellman, Richard Ernest. 1978. *An Introduction to Artificial Intelligence: Can Computers Think?* San Francisco: Boyd & Fraser Publishing Company.

Bernd, Lidia. 2024. "AI-Enabled Deception: The New Arena of Counterterrorism." *Georgetown Security Studies Rewiev,* May, 3. https://georgetownsecuritystudiesreview.org/2024/05/03/ai-enabled-deception-the-new-arena-of-counterterrorism/

Bostrom, Nick. 2016. *Superinteligencja. Scenariusze, strategie, zagrożenia*. Gliwice: Helion.

Chasan, Aliza, 2025. *Tesla Cybertruck bomber used ChatGPT to plan Las Vegas attack, police say.* CBC News. January, 7. https://www.cbsnews.com/news/las-vegas-cybertruck-explosion-fire-chatgpt-plan/

Criezis Meili. 2024. *AI Caliphate: The Creation of Pro-Islamic State Propaganda Using Generative AI.* Global Network on Extremism and Technology, https://gnet-research.org/2024/02/05/ai-caliphate-pro-islamic-state-propaganda-and-generative-ai/

Cummings, Missy L. 2018. "Artificial intelligence and the future of warfare" In *Artificial intelligence and international affairs. Disruption anticipated*, edited by Missy L. Cummings et al. 7. London: The Royal Institute of Foreign Affairs.

Early terrorist experimentation with generative artificial intelligence services. 2023. Tech Against Terrorism. https://techagainstterrorism.org/hubfs/Tech%20Against%20Terrorism%20Briefi

ng%20-%20Early%20terrorist%20experimentation%20with%20generative%20artificial%20intelligence%20services.pdf

Emerging Threats to Critical Infrastructure: AI Driven Cybersecurity Trends for 2025. 2025, January 3. Capitol Technology University. https://www.captechu.edu/blog/ai-driven-cybersecurity-trends-2025

Esmailzadeh Yaser. 2023. "Potential Risks of ChatGPT: Implications for Counterterrorism and International Security." *International Journal of Multicultural and Multireligious Understanding* 10(4): 535-543.

Gaikwad, Tushar. 2018. "Artificial Intelligence based Chat-Bot." *International Journal for Research in Applied Science and Engineering Technology* 6(4): 2305-2306.

Generative AI in 2025: History, Innovations, and Challenges. 2025. https://www.sandgarden.com/learn/generative-ai

Haenlein Michael and Kaplan Andreas. 2019. "A Brief History of Artificial Intelligence: On the Past, Presnt, and Future of Artificial Intelligence." *California Management Review* 61(4): 1-9.

Hall, Jonathan. 2024. *Generative AI, Drones, and Terrorism*. London, October 22. https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2024/10/IRTL-GenAI-Drones-Oct-24-1.pdf

Hope, Graham. 2025. *UN Warns of Terrorist Threat for Self-Driving Cars, Slaughterbots.* https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.rand.org/pubs/commentary/2018/01/autonomous-vehicles-terrorist-threat-or-security-opportunity.html&ved=2ahUKEwiot7DigaaPAxWTSPEDHSuoMFwQFnoECB8QAQ&usg=AOvVaw03a7DDq6ThwQAulvswzZHy

Horowitz, Michael, C. 2018. "Artificial intelligence. International competition and balance of power." *Texas National Security Review* 1(3): 40.

Kajjo Sirwan. 2024. *IS turns to artificial intelligence for advanced propaganda amid territorial defeats.* VOA Technology. https://www.voanews.com/a/is-turns-to-artificial-intelligence-for-advanced-propaganda-amid-territorial-defeats/7624397.html

Krašovec, Primož. 2024. "A Critique of Anthropocentrism in the Evaluation(s) of Artificial Creativity." *Media Research: Croatian Journal for Journalism and the Media* 30 (2): 31-50.

Marr, Bernard. 2024. *Generative AI in Practice : 100+ Amazing Ways Generative Artificial Intelligence is Changing Business and Society*. Hoboken, NJ : John Wiley & Sons.

Mathur, Priyank and Boekaert, Clara and Clark, Colin P. 2024. *The Radicalization (and Counter-radicalization) Potential of Artificial Intelligence.* https://icct.nl/publication/radicalization-and-counter-radicalization-potential-artificial-intelligence

Meacham, Margie. 2021. "A Brief History of AI and Education. *Global Science Research Journals*." 2 (4): 1-2.

Menzel, Peter and D'Aluisio, Faith. 2001. *2002. Robo Sapiens: Evolution of a New Species*, Cambridge: MIT Press.

Minniti, Fabrizio. 2025. *Automated Recruitment: Artificial Intelligence, ISKP, and Extremist Radicalisation*. Global Network on Extremism and Technology. https://gnet-research.org/2025/04/11/automated-recruitment-artificial-intelligence-iskp-and-extremist-radicalisation/

Mostfa, Ali. 2021. "Violence and Jihad in Islam: From the War of Words to the clashes of Definitions." *Religions* 12(966): 1-17.

Mudasir, Ashraf. 2024. "Generative AI: Challenges and the Road Ahead." *International Journal of Science and Research (IJSR)* 13(10): 716-725.

Neifakh, Vernica. 2024. *Terrorists Exploit AI for Propaganda and Operations, Exposing Critical Gaps in Tech Safeguards*. https://themedialine.org/top-stories/terrorists-exploit-ai-for-propaganda-and-operations-exposing-critical-gaps-in-tech-safeguards/

Pratt, Douglas. 2006. "Terrorism and Religious Fundamentalism: Prospects for a Predictive Paradigm." *Journal of Religion* 11(1): 438-456.

Raiskin, Or Anat Elimelech. 2019. "ISIS's use of cyberspace – furthering the organization's goals utilizing new media." *Humaniora* 25(1): 53-60.

Report: State of Play - Trends in Terrorist and Violent Extremist Use of the Internet 2022. 2023. Tech Against Terrorism. January 19. https://www.techagainstterrorism.org/hubfs/FINAL-State-of-Play-2022-TAT.pdf

Russell, Stuart and Norvig, Peter. 2003. *Artificial Intelligence: A Modern Approach*, London: Pearson Education Inc.

Saltman, Erin and Gilmour, Skip. 2025. *Artificial Intelligence: Threats, Opportunities, and Policy Frameworks for Countering VNSAs*. GIFCT. https://gifct.org/wp-content/uploads/2025/04/GIFCT-25WG-0425-AI_Report-Web-1.1.pdf

Schaer, Cathrin. 2024. *How extremist groups like 'Islamic State' are using AI*. https://www.dw.com/en/how-extremist-groups-like-islamic-state-are-using-ai/a-69609398

Schalkoff, Robert. 1990. *Artificial Intelligence: An Engineering Approach*. New York: McGraw-Hill Inc.

Sheikh, Haroon and Prins, Corien and Schrijvers, Erik. 2023. *Mission AI: The New System Technology*, The Haag: Springer.

Siegel, Daniel. 2024. *AI Jihad: Deciphering Hamas, Al-Qaeda and Islamic State's Generative AI Digital Arsenal*. Global Network on Extremism and Technology. February, 19. https://gnet-research.org/2024/02/19/ai-jihad-deciphering-hamas-al-qaeda-and-islamic-states-generative-ai-digital-arsenal/

Skaker, Alalaq Ahmed. 2025. "The History of the Artificial Intelligence Revolution and the Nature of Generative AI Work." *DS. Journal of Artificial Intelligence and Robotics* 2(4): 1-15.

Snyman, Nicole. 2024. *How might terrorist groups and other actors utilise GenAI?* https://www.another-day.com/resources/how-might-terrorist-groups-and-other-actors-utilise-genai

Tegmark, Max. 2019. *Życie 3.0. Człowiek w erze sztucznej inteligencji*. Warszawa: Prószyński i S-ka.

Terrorist Groups Looking to AI to Enhance Propaganda and Recruitment Efforts. 2024, October 3. https://thesoufancenter.org/intelbrief-2024-october-3/

Thagard, Paul. 1993. Computational Philosophy of Science. Cambridge: The MIT Press.

Thompson, Emily and Lamphere-Englund, Galen. 2024. *30 Years of Trends in Terrorist and Extremist Games*. Global Network on Extremism and Technology Report. King's College London. https://gnet-research.org/wp-content/uploads/2024/10/GNET-47-Extremist-Games_web.pdf

Verma, Aashi and Goyal, Ajal. 2024. *Advantages and Disadvantages of Generative AI.* https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.pickl.ai/blog/advantages-and-disadvantages-of-generative-ai/&ved=2ahUKEwjNvbTyj6GPAxVAgv0HHbP1DSEQFnoECBkQAQ&usg=AOvVaw2QvFGEFvWCYSmDCSZYlLZR

Voronkov, Vladimir and De Meo, Antonia Marie. 2021. *Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes. A Joint Report by UNICRI and UNCCT*. New York, United Nations Office of Counter-Terrorism (UNOCT). https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf

Weiman, Gabriel et al. 2024. "Generating Terror: The Risks of Generative AI Exploitation." *CTC Sentinel* 17 (1): 17-24.

Whittaker, Joe. 2022. "Rethinking Online Radicalization." *Perspectives On Terrorism* 16(4): 71-79.

Wood, Christina X. 2024. *10 Top* Generative *AI Chatbots. March*, 28. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.vktr.com/ai-platforms/10-top-generative-ai-chatbots/&ved=2ahUKEwjU45ePjqGPAxWyhP0HHcy1CbkQFnoECCkQAQ&usg=AOvVaw35dVNyvd9xFDNpittHrFSD