Jurnal Pertahanan: Media Informasi tentang Kajian dan Strategi Pertahanan yang Mengedepankan Identity, Nasionalism dan Integrity
Vol. 11 No. 1 (2025) pp.120-134
https://jurnal.idu.ac.id/index.php/DefenseJournal

The Potential Growth of Terrorism in the Age of Artificial Intelligence and The Quranic Response to Counteraction Scenarios

Habib Maulana Maslahul Adi[1*], Afifah Ikram Mufidah[2]
[1,] Pendidikan Kader Ulama Masjid Istiqlal, Indonesia
[2] Sunan Kudus State Islamic University, Indonesia

maslahulhabib@gmail.com[1*], afifahikram@ms.iainkudus.ac.id[2]
*Corresponding Author

Article Info

Article history:
Received: October 31, 2024
Revised: April 16, 2025
Accepted: April 30 , 2025

Keywords:
Al-Qur'an,
Artificial Intelligence,
Library research,
Terrorism

DOI:
http://dx.doi.org/10.33172/jp.v11i1.19758

Abstract

The sophistication of Artificial Intelligence (AI) has the potential to increase the complexity of terrorism, although AI can also facilitate counter-terrorism efforts. On the other hand, the Quran, as a source of inspiration and guidance for Muslims, encourages Muslim intellectuals to actualize its teachings in response to emerging issues. This article aims to discuss the potential development of terrorism that utilizes AI and to explore the Quranic response to counter-terrorism scenarios in the AI era. The method used is qualitative, categorized as library research based on its data sources. Documentation serves as the main data collection technique. The analysis is conducted inductively, with comparative analysis prior to drawing the conclusion. The findings of this study indicate that the potential development of terrorism through AI includes enhanced cyber-attack capabilities, autonomous weapons, false propaganda dissemination, data exploitation, disruption of vital infrastructure, and recruitment and deepening of radicalization. Furthermore, scenarios for using AI in counter-terrorism and the Quranic response to them include predictive analysis of terrorist activities and identification of radicalization warning signs as preventive measures aligned with the Quranic teaching of *sadd aż-żarī'ah*, detection of misinformation and disinformation in line with the values in Surah Al-Hujurat [49: 6], moderation and automatic content removal aligned with the values in Surah An-Nisa [4: 148], and counter-narratives to terrorism and extremism aligned with the values in Surah An-Nahl [16: 125]. Therefore, it is also important for Islamic scholars, as successors holding religious authority in Islam, to actively participate in disseminating the values of the Qur'an that reject all forms of terrorism, so they can contribute to combating the growth of terrorism in the AI era.

INTRODUCTION

The rapid development of information technology and the emergence of Artificial Intelligence (AI) have transformed the global security paradigm (Masakowski, 2020). Alongside these technological advancements, one of the pressing and increasingly complex security challenges facing the world today is terrorism (Ige et al., 2023). In efforts to address this challenge, optimizing the use of AI technology has become crucial for preventing acts of terrorism (Minchah, 2020). This is due to AI's capability to analyze vast volumes of data in a relatively short time and to identify patterns that might be difficult for humans to detect (Jarrahi, 2018). However, while AI promises innovative and up-to-date solutions for counter-terrorism, it is important to remember that this technology can also be exploited by terrorist groups to develop new strategies and more sophisticated tactics. Therefore, there is an urgent need to understand the complex dynamics between AI technology development and the fight against terrorism (Johnson, 2019).

To date, there have been no direct instances of terrorism in Indonesia leveraging Artificial Intelligence. However, upon closer examination, the potential threat of digital attacks utilizing AI is already being felt and, in some cases, has subtly emerged without full awareness. This is evidenced by the increasing prevalence of phishing activities (Ahdiat, 2023), malware and ransomware attacks (Wire, 2023; Zuhdi, 2023), and fraud via chatbots in Indonesia (Prasasti, 2023). This suggests that AI's significant development may eventually impact the broader landscape of terrorism. Addressing these contemporary challenges, particularly in counter-terrorism, which has become increasingly complex with the involvement of technologies such as AI, requires a holistic solution that aligns with technological advancements.

As is well known, the roots or driving factors behind terrorism are quite varied, ranging from political, ideological, and economic to religious factors (Brooke, 2022). Regarding religion as a driving factor or motive for acts of terrorism, misunderstandings often occur—for example, the assumption that a particular religion (other than one's own) advocates terrorism. However, this is not the case; rather, the factor driving religious-based terrorism stems from an individual's misunderstanding of religious teachings, which leads them toward the path of terrorism (Khairunnisa & Rohman, 2018). Among the religions often targeted and accused of promoting terrorism is Islam. This is due to the actions of certain individuals within the Muslim community who hold pro-violence views. Islam's position, frequently portrayed as a religion that endorses terrorism, requires more than just clarification and explanation from its followers. Instead, it presents an opportunity to demonstrate that Islam emphasizes peace, includes teachings opposed to terrorism, and offers practical inspiration for its prevention.

The Quran, as the holy book of Muslims, serves as a guiding source for addressing complex issues and remains relevant in providing solutions to these challenges (Ridwan

et al., 2023). As a source of inspiration, the Quran deserves to be explored in the development of counter-terrorism strategies that consider advancements in AI technology (Tang, 2023). A comprehensive study of the Quran is essential to disseminate its teachings in response to contemporary challenges. Combining Quranic teachings with AI advancements may contribute to a deeper understanding of how to address modern challenges grounded in the moral and ethical values contained in Islam's holy scripture. Therefore, analyzing Quranic verses related to peace, justice, and security can serve as a foundation for formulating balanced and comprehensive approaches to responding to increasingly complex terrorism threats. The results of such analyses can form the basis for designing effective policies to prevent and combat terrorism in the age of Artificial Intelligence.

Studies on the Quran to inspire general counter-terrorism strategies are indeed common, as is discourse on leveraging AI technology in counter-terrorism efforts. However, research linking the Quran specifically to the challenges of counter-terrorism in the era of Artificial Intelligence appears to be uncharted. In other words, the Quran has not yet been fully considered as a source of inspiration, nor thoroughly explored, for addressing these issues. Based on current research, studies on AI related to Islamic teachings tend to focus on topics such as the ethical challenges of AI from the perspective of *maqāṣid al-syarī'ah* (Mohadi & Tarshany, 2023; Rahman & Ibrahim, 2019), correlations between collective and cooperative behaviors in AI and similar behaviors in the Quran (Hashim et al., 2017), the use of AI in Quranic studies and interpretation (Saihu, 2022), and assessing the accuracy of AI in presenting Quran-related information (Handayani et al., 2021).

The lack of research on counter-terrorism discourse in the era of Artificial Intelligence from a Quranic perspective represents a gap that should be addressed to inspire proactive steps in tackling terrorism in the future. Therefore, this study aims to uncover insights from the Quran and discuss counter-terrorism discourse in the age of AI through a Quranic lens. By gaining a deep understanding of this relationship, it is hoped that effective and balanced strategies can be developed to mitigate the threat of terrorism in the AI era in alignment with Quranic guidance.

METHODS

To achieve the objectives of this study, a qualitative research method is employed, so the researcher plays a primary role in interpreting the phenomenon (Denzin & Lincoln, 2018). From the perspective of data collection, this research falls under library research because there is no direct observation of the phenomenon occurring in the field (Merriam & Tisdell, 2016). Data collection is conducted using documentation techniques, which are also commonly used in various social research (Punch, 1998).

As a library study, the data explored includes various literature sources such as books, journals, and other research findings that discuss counter-terrorism in general, counter-terrorism discourse in the era of Artificial Intelligence, Quranic perspectives on counter-terrorism, and Islamic views on AI. The collected data is then analyzed

inductively, with comparative analysis performed prior to drawing conclusions and revealing findings on counter-terrorism discourse in the AI era from a Quranic perspective.

RESULT AND DISCUSSION

Potential Scenarios of Terrorism Involving Artificial Intelligence

In the age of artificial intelligence, there exists the potential for terrorist entities to exploit this technology. While AI offers many positive applications, it also poses certain risks if misused for malicious purposes (Hayward & Maas, 2021). The potential terrorism scenarios in the AI era can encompass various aspects involving the use of advanced technology to plan and execute attacks. Although most technological advancements positively contribute to society, there are potential risks and abuses of AI in the context of terrorism (McKendrick, 2019). Referring to various academic studies that reveal AI's capabilities, several potential scenarios that may emerge can be outlined as follows:

Enhanced Cyberattack Capabilities

Terrorists have the potential to use AI to enhance their cyberattack capabilities. It is well known that AI can be utilized to conduct sophisticated cyberattacks, such as automated hacking, advanced phishing, or the creation of malware with adaptive and evolving features. AI-supported tools can also analyze and exploit security vulnerabilities, even recognizing security patterns to evade detection in computer systems more efficiently than traditional methods (Chakraborty et al., 2023). An illustration of the potential use of this method begins with the training of AI systems to identify vulnerabilities within critical infrastructure. This is followed by a coordinated cyberattack targeting power plants and electrical grid systems. After the attack, the perpetrators release a video claiming responsibility, aiming to incite public fear and undermine trust in the government (Weimann, 2015).

Use of Autonomous Weapons

Terrorist groups may use autonomous weapons equipped with AI to carry out attacks using robotic systems or drones. With advanced navigation capabilities, drones and other autonomous weapons programmed for this purpose could be used to identify and execute targets independently, making them potentially more lethal and harder to counter, thus leading to conflicts without direct human involvement in decision-making (Chakraborty et al., 2023). Equipped with AI-powered drones capable of autonomous navigation, the perpetrators target public events to gain attention and record the incident. The footage of the attack is then released as a demonstration of their technological capability and to inspire copycat actions (Scharre, 2018).

Spread of False Propaganda

Terrorism may begin with the exploitation of AI through the creation and dissemination of deepfake content tailored to specific audiences for propaganda purposes. This is due to deepfake technology's ability to create realistic audio or video content that is difficult to distinguish from original recordings (Gill, 2019). Terrorists could utilize this technology to spread false information, manipulate public opinion, or impersonate political figures to issue misleading statements. In another scenario, preparation involves stealing audio and video data to create deepfake content. The action consists of massive dissemination of the manipulated media through social platforms. The post-action consequence is widespread public confusion and a deterioration of political stability (Nasiri & Hashemzadeh, 2025).

Advanced Surveillance, Data Exploitation, and Social Engineering

The era of Artificial Intelligence allows for advanced surveillance, monitoring individuals' behaviors and tendencies, and observing public spaces from a distance for malicious purposes. Even AI algorithms connected with big data can exploit information for analysis in social media, finance, or personal data (McKendrick, 2019). In addition to using such tools to identify vulnerabilities, targets, or potential recruits, terrorists could also use them as intermediaries in social engineering tactics to create more convincing and personalized phishing attacks.

Disruption of Critical Infrastructure

AI can be employed to identify weaknesses in systems controlling essential services, such as electricity networks, transportation, and communication networks (Dick et al., 2019). Terrorists have the potential to use AI to target and disrupt critical infrastructure to create significant damage and broader social impacts (Gürkaş-Aydin & Gürtürk, 2022). Another approach includes developing AI algorithms for emotion detection during the preparation phase. In the action phase, operatives make personalized contact using empathetic messages. The post-action result is that the targeted individuals may become sympathizers or even participants in radical networks (Phadke & Mitra, 2021).

Recruitment and Deepening Radicalization

Chatbots and AI-powered algorithms can be used to identify individuals vulnerable to radicalization, tailoring propaganda and recruitment messages to specific demographics. Terrorists may leverage this technology to design recruitment campaigns or automatically disseminate extremist propaganda, reaching many people in a short period (Bazarkina, 2023). In the recruitment context, preparation entails analyzing the online behavior of potential targets. The action involves delivering personalized videos or inviting them to participate in radical forums. The post-action outcome is a covert increase in recruitment, particularly within digital environments (Conway et al., 2019).

In response to the complexities of potential terrorism that exploits AI technology, a combination of technological solutions, international cooperation, and ethical guidelines for the development and use of AI is required to mitigate these risks. Governments, technology companies, and security agencies must collaborate to implement robust

cybersecurity measures and ensure the responsible development of AI to prevent its misuse by criminals. However, it is important to note that while these potential risks exist, governments, technology companies, and security agencies have made many efforts to develop solutions and policies that can minimize terrorist threats in the era of Artificial Intelligence. Therefore, global collaboration and attention to the ethics of AI development and use will be key to addressing these potential risks.

The Quran and Terrorism Prevention

As previously mentioned, the factors driving acts of terrorism are varied, encompassing political, ideological, economic, and religious factors (Brooke, 2022). Therefore, a holistic approach to prevention is required, tailored to the specific factors that may underlie these terrorist actions. Among the guidance that can be drawn from the Quran in designing counter-terrorism strategies are as follows:

1. Economic Empowerment

   Developing economic empowerment programs to address poverty and dissatisfaction can trigger acts of terrorism. QS At-Taubah [9]:60 "*Zakat is only for the poor, the needy, those employed to collect it, those whose hearts are to be reconciled (new converts), for freeing slaves, for those in debt, for the cause of Allah, and for travelers in need—an obligation from Allah...*", emphasizes the importance of zakat and infaq as forms of community economic empowerment (Achmad, 2015).
2. Dissemination of Tolerance and Acceptance Teachings

   Promoting tolerance, acceptance, and respect for diversity. QS Al-Hujurat [49]:13 "*Oh mankind! Indeed, We have created you from a male and female, and made you into nations and tribes so that you may know one another...*", teaches that differences in race and ethnicity are the will of Allah, created so that people may know one another.
3. Promotion of Justice

   Encouraging active participation in social justice and community welfare efforts. The Quran emphasizes the importance of standing up for justice and respecting the rights of others in QS An-Nisa [4]:135 *"Oh you who believe! Be steadfast in upholding justice among all of humanity and bear true witness for the sake of Allah, without discrimination–even against yourselves, your parents, or your close relatives..."*.
4. Revitalization of Morality and Ethics

   A strong moral and ethical education based on Quranic teachings can shape individuals to avoid actions like terrorism. Encouraging individuals to follow Islamic teachings by leading a moral life. The Quranic spirit of fostering interfaith dialogue is indirectly reflected in QS Yusuf [10]:99 *"And if your God had willed, all the people on earth would have believed. But will you compel people to become believers?"* this verse explicitly states that coercion in matters of faith contradicts Allah's decree (Al-Sa'di, 2006, p. 374).
5. Mainstreaming Interfaith Dialogue

   Promoting interfaith dialogue to foster understanding and respect for differences in belief, as reflected in Surah Al-Kafirun [109]:6, *"To you be your religion, and to me my*

religion." This verse teaches that everyone has their own beliefs and ways of worship, and it serves as a guide for showing respect toward differing religious convictions.

6. Conflict Resolution through Consultation

Encouraging and designing mechanisms for conflict resolution through consultation and dialogue, rather than violence. QS An-Nisa [4]:114 "*There is no good in most of their secret conversations, except for those who enjoin charity, godness, or reconciliation among people...*", emphasizes the importance of deliberation in resolving disputes.

7. Promotion of Peace and Security

Teaching the values of peace and security and avoiding actions that could harm community security. QS Al-Baqarah [2]:205 "*And when he turns away from you, he strives to spread corruption on the earth, destroying crops and livestock, while Allah does not like corruption*", stresses that Allah loves peace. Governments also bear the responsibility to ensure the safety and protection of society from terrorism threats by using security mechanisms that align with Islamic laws and norms.

This can also be achieved by fostering peaceful, harmonious communities and encouraging dialogue among people of various religious and cultural backgrounds. QS Al-Ma'idah [5]:48 "*...So judge among them according to what Allah has revealed, and do not follow their desires by turning away from the truth that has come to you. For each nation among you, We have prescribed a law and a clear way...*", teaches that each community has its own laws and way of life.

The Potential of Artificial Intelligence in Countering Terrorism and its Correlation with the Teachings of the Qur'an

Artificial Intelligence indeed has the potential to be used by terrorist groups to carry out acts of terrorism; however, if AI falls into the right hands, it can also be utilized in efforts to combat terrorism itself. The potential for countering terrorism using AI is also explained in a report released by the United Nations Office of Counter-Terrorism (UNOCT) in collaboration with the United Nations Interregional Crime and Justice Research Institute (UNICRI) in 2021. Among the potentials mentioned are predictive analysis of terrorist activities, identification of signs of radicalization, detection of misinformation and disinformation spread by terrorists, moderation and automatic removal of content, as well as counter-narratives against terrorism and violent extremism (UNCCT & UNICRI, 2021). The potential for countering terrorism using AI, as mentioned in the United Nations report, actually correlates with the values taught by the Qur'an. The explanations are as follows:

Predictive Analysis of Terrorist Activities

The application of predictive analysis for counter-terrorism allows for moving beyond traditional reactive approaches to terrorism and becoming more proactive by anticipating future terrorist activities and intervening before attacks occur. Instead of monitoring individuals online and predicting their behavior, predictive models based on statistics from fully anonymized online sources—or at least obscured to protect user

privacy—can be used to identify trends or forecast future terrorist behavior. Analysis based on aggregated data can help support security and intelligence agencies in prioritizing scarce resources for operational support, making strategic decisions, or providing warnings to competent authorities (UNCCT & UNICRI, 2021).

Automated models for countering terrorist networks through the systematic collection of data about an organization can support efforts to combat terrorism by identifying priorities and the most effective strategies to "influence" terrorist behavior. For instance, researchers have applied AI, including Social Network Analysis (SNA) algorithms, to predict the fragmentation of terrorist groups, creating deeper insights into how and when terrorist organizations like ISIS and Al-Qaeda split (INSIKT-AI, 2018; UNCCT & UNICRI, 2021).

The predictive analysis described above essentially underscores preventive efforts to close gaps that may lead to acts of terror. This aligns with the principles taught in the Qur'an regarding the closure of pathways to corruption and immorality, commonly referred to in the discipline of *uṣūl fiqh* as *sadd al-żārī'ah*. Regarding the prevention of wrongdoing, Imām 'Izz al-Dīn bin 'Abd al-Salām uses Surah Al-An'am [6]:18 as a reference or *ḥujjah* ('Abdissalam, 2003). It is understood that terrorist actions cause destruction and are a cause of bloodshed, which is clearly part of the prohibitions found in the Qur'an, specifically in Surah Al-Maidah [5]:32.

Identification of Radicalization Warning Signs

Although radicalization is a complex social phenomenon, and the pathways to radicalization are highly personal and often political, machine learning techniques such as Natural Language Processing (NLP) can provide valuable support to law enforcement and counter-terrorism agencies, as well as other relevant actors in society, such as social workers. NLP can be used, for instance, to identify keywords that may indicate a state of radicalization in social media accounts or a person's vulnerability to online terrorist narratives. Recognizing specific behavioral patterns, such as consuming or browsing content related to terrorism and violent extremism that align with radicalization indicators, can also be beneficial (UNCCT & UNICRI, 2021).

The Real-time Early Detection and Alert System for Online Terrorist Content (RED-Alert) project, funded by the European Union (EU), is one example of a tool aimed at detecting early-stage radicalization while striving to meet high privacy and security standards. RED-Alert utilizes NLP, Social Network Analysis (SNA), and complex event processing to collect, process, visualize, and store online data related to terrorist groups, including early stages of radicalization based on social media content (Horizon, 2020). This tool supports the search for known keywords or subjects within unidentifiable relevant content. Additionally, it includes anonymization and de-anonymization processes that align with law enforcement agency protocols, which seem promising for other fields handling sensitive data (INSIKT AI, 2020; UNCCT & UNICRI, 2021). In addition to this tool, Moonshot, a technology company in the UK specializing in counter-terrorism and funded by the Monitoring System and Transfer Platform Radicalization

(MOTRA), is also developing a system aimed not only at identifying individuals vulnerable to online radicalization but also at connecting these vulnerable individuals with "positive messages."

Similar to the previous scenario, this step is part of preventive measures against the dangers of terrorism in the AI era, thereby aligning with the implementation of the Qur'anic teachings related to *sadd al-żarī'ah*. The texts used in this *sadd al-żarī'ah* principle have been mentioned earlier. Moreover, radicalization that may lead an individual toward extremism indeed needs to be prevented, as it contradicts the Qur'anic teachings on moderation, as stated in Surah Al-Baqarah [2]:143.

Detection of Misinformation and Disinformation Spread by Terrorists

The falsification or distortion of information can be dangerous and has the potential to contribute to spreading terrorist or violent extremist narratives into mainstream discourse (UNCCT & UNICRI, 2021). For example, during the COVID-19 pandemic, terrorists and violent extremists leveraged social media's vulnerability to conspiracy narratives and fake news, creating and disseminating misleading content on a large scale. This misinformation was capable of undermining public trust in government and bolstering extremist narratives, aiding non-state actor recruitment strategies (UNICRI, 2020). The spread of false information and propaganda was further intensified through the use of bots or social media "robots," leading to the development of chatbots. A study by Salge & Berente (de Lima Salge & Berente, 2017) estimated that around 23 million bots existed on Twitter, 140 million on Facebook, and 27 million on Instagram. Another report by Berger & Morgan (Berger & Morgan, 2015) indicated that groups like ISIS had demonstrated expertise in using social media bots to automate the dissemination of their propaganda.

One example of countering misinformation and disinformation spread by terrorists is seen in the efforts of the UK's intelligence and security organization, the Government Communications Headquarters (GCHQ). Utilizing AI, GCHQ automates fact-checking through validation of trusted sources to detect and block botnets and identify internet troll groups, often referred to as "troll farms" (GCHQ, 2021). Another initiative is by the journalism and technology company NewsGuard, which uses AI to assess the credibility of news and information sites and tracks online misinformation through a database of misinformation entries combined with natural language processing (NLP) and other machine learning tools (Stelter 2018; UNCCT & UNICRI, 2021).

While the detection of misinformation and disinformation spread by terrorists is not explicitly discussed in the Qur'an, several verses underscore the importance of *tabayyun*, or fact-checking, when receiving information before sharing it (Syarifudin, 2019). This is highlighted in the Qur'an in Surah Al-Hujurat [49]:6, *"O believers! If a wicked person comes to you with any news, verify it, so you do not harm people unknowingly and later regret what you have done."* The phrase fa tabayyanū, which is read in another *qirā'ah* (variant reading) as *"fa taśabbatū"* (Ma'rūf & Al-Ḥurastānī, 1994, p. Juz 6, 79), is interpreted by Imam Asy-Syaukani as the pursuit of knowledge, investigation, and truth-

seeking regarding received news. In other words, this verse instructs people to fact-check information before spreading it to avoid causing harm to others (Achmad, 2015). In the context of counter-terrorism, this verse serves as inspiration for detecting, fact-checking, and deeply investigating information disseminated by groups suspected or confirmed to be affiliated with terrorist organizations, which may contain disinformation or misinformation.

Moderation and Automatic Content Removal

One of the responses by social media companies to combat misuse of their platforms, particularly concerning terrorist and extremist content, is known as "deplatforming," which involves preventing and countering violations of their terms of service or community standards (Rogers, 2020). Additionally, there is the technique of "shadow-banning," where content is either fully removed or its visibility is significantly restricted, unbeknownst to the user who posted it (Savolainen, 2022; UNCCT & UNICRI, 2021).

It's important to note that curbing terrorist activity isn't always easy simply by deleting accounts or restricting content visibility. For instance, the perpetrators of the 2019 Christchurch terror attack live-streamed their assaults. Although Facebook managed to remove the original video 12 minutes after the broadcast ended, the video went viral, with 1.5 million attempts to upload copies of it across various sites worldwide within the next 24 hours (Macklin, 2019). This event serves as a reminder of the importance of not only being able to delete accounts and limit content visibility on a single platform but also of having the capability to operate across multiple platforms to promptly prevent the strategic distribution of terrorist content (UNCCT & UNICRI, 2021).

The spread of content that incites terror or encourages others to engage in extreme behavior is an evil act (Saul, 2005). Such harmful acts should be avoided, as harmful speech is clearly disliked by Allah, as reflected in the Quran, Surah An-Nisa [4]:148. According to Imam Mawardi, written words are equivalent to spoken words, with the only difference being the medium used for expression. In today's era, "written words" can be interpreted more broadly to mean "content" encompassing spoken words, written text, images, or videos. Thus, it is appropriate that harmful content should be removed from media, especially when it relates to terrorism and extremism, to prevent further widespread negative impact.

Counter-Narratives to Terrorism and Violent Extremism

In addition to identifying vulnerable individuals, NLP algorithms and machine learning need to play a more proactive role in combating online terrorism. AI can be used to analyze user behavior and guide them toward content that counters terrorist narratives (UNCCT & UNICRI, 2021). The potential for AI to counter terrorist narratives online is clear, especially when reaching at-risk individuals and groups. However, AI tools are only part of the solution. While AI can help connect the dots, a deeper understanding of individuals' pathways to radicalization, which these tools cannot fully

capture, is essential to effectively counter terrorist narratives online. Additionally, the significant role of civil society organizations and similar initiatives in this process cannot be overlooked (UNCCT & UNICRI, 2021).

An example of AI use for countering terrorism and violent extremism is the work done by Moonshot. Through its innovative "Redirect Method," Moonshot utilizes automated risk assessments and NLP to identify vulnerable audiences based on their online search behavior, simultaneously displaying counter-terrorism content via its algorithms (Shortland & McGarry, 2023). The London-based Institute for Strategic Dialogue, in collaboration with the Network Against Violent Extremism and supported by Facebook and Twitter, also employed AI-driven social media advertising tools to counter terrorist narratives online, launching curated counter-narrative campaigns in 2015 to address terrorist propaganda (Silverman et al., 2016).

As with other potential counter-terrorism measures in the AI era mentioned earlier, countering terrorism and violent extremism narratives is not directly addressed in the Qur'an. However, there are teachings in the Qur'an that align with the efforts to counter falsehood (Febriansyah, 2021), as in Qur'an, Surah An-Nahl [16]:125, *"Invite (all) to the Way of your Lord with wisdom and beautiful preaching; and argue with them in ways that are best and most gracious."* This verse suggests the importance of responding to false narratives with wisdom and constructive discourse, an approach that is aligned with the objectives of counter-narratives to terrorism and violent extremism. *"Wa jādilhum bi al-latī hiya aḥsan"* is interpreted by Al-Biqā'i as a directive to refute those who are entrenched in falsehood they believe and propagate, but to do so with kindness and in a constructive manner (al-Ḥasan Al-Biqā'ī, 1990). This concept can serve as a basis for countering terrorism by presenting counter-narratives to those spread by terrorist and extremist groups. For instance, this could involve reinterpreting verses on qitāl (fighting), which extremists have often misinterpreted to justify their acts of terror (Fawaid, 2019).

CONCLUSIONS, RECOMMENDATIONS, AND LIMITATIONS

The potential use of Artificial Intelligence (AI) in terrorism-related scenarios or acts leading to terrorism is a tangible reality. Various potential developments in terrorism through the utilization of AI include enhanced cyberattack capabilities, the use of autonomous weapons, the spread of false propaganda, data exploitation, disruption of critical infrastructure, and recruitment and deepening of radicalization through AI-supported algorithms. The scenarios involving the use of AI in counter-terrorism efforts and the Qur'an's response to these efforts are as follows: 1) predictive analysis of terrorist activities, aligning with the values contained in the Qur'an in Surah Al-Maidah [5: 32]; and 2) the identification of warning signs of radicalization, where radicalization leading to extremism contradicts the values found in the Qur'an in Surah Al-Baqarah [2: 143]. These first and second points are preventive measures in line with the Qur'anic teaching of *sadd aż-żarī'ah*; 3) detection of misinformation and disinformation spread by terrorists, in accordance with the values in Surah Al-Hujurat [49: 6]; 4) automatic

moderation and removal of content, aligning with the values in Surah An-Nisa [4: 148]; and 5) counter-narratives to terrorism and violent extremism, in line with the values found in Surah An-Nahl [16: 125].

The Indonesian government, particularly through the National Counterterrorism Agency (BNPT), has undoubtedly designed various scenarios to address the potential development of terrorism in the AI era, along with tactical steps for their implementation. However, considering that Indonesia is a nation that upholds religious values, it is only fitting that a more extensive religious approach be pursued as a preventive measure against the spread of terrorism in the country. Therefore, the involvement of religious figures becomes a strategic path in preventing the growth of terrorism from its very inception—since it is undeniable that terrorism often originates from extreme religious thoughts. This includes the involvement of Islamic scholars, given that the majority of Indonesians adhere to Islam. The anti-terrorism narratives, which reflect the spirit of the Qur'an as explained above, should be widely disseminated to ensure that no mindset normalizes extreme perspectives or actions that lead to terrorism.

REFERENCES

'Abdissalam, 'Izzuddin bin. (2003). *Syajārah al-Ma'ārif wa al-Aḥwāl wa Ṣāliḥ al-Aqwal wa al-A'māl*. Dār al-Kutub al-'Ilmiyyah.

Achmad, M. (2015). *Fatḥ al-Qādir Karya Al-Imam Al-Syaukani*. Universitas Islam Negeri Alauddin.

Ahdiat, A. (2023). *Tren Serangan Phishing Terus Meningkat, Capai Rekor Tertinggi pada 2022*. Databooks Katadata. https://databoks.katadata.co.id/datapublish/2023/05/17/tren-serangan-phishing-terus-meningkat-capai-rekor-tertinggi-pada-2022

al-Ḥasan Al-Biqā'ī, B. al-D. A. (1990). *Naẓm al-Durar fī Tanāsub al-Āyāt wa al-Suwar*. Dār al-Kutub al-Islāmī.

Al-Sa'di, 'Abd al-Rahman. (2006). *Tafsīr al-Sa'dī*. Dār al-Ḥaqq.

Bazarkina, D. (2023). Current and Future Threats of the Malicious Use of Artificial Intelligence by Terrorists: Psychological Aspects. In E. Pashentsev (Ed.), *The Palgrave Handbook of Malicious Use of AI and Psychological Security* (1st ed., pp. 251–272). Springer International Publishing. https://doi.org/10.1007/978-3-031-22552-9_10

Berger, J. M., & Morgan, J. (2015). *The ISIS Twitter Census: Defining and Describing The Population of ISIS Supporters on Twitter* (20). The Brookings Institution.

Brooke, N. (2022). What Are the Root Causes of Terrorism? In D. M. Tim Wilson (Ed.), *Contemporary Terrorism Studies* (1st ed., pp. 157–176). Oxford University Press.

Chakraborty, A., Biswas, A., & Khan, A. K. (2023). Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation. In Springer International Publishing (Ed.), *Artificial Intelligence for Societal Issues* (pp. 3–25). Springer International Publishing. https://doi.org/10.1007/978-3-031-12419-8_1

Conway, M., Khawaja, M., Lakhani, S., Reffin, J., Robertson, A., & Weir, D. (2019). Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts. *Studies in Conflict & Terrorism*, *42*(1–2), 141–160. https://doi.org/https://doi.org/10.1080/1057610X.2018.1513984

de Lima Salge, C. A., & Berente, N. (2017). Is That Social Bot Behaving Unethically? *Communications of the ACM*, *60*(9), 29–31. https://doi.org/10.1145/3126492

Denzin, N. K., & Lincoln, Y. S. (2018). Introduction: The Discipline and Practice of Qualitative Research. In N. K. Denzin & Y. S. Lincoln (Eds.), *The Sage Handbook of Qualitative Research* (5th ed., pp. 29–71). Sage Publications.

Dick, K., Russell, L., Dosso, Y. S., Kwamena, F., & Green, J. R. (2019). Deep Learning for Critical Infrastructure Resilience. *Journal of Infrastructure Systems*, *25*(2), 1–11. https://doi.org/10.1061/(ASCE)IS.1943-555X.0000477

Fawaid, A. (2019). *Kontra Narasi Ekstremisme terhadap Ayat-ayat Qital dalam Tafsir Al-Jalalain Karya Jalal al-Din al-Mahalli dan Jalal al-Din al-Suyuti (Kajian atas Pemahaman Kiai di Daerah Tapal Kuda Jawa Timur)*. Universitas Islam Negeri Sunan Ampel Surabaya.

Febriansyah, R. (2021). Implementasi Teori Psikologi Kognitif Ibnu Qayyim dalam Meluruskan Pernyataan Radikalisme di Indonesia. *Jurnal Intelektualita: Keislaman, Sosial, Dan Sains*, *10*(1), 1–5. https://doi.org/10.19109/intelektualita.v10i1.6376

GCHQ. (2021). *Pioneering a New National Security: The Ethics of Artificial Intelligence*. Government Communications Headquarters (GCHQ).

Gill, A. S. (2019). Artificial Intelligence and International Security: The Long View. *Ethics & International Affairs*, *33*(2), 169–179. https://doi.org/10.1017/S0892679419000145

Gürkaş-Aydin, Z., & Gürtürk, U. (2022). Cyber Threats and Critical Infrastructures in the Era of Cyber Terrorism. In Springer International Publishing (Ed.), *ICAIAME 2022: 4th International Conference on Artificial Intelligence and Applied Mathematics in Engineering* (pp. 274–287). Springer International Publishing. https://doi.org/10.1007/978-3-031-31956-3_23

Handayani, N., Ramadhani, R. Z., & Arrosyid, A. A. (2021). Information System Search for Verses of the Qur'an Based on the Background of the Surah. *Jurnal Teknik*, *10*(2), 105–118. https://doi.org/10.31000/jt.v10i2.5474

Hashim, Hanim, F., Abdullah, & Wan, W. N. (2017). Swarm Intelligence: From the Perspective of Al-Quran and Al-Sunnah to Natural and Artificial Systems. *Advanced Science Letters*, *23*(5), 4580–4585. https://doi.org/10.1166/asl.2017.8996

Hayward, K. J., & Maas, M. M. (2021). Artificial Intelligence and Crime: A Primer for Criminologists. *Crime, Media, Culture: An International Journal*, *17*(2), 209–233. https://doi.org/10.1177/1741659020917434

Horizon, E. U. (2020). *Real-time Early Detection and Alert System for Online Terrorist Content based on Natural Language Processing, Social Network Analysis, Artificial Intelligence and Complex Event Processing*. European Commission. https://doi.org/10.3030/740688

Ige, T., Kolade, A., & Kolade, O. (2023). Enhancing Border Security and Countering Terrorism Through Computer Vision: A Field of Artificial Intelligence. In Springer (Ed.), *Proceedings of the Computational Methods in Systems and Software* (pp. 656–666). Springer International Publishing. https://doi.org/https://doi.org/10.1007/978-3-031-21438-7_54

INSIKT-AI. (2018). *What are Social Media Companies Really doing to Combat Terrorism Online?* INSIKT AI. https://new.insiktintelligence.com/social-media-combatting-terrorism-online/

INSIKT AI. (2020). *RED-Alert Final Conference*. International Institute for Counter-Terrorism (ICT). https://insiktintelligence.com/red-alert-final-conference/

Jarrahi, M. H. (2018). Artificial Intelligence and the Future of Work: Human-AI Symbiosis

in Organizational Decision Making. *Business Horizons*, *61*(4), 1–10. https://doi.org/10.1016/j.bushor.2018.03.007

Johnson, J. (2019). Artificial Intelligence & Future Warfare: Implications for International Security. *Defense & Security Analysis*, *35*(2), 1–23. https://doi.org/10.1080/14751798.2019.1600800

Khairunnisa, B. W., & Rohman, A. (2018). Strategi Kepolisian Surabaya dalam Pencegahan Terorisme Pasca Ledakan Bom di Surabaya Tahun 2018. *Syiar Journal*, *2*(2), 162–177. https://doi.org/10.15642/siyar.2022.2.2.162-177

Ma'rūf, B. 'Awwād, & Al-Ḥurastānī, 'Iṣām Fāris. (1994). *Tafsīr aṭ-Ṭabarī min Kitābih Jāmi' al-Bayān 'an Ta'wīl al-Qur'ān*. Muassasaḥ al-Risālah.

Macklin, G. (2019). The Christchurch Attacks: Livestream Terror in the Viral Video Age. *CTC Sentinel*, *12*(6), 18–29.

Masakowski, Y. R. (2020). Artificial Intelligence and the Future Global Security Environment. In Y. R. Masakowski (Ed.), *Artificial Intelligence and Global Security* (1st ed., pp. 1–34). Emerald Publishing Limited. https://doi.org/10.1108/978-1-78973-811-720201001

McKendrick, K. (2019). *Artificial Intelligence Prediction and Counterterrorism* (The Royal Institute of International Affairs (ed.)). The Royal Institute of International Affairs.

Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative Research: A Guide to Design and Implementation* (4th ed.). Jossey-Bass.

Minchah, N. (2020). Perkembangan Teknologi Artificial Intelligence Cina: Ancaman dan Implikasinya terhadap Keamanan Nasional Amerika Serikat. *Jurnal Studi Diplomasi Dan Keamanan*, *12*(2), 56–75. https://doi.org/10.31315/jsdk.v12i2.3524

Mohadi, M., & Tarshany, Y. (2023). Maqasid Al-Shari'ah and the Ethics of Artificial Intelligence: Contemporary Challenges. *Journal of Contempory Maqasid Studies*, *2*(2), 79–102. https://doi.org/10.52100/jcms.v2i2.107

Nasiri, S., & Hashemzadeh, A. (2025). The Evolution of Disinformation from Fake News Propaganda to AI-driven Narratives as Deepfake. *Journal of Cyberspace Studies*, *9*(1), 229–250. https://doi.org/10.22059/jcss.2025.387249.1119

Phadke, S., & Mitra, T. (2021). Educators, Solicitors, Flamers, Motivators, Sympathizers: Characterizing Roles in Online Extremist Movements. In J. Nichols (Ed.), *Proceedings of the ACM on Human-Computer Interaction* (Vol. 5, Issue CSCW2, pp. 1–35). Association for Computing Machinery. https://doi.org/10.1145/3476051

Prasasti, G. D. (2023). *Waspada, Marak Penipuan Siber Bawa-Bawa Nama ChatGPT OpenAI*. Liputan 6. https://www.liputan6.com/tekno/read/5276827/waspada-marak-penipuan-siber-bawa-bawa-nama-chatgpt-openai

Punch, K. F. (1998). *Introduction to Social Research: Quantitative& Qualitative Approaches* (Sage Publications (ed.); 1st ed.). Sage Publications.

Rahman, S. N. M. A., & Ibrahim, A. (2019). Safety Plan and Control of Artificial Intelligence: Integrating Maqāṣid Al-Shari'ah, Hisbah and Tasawur as Mechanism. *Journal of Islamic, Social, Economics and Development (JISED)*, *4*(23), 1–8.

Ridwan, I., Hermawan, I., Sari, B. N., Komarudin, O., & Pardinand, A. (2023). Strategi Literasi Digital Berbasis Al-Qur'an dalam Program NgabuburIT Relawan TIK Karawang untuk Peningkatan Literasi Digital Masyarakat Karawang. *Jurnal Ilmiah Karawang*, *1*(1), 46–54.

Rogers, R. (2020). Deplatforming: Following Extreme Internet Celebrities to Telegram and Alternative Social Media. *European Journal of Communication*, *35*(3), 213–229. https://doi.org/10.1177/0267323120922066

Saihu, M. (2022). Al-Qur'an and The Need for Islamic Education to Artificial Intelligence.

Mumtaz: Jurnal Studi Al-Qur'an Dan Keislaman, *6*(1). https://doi.org/10.36671/mumtaz.v6i01.274

Saul, B. (2005). Speaking of Terror: Criminalising Incitement to Violence. *University of New Wales Law Journal*, *28*(3), 868–886. https://doi.org/10.3316/ielapa.114741244221161

Savolainen, L. (2022). The Shadow Banning Controversy: Perceived Governance and Algorithmic Folklore. *Media, Culture and Society*, *44*(6), 1091–1109. https://doi.org/10.1177/01634437221077174

Scharre, P. (2018). *Army of None: Autonomous Weapons and the Future of War* (1st ed.). W. W. Norton & Company.

Shortland, N., & McGarry, P. (2023). The Jigsaw Initiative: Theoretical and Practical Considerations for Preventing Harm from Extreme and Extremist Content Online. In D. Hummer & J. Byrne (Eds.), *Handbook on Crime and Technology* (1st ed., pp. 375–394). Edward Elgar Publishing.

Silverman, T., Stewart, C. J., Amanullah, Z., & Birdwell, J. (2016). *The Impact of Counter-Narratives: Insights from a Year-Long Cross-Platform Pilot Study of Counter-Narrative Curation, Targeting, Evaluation and Impact*.

Stelter, B. (2018). *This Start-Up Wants to Evaluate Your News Sources*. CNN Business. https://money.cnn.com/2018/03/04/media/newsguard-steven-brill-gordon-crovitz/index.html

Syarifudin, F. (2019). Urgensi Tabayyun dan Kualitas Informasi dalam Membangun Komunikasi. *Al-Kuttab: Jurnal Kajian Perpustakaan, Informasi, Dan Kearsipan*, *1*(2), 29–39. https://doi.org/10.24952/ktb.v1i2.1994

Tang, A. (2023). Active Learning Perspektif Wahyu Pertama dalam Al-Qur'an. *PAIDA: Jurnal Pendidikan Agama Islam UNIMUDA Sorong*, *2*(1), 148–155. https://doi.org/https://doi.org/10.36232/jurnalpaida.v2i1.1464

UNCCT, & UNICRI. (2021). *Countering Terrorism Online with Artificial Intelligence: An Overview for Law Enforcement and Counter Terrorism Agencies in South Asia and South-East Asia*.

UNICRI. (2020). *Stop the Virus of Disinformation: The Risk of Malicious Use of Social Media during COVID-19 and the Technology Options to Fight it*.

Weimann, G. (2015). *Terrorism in Cyberspace: The Next Generation*. Columbia University Press.

Wire, P. (2023). *2023, Serangan Ransomware Melonjak Dua Kali Lipat di Indonesia*. Antara News.

Zuhdi, N. (2023). *361 Juta Serangan Siber Masuk ke Indonesia Per Oktober 2023*. Media Indonesia. https://mediaindonesia.com/teknologi/630255/361-juta-serangan-siber-masuk-ke-indonesia-per-oktober-2023