INTERNATIONAL TERRORISM AND SOCIAL THREATS OF ARTIFICIAL INTELLIGENCE

Yaser Esmailzadeh

University of Tehran, Iran

Ebrahim Motaghi

University of Tehran, Iran

This article delves into the link between global terrorism and the growing dangers presented by Artificial Intelligence (AI). We examine how terrorism utilizes AI technologies, such as advanced deep learning algorithms like ChatGPT, to bolster their activities both on the internet and in the world. Additionally, we assess the possible advantages and obstacles of using AI to combat terrorism, emphasizing the ethical and legal dilemmas involved. The article discusses the importance of regulating, educating, and prioritizing ethical considerations in AI development to tackle issues like disinformation, privacy violations, and job displacement. It emphasizes the need for a comprehensive approach involving cooperation among various groups to tackle the challenges posed by AI-driven terrorism while advocating for human rights and social justice.

Keywords: *terrorism, international terrorism, Artificial Intelligence, social threats, the Middle East.*

Introduction

Terrorism has had a profound impact on the global landscape, notably over the past two decades, leading to a setback in economic development and societal advancement. As defined by the Global Terrorism Index (GTI), terrorism is delineated as the application or threat of physical force by non-state entities to coerce compliance and instill apprehension in targeted groups, thereby advancing the entity's political, economic, religious, or social agenda (Khan *et al.* 2023). With the advent and rapid adoption of sophisticated deep-learning models such as ChatGPT, there is growing concern that terrorists and violent extremists could use these tools to enhance their operations online and in the real world. Large language models have the potential to enable terrorists to learn, plan, and propagate their activities with greater efficiency, accuracy, and impact than ever before (Weimann *et al.* 2024: 17).

Humankind is in the midst of a technological revolution, no less significant than the Industrial Revolution of the eighteenth and nineteenth centuries – the Artificial Intelligence (AI) revolution. Henry Kissinger, who examined the challenges of the modern

Recommended citation: Esmailzadeh, Y., and Motaghi, E. International Terrorism and Social Threats of Artificial Intelligence. *Journal of Globalization Studies*, Vol. 15 No. 1, May 2024, pp. 168–179. DOI: 10.30884/jogs/2024.01.09.

world in light of the AI revolution, noted that this revolution and its implications will have no less impact than the historical effects of technological revolutions of the past (Kissinger 2018). Artificial intelligence, based on the advanced processing of big data via machine learning, is changing thought patterns and strategies in many different areas. The development of AI in combination with other technological advances, for example, in the field of robotics will probably lead to the elimination of various professions, such as professional drivers (given the development of the autonomous vehicle), accountants, pilots, and combat soldiers (Ganor 2021: 605).

Artificial Intelligence (AI) has rapidly gained prominence in recent years and has been extensively adopted in various fields, including finance, healthcare, and education, to name a few. The potential benefits of AI are vast, ranging from increased efficiency and productivity to improved decision-making capabilities. However, with the benefits of AI, there is also a growing concern about the potential threats it poses to society, particularly regarding international terrorism. As AI continues to evolve, the concern over its potential use in terrorist activities has been increasing, with security experts warning of the growing risk posed by terrorists using AI to carry out attacks.

There is a growing worry in the Middle East about the increase in social threats due to global terrorism utilizing advances in Artificial Intelligence. Terrorist groups are exploiting AI technologies to disseminate their propaganda on various online platforms. Through tools like chat-GPT, they aim to influence public sentiment and expand the impact of their attacks.

Terrorist groups are always finding new ways to harm and evade detection, making the world vulnerable to ongoing security threats. Technology advancements have allowed these groups to carry out attacks worldwide, leveraging social media for coordination and messaging. Additionally, there is growing fear of terrorists utilizing AI for enhancing their operations, like spreading propaganda and recruiting members.

However, AI also has the potential to be used in the fight against international terrorism. AI-powered predictive analytics can be used to identify potential terrorist threats by analyzing vast amounts of data, including social media posts, internet searches, and financial transactions. Real-time threat detection systems powered by AI can also help to prevent terrorist attacks by detecting suspicious behavior and alerting security agencies.

The potential of AI in the fight against international terrorism is significant. However, there are also concerns about the ethical and legal implications of using AI in counterterrorism efforts. For instance, the use of AI in surveillance raises concerns about privacy and civil liberties. Additionally, there is the risk of false positives, where innocent individuals are identified as potential threats, leading to unwarranted surveillance and intrusion into their private lives.

This article adds to the increasing research on the potential effects of artificial intelligence on global terrorism and the strategies to address it. It explores how terrorists might use AI and how AI can be used to prevent terrorist actions, shedding light on the intricate connection between AI and the different societal risks posed by global terrorism. The conclusions in this article are crucial for policymakers, security organizations, and researchers in the counterterrorism field. While AI has the potential to transform counterterrorism efforts, it also brings significant challenges. The article emphasizes the importance of more research in this area.

Literature Review

Artificial Intelligence (AI) has been touted as one of the most transformative technologies of the twenty-first century, with the potential to revolutionize a wide range of industries, from healthcare to finance to manufacturing. However, as with any powerful technology, there are also concerns about the potential risks and negative consequences that could arise from the misuse or abuse of AI.

Boaz Ganor (2021) highlights the emergence of a new revolution in counterterrorism that is driven by artificial intelligence (AI). The author explains that the use of AI and big data is having a significant impact on various aspects of security and intelligence, including the field of counterterrorism. However, there are intense debates between proponents and opponents of the use of AI and big data in counterterrorism. The author notes that this technology creates a delicate balance between effectiveness in the fight against terrorism and the preservation of liberal democratic values in society. The article suggests that the integration of AI and big data technologies in counterterrorism requires careful consideration of the ethical and legal implications to maintain the balance between security and individual rights.

Louis H. Bluhm (1987) focuses on the relationship between trust and terrorism. Bluhm argues that the development of civilization involves the evolution of complex trust mechanisms that allow individuals to interact, even if they are strangers. He identifies the predictability of consequences and an evaluation of consequences in terms of self-interest or values as key elements of trust, which can be enhanced by values, ethics, and norms. Bluhm asserts that terrorists destroy trust by introducing an unpredictable event that has negative consequences. However, he suggests that terrorist-like situations occur in day-to-day activities and that technology itself makes the world more interdependent and less predictable. Furthermore, technological 'accidents' and disasters, which are also unpredictable and negative, may prompt individuals to perceive technology as if it were a 'terrorist.'

Maria Stefania Cataleta's 2020 research delves into the relationship between artificial intelligence (AI) and human rights. She stresses the critical need to protect human rights as we increasingly depend on AI for autonomous decision-making. Cataleta particularly focuses on the application of AI in human surveillance, such as video surveillance and biometric tracking, which governments employ to prevent illegal and dangerous behaviors like international terrorism. While these technologies do make people's lives more secure and prevent criminal activity, they also monitor and track ordinary citizens, potentially violating individual privacy and leading to discrimination based on religious beliefs, health conditions, or political opinions. Cataleta further discusses how technological advancements, particularly in the nanotechnology sector, challenge the legal concept of a person. As the scientific and technological world increasingly encroaches on the already defined legal dimension of a person, Cataleta argues that this could have significant implications for human rights and how we define and protect them.

Kasapoğlu and Kırdemir's report (2019) is part of EDAM's contribution to the New Perspectives on Shared Security: NATO's Next 70 Years events. The report consists of four parts. The first part explains how current developments in artificial intelligence (AI) and robotics are likely to trigger a 'Cambrian Explosion' akin to the unprecedented bio-diversity that emerged millions of years ago. The second part discusses the short-term political implications of the AI revolution. The third part focuses on the 'geopoli-

tics of artificial intelligence' and the new great power competition that is emerging in this field. Finally, the fourth part presents an in-depth analysis of the evolving characteristics of armed conflicts and the future of warfare that AI-enabled technologies and concepts will bring. This section divides the battle space of network-centric warfare into physical, informational, and cognitive battlefields, and explores how each of these interacts with Artificial Intelligence.

The report by Jiang Tianjiao (2019), which is a part of EDAM's contribution to the *New Perspectives on Shared Security: NATO's Next 70 Years* events, covers several aspects of artificial intelligence (AI). The first part of the report explains how current developments in AI and robotics are likely to cause a 'Cambrian Explosion' that can bring about an unprecedented level of biodiversity similar to what happened millions of years ago. The second part of the report assesses the short-term policy implications of the AI revolution. The third part discusses the 'geopolitics of artificial intelligence' and the new great power competition that comes with it. The fourth part of the report provides an in-depth analysis of the evolving characteristics of armed conflicts and the future of warfare due to AI-enabled technologies and concepts. This section divides the battle space of network-centric warfare into physical, informational, and cognitive battlefields, and examines the interaction between each part and artificial intelligence. The fifth part of the report focuses on the transatlantic alliance's AI agenda and the future security environment in which allied leaders will have to operate. Finally, the report concludes with its findings and policy recommendations.

Alexander von Rosenbach (2021) discusses the cyberattack that occurred in May 2021 on the largest fuel pipeline in the United States, which was forced offline for nearly a week. The criminal gang responsible for the attack, called DarkSide, received a ransom payment of $4.4 million from the pipeline owners before normal operations were restored. However, the consequences of the attack were far-reaching, leading to gas shortages and economic disruption across the US Southeast and highlighting the vulnerability of critical national infrastructure in digitally enabled societies.

Liran Antebi (2021) discusses the significance of Artificial Intelligence (AI) as a groundbreaking technological field that can display intelligent behavior and create new insights and information. The article highlights that AI has the potential to impact various fields, including national security, and can be implemented efficiently and cost-effectively on a large scale. For Israel, AI is of utmost importance, given its economic strength, which largely relies on the high-tech industry, and Israel's leading position in AI development. The article also outlines the perceptual-technological areas of AI, including machine learning, deep learning, computerized vision, and natural language processing, and how these technologies are interrelated.

Lance Y. Hunter, Craig Albert, Josh Rutland, and Chris Hennigan (2022) discuss the emerging field of scholarship in Artificial Intelligence (AI) and computing, which suggests that AI has the potential to significantly impact the political and economic landscapes within states by reconfiguring labor markets, economies, and political alliances. This can lead to possible societal disruptions, which the study aims to examine in detail. The study explores the potentially destabilizing economic and political effects that AI technology can have on societies and the resulting implications for domestic conflict. The authors draw on research in the fields of political science, sociology, economics, and artificial intelligence to analyze the possible impact of AI on society.

1. AI-Enabled Recruitment and Radicalization

To comprehend security and global terrorism, we must acknowledge different risks and chances. The progressions in artificial intelligence (AI) suggest that this technology will have a significant effect on military power, strategic competition, and worldwide politics. An issue with AI concerning global terrorism is its capability to identify and enlist vulnerable individuals for extremist motives. AI algorithms can be used to analyze social media activity, identify individuals who may be receptive to extremist ideologies, and then target them with personalized messaging and content.

AI-enabled recruitment and radicalization refers to the use of AI algorithms and tools to identify and recruit individuals for extremist activities, including acts of international terrorism. The use of AI in recruitment and radicalization is of concern due to the potential for AI to identify and target vulnerable individuals with extremist messaging and propaganda, leading them to become radicalized and engage in violent activities.

AI can be utilized for recruitment and radicalization by analyzing social media activity. AI algorithms can scan social media posts to pinpoint individuals susceptible to extremist messaging, like those who have undergone life-altering events. By targeting these vulnerable individuals with personalized messaging, AI can compel them to participate in extremist activities.

Artificial intelligence has the ability to be utilized in recruitment and radicalization strategies through the use of chatbots and conversational agents. By engaging in conversations with individuals on social media platforms, these tools can gradually expose them to extremist materials. This approach is particularly successful in targeting susceptible individuals who may be isolated and susceptible to outside influences.

In addition to recruitment, AI can also be used for radicalization, or the process of reinforcing extremist beliefs and encouraging individuals to engage in violent activities. AI algorithms can be used to analyze social media activity and identify individuals who are already sympathetic to extremist ideologies. These individuals can then be targeted with personalized messaging that reinforces their beliefs and encourages them to take action.

The use of AI for recruitment and radicalization raises several ethical and legal concerns. For example, there are questions about the use of personal data in the recruitment process, and whether the use of AI to target vulnerable individuals for extremist activities constitutes a form of psychological manipulation or coercion. There are also concerns about the potential for AI to be used to create deepfakes or other forms of manipulated content that could be used to further radicalize individuals.

To address these concerns, it is important to develop ethical guidelines and best practices for the use of AI in recruitment and radicalization. These guidelines should address issues such as data privacy, transparency, and accountability, and should be developed in collaboration with experts in the fields of AI, psychology, and counterterrorism. Additionally, it is important to develop counter-narratives and other strategies to counteract the messaging and propaganda of extremist groups and to provide support and resources to individuals who have been targeted by these groups.

Overall, the use of AI for recruitment and radicalization is a complex and challenging issue that requires careful consideration and attention from researchers, policymakers, and practitioners. While AI has the potential to be a powerful tool in the fight

against terrorism, it is important to recognize the potential risks and challenges associated with its use to develop strategies to mitigate these risks and ensure that AI is used ethically and responsibly.

2. AI-Enabled Planning and Coordination of Attacks

As an enabler and force multiplier of a broad range of military capabilities, AI is more akin to electricity, radio, radar, and C4ISR systems, than a 'weapon' per se (Johnson 2018). As a new and potentially more powerful class of technology, AI could redefine and transform the status quo in military-use technology with unpredictable and likely highly destabilizing strategic implications (Johnson 2019: 150).

Another potential social threat is the use of AI to plan and coordinate terrorist attacks. AI algorithms could be used to analyze data on potential targets, identify vulnerabilities and weak points, and develop attack plans that are tailored to maximize the impact of the attack. One way in which AI is being used to facilitate terrorist attacks is through the creation of autonomous weapons systems. These systems can identify and Attack targets without human intervention, making them particularly effective in asymmetric warfare situations. Autonomous weapons systems can be programmed to detect and respond to specific stimuli, such as the presence of a particular individual or group, and can be equipped with advanced sensors and weapons to carry out attacks with precision and efficiency. Another way in which AI is being used to facilitate terrorist attacks is through the development of deepfake technology. Deepfakes are highly realistic digital forgeries that use AI algorithms to manipulate images, video, and audio recordings to create false or misleading content. Terrorist groups can use deepfakes to spread propaganda, manipulate public opinion, and even carry out attacks by creating fake video or audio recordings that incriminate or discredit their enemies.

Moreover, AI can also be used to bypass security measures and evade detection by law enforcement agencies. For example, AI-powered malware can be used to infiltrate computer networks and steal sensitive information, while AI-based phishing attacks can be used to trick individuals into revealing their personal information or login credentials. Additionally, AI can be used to analyze large amounts of data and identify vulnerabilities in security systems that can be exploited by terrorists.

To counter these threats, law enforcement agencies and other stakeholders must work to develop new strategies and technologies that can keep pace with the rapid evolution of AI-enabled terrorism. This includes investing in advanced technologies such as machine learning and computer vision, as well as developing new detection and response protocols that can quickly identify and neutralize emerging threats.

One promising approach is the use of AI algorithms to analyze social media and other online platforms for signs of radicalization and potential terrorist activity. By monitoring online behavior patterns and identifying key indicators of radicalization, law enforcement agencies can intervene early to prevent individuals from becoming involved in terrorist activities.

Overall, the use of AI for coordinating and executing terrorist attacks poses a significant threat to global security. As the technology continues to evolve and become more sophisticated, stakeholders must work together to develop effective countermeasures and safeguard against the malicious use of AI by terrorist groups.

3. AI-Enabled Dissemination of Propaganda

The issues of authoritarianism, propaganda, and political montage seem to be part of a contemporary worldwide phenomenon (Rojas 2022: 262) AI algorithms can also be used to disseminate propaganda and extremist messages on a large scale. By analyzing social media and other online platforms, AI algorithms can identify individuals who are most likely to be receptive to extremist messaging and target them with personalized content that is designed to reinforce their beliefs and encourage them to engage in violent activities.

One of the main challenges faced by government counter-terrorism policies is the need for realistic threat evaluations. One of the most relevant indicators in such analysis is the propaganda activity of terrorist organizations. Terrorist groups use their public communications not only to reiterate their demands and attempt to legitimize their existence and actions but also to distribute a wealth of information about their objectives and priorities. Propaganda thus becomes a prime indicator for calibrating the extent of the terrorist threat (Torres-Soriano 2020: 365).

AI-powered bots and algorithms can be used to create and disseminate propaganda and disinformation campaigns across a wide range of digital platforms, including social media, messaging apps, and online forums. These campaigns can be designed to target specific demographics, manipulate public opinion, and spread false or misleading information.

A key advantage of AI-powered propaganda and disinformation campaigns is their ability to operate at scale and with minimal human oversight. AI algorithms can be programmed to automatically generate and distribute content based on pre-defined parameters, allowing terrorist groups to rapidly spread their message and reach a wider audience than ever before.

AI can also be used to enhance the effectiveness of propaganda and disinformation campaigns by analyzing and responding to user engagement metrics in real time. By tracking how users interact with specific types of content, AI algorithms can adjust the messaging and delivery of propaganda to maximize its impact and influence.

To counter these threats, researchers and technologists are developing new approaches to detecting and combating AI-generated propaganda and disinformation. This includes using machine learning algorithms to analyze large volumes of online content and identify patterns and anomalies that may indicate the presence of propaganda or disinformation campaigns.

Another promising approach is the development of digital forensic tools that can detect deepfake videos and images. These tools use advanced AI algorithms to analyze the visual and auditory characteristics of media content and identify signs of manipulation or forgery.

Researchers are also exploring the use of counter-narratives and other forms of digital media to counter the influence of extremist propaganda. By creating and disseminating content that promotes positive values and messages, such as tolerance and inclusion, researchers can help undermine the appeal of extremist ideologies and prevent individuals from becoming radicalized.

Overall, the use of AI for propaganda and disinformation campaigns poses a significant threat to global security and social stability. As the technology continues to evolve

and become more sophisticated, stakeholders must work together to develop effective countermeasures and safeguard against the malicious use of AI by terrorist groups.

4. AI-Enabled Cyberattacks

The cost of cyber-attacks is enormous and it increases every year. A 2016 report estimated that cybercrime would cost the world $6 trillion annually by 2021, a significant increase from the $3 trillion in 2015. 'This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined' (Marks 2020). Moreover, this prediction has been confirmed by hundreds of major media outlets, academics, senior government officials, associations, industry experts, the largest technology and cybersecurity companies, and cybercrime fighters globally (Norris and Mateczun 2023: 2).

Another potential social threat of AI in the context of international terrorism is the use of AI to carry out cyberattacks on critical infrastructure and other targets. AI algorithms can be used to identify vulnerabilities in networks and systems and to develop targeted attacks that are difficult to detect and defend against.

AI has the potential to significantly enhance the capabilities of cyber attackers, allowing them to launch more sophisticated and targeted attacks against critical infrastructure, governments, and businesses. AI algorithms can be used to scan and analyze large amounts of data, identify vulnerabilities and weaknesses in software and networks, and develop tailored attack strategies. This can include using machine learning to identify patterns and weaknesses in security protocols and devising strategies to circumvent or exploit these vulnerabilities. One of the most worrying aspects of AI-enabled cyberattacks is the potential for these attacks to be fully automated, allowing attackers to launch large-scale, coordinated attacks with minimal human involvement. This could lead to devastating consequences, such as the disruption of critical infrastructure systems, stealing sensitive data, and compromising national security. In addition to the use of AI in offensive cyber operations, AI is also being used by defenders to detect and prevent attacks. This includes the use of machine learning algorithms to identify anomalous network traffic patterns and detect new and emerging threats. However, the use of AI in cybersecurity is a double-edged sword. While it can enhance the capabilities of defenders, it can also be used by attackers to evade detection and bypass security measures. For example, attackers could use AI to generate sophisticated and realistic phishing emails or to create fake digital identities that are difficult to detect.

To address these threats, researchers and security professionals are exploring new approaches to cybersecurity that incorporate AI and machine learning. This includes the development of AI-based threat intelligence platforms that can analyze large amounts of data to identify emerging threats and vulnerabilities. In addition, researchers are exploring the use of AI-based deception techniques, such as honey pots, to trick attackers into revealing their tactics and techniques. This can help defenders to understand better the tactics and techniques used by attackers and develop more effective countermeasures.

Overall, the use of AI in cyberattacks presents a significant threat to global security and requires ongoing research and development of effective countermeasures. Stakeholders must work together to develop new approaches to cybersecurity that incorporate AI-based technologies, while also addressing the potential risks and vulnerabilities that these technologies pose.

5. AI-Enabled Surveillance and Monitoring

The field of violence, political violence, and conflict prevention is about to face an upheaval as it confronts renewed questions about its capacity to analyze data, mitigate risks, and exert normative leadership in an era of converging security threats. The threats to human rights and security triggered by Artificial Intelligence (AI) and data collection technologies will require peacebuilding and violence prevention actors to bridge the gap between early warning and response and to anticipate new challenges (Pauwels 2020: 1). In this context, political violence is considered as the root cause of issues such as international terrorism and violent conflicts in the world. AI is the focus of much controversial discussion, including among scholars and policymakers in Europe and beyond, often without a clear understanding of what makes it distinctive. It is variously described as 'the technology of the future,' an already widely used 'general purpose technology,' a particular 'key technology,' or a 'set' of quite diverse technologies. Such different conceptions and definitions do not just prompt academic debates. How we define AI matters, inter alia for the rights of stakeholders: when laws and regulations assign specific rights and obligations to AI users (and others affected by the use of AI), those rights depend on what is considered an AI application or system (Büthe *et al.* 2022).

There is a concern that AI could be used to conduct mass surveillance and monitoring of individuals and groups. AI algorithms can be used to analyze large amounts of data from social media, CCTV cameras, and other sources, to identify potential threats and monitor the activities of individuals and groups. This could have a chilling effect on civil liberties and privacy and could be used to target individuals and groups based on their beliefs or affiliations.

AI can be used to create and distribute targeted messages across a wide range of digital platforms, including social media, news websites, and messaging apps. This can be used to spread false information, incite violence, and manipulate public opinion in support of terrorist organizations or their agendas.

AI algorithms can be used to identify and target vulnerable populations, such as individuals who are already predisposed to extremist views or are susceptible to manipulation. These algorithms can analyze vast amounts of data from social media platforms, search engines, and other sources to identify individuals who may be receptive to terrorist messaging. Once identified, AI can be used to create tailored messages that appeal to these individuals' beliefs, interests, and emotions. This can include the use of deepfake technology to create convincing audio and video content that is difficult to distinguish from real footage. In addition to creating and disseminating propaganda, AI can also be used to manipulate public opinion through the use of bots and other automated tools. These tools can be used to create the impression of widespread support for terrorist organizations or their causes or to amplify the reach of extremist messaging across social media platforms.

One of the key challenges in addressing the threat of AI-enabled propaganda is the sheer volume and complexity of the data involved. AI algorithms can analyze and process vast amounts of data at high speeds, making it difficult for human analysts to keep up.

To address this challenge, researchers are developing new approaches to detecting and countering AI-enabled propaganda. This includes the development of AI-based tools that can detect and identify false information and deep fakes, as well as tools that can analyze social media activity in real-time to identify and counter the spread of ex-

tremist messages. Another key challenge is to balance the need for effective countermeasures with the need to protect freedom of expression and other fundamental democratic values. Governments and other stakeholders must be careful not to overreact to the threat of AI-enabled propaganda and inadvertently undermine the principles of free speech and open debate that are essential to a healthy democracy.

Overall, the use of AI in the dissemination of propaganda and the manipulation of public opinion poses a significant threat to global security and requires ongoing research and development of effective countermeasures. Stakeholders must work together to develop new approaches to counter AI-enabled propaganda that are both effective and respectful of democratic values.

Conclusion

The convergence of Artificial Intelligence (AI) and data capture technologies has powerful implications for the changing nature of conflicts and the global security landscape, including about violent extremism and international terrorism (Pauwels 2020: 1). On the one hand, AI can help identify and prevent terrorist activities by analyzing vast amounts of data from various sources, such as social media and surveillance systems. This can help security agencies respond to threats more quickly and efficiently, potentially saving lives and preventing harm to communities. However, the use of AI in addressing the social threats of international terrorism also has potential risks that need to be addressed.

In addition, concerns regarding the potential misuse of artificial intelligence (AI) in counter-terrorism efforts are significant and prevalent in various regions worldwide, including the Middle East. For example, the use of AI in profiling and targeting individuals or groups based on their online behavior raises concerns about privacy and civil liberties. In addition, the reliability and accuracy of AI systems in identifying and predicting terrorist threats remain in question, and there are concerns about the potential for false positives and the exacerbation of bias and discrimination.

Therefore, it is essential to approach the use of AI in counter-terrorism efforts with caution and consideration of the potential ethical implications. The development and deployment of AI systems should involve transparency, accountability, and rigorous testing and evaluation to ensure that they are reliable, accurate, and fair. It is also crucial to involve different stakeholders in the development and implementation of AI systems to ensure that the technology is used in ways that are consistent with ethical, legal, and human rights standards.

Furthermore, while AI can play a vital role in identifying and preventing terrorist threats, it cannot address the underlying social and political factors that drive extremism and international terrorism. Addressing these factors requires a more comprehensive approach to addressing inequality, discrimination, and political grievances. Therefore, it is essential to view the use of AI in counter-terrorism efforts as part of a broader strategy that involves engaging with affected communities, addressing the root causes of violence, and promoting social cohesion and inclusion.

In summary, the use of Artificial Intelligence in counter-terrorism efforts has potential benefits and risks. While AI can help identify and prevent terrorist threats, it is crucial to approach its development and use with caution and consideration of the potential ethical implications. It is also important to view AI as part of a broader strategy that

addresses the underlying social and political factors that drive extremism and terrorism. Ultimately, the responsible use of AI in counter-terrorism efforts requires a holistic approach that balances security with privacy, human rights, and social justice.

While the development of AI has brought significant benefits and advancements to many fields, it has also created new social threats that must be addressed. Some of the main social threats resulting from AI include the spread of disinformation, the loss of privacy, the potential for job displacement, and the use of AI in terrorist activities. To reduce these threats, several suggestions and solutions can be implemented, including the following:

- Increased regulation: One of the most effective ways to reduce the social threats posed by AI is through increased regulation. Governments and organizations should work together to establish clear guidelines and regulations for the development and use of AI. This can help to prevent the spread of disinformation, protect individual privacy, and limit the use of AI for malicious purposes.
- Education and awareness: Another important solution is to increase education and awareness about AI and its potential social impacts. This can be done through educational programs, public awareness campaigns, and media coverage. By educating people about the potential risks and benefits of AI, individuals, and organizations can make more informed decisions about its use.
- Ethical considerations: In addition, ethical considerations should be taken into account when developing and using AI. These include considerations around bias and discrimination, transparency and accountability, and the potential for AI to harm human values and interests. By prioritizing ethical considerations, organizations and individuals can work to ensure that AI is developed and used responsibly and beneficially.
- Collaboration: Collaboration between governments, organizations, and individuals is also important for reducing the social threats posed by AI. By working together, stakeholders can share information, resources, and expertise to develop effective solutions and strategies for addressing the social impacts of AI.
- Developing countermeasures: Finally, it is important to develop countermeasures to address the potential use of AI in terrorist activities. This includes investing in research and development to detect and prevent the use of AI for malicious purposes, as well as working to develop effective response strategies in the event of an AI-enabled terrorist attack.

Disclosure Statement

This postdoctoral research conducted at the University of Tehran was financially supported by the Research Institute for Strategic Studies (RISS).

REFERENCES

Antebi, L. 2021. *Artificial Intelligence and National Security in Israel*. Institute for National Security Studies. URL: http://www.jstor.org/stable/resrep30590.

Bluhm, L. H. 1987. Trust, Terrorism, and Technology. *Journal of Business Ethics* 6 (5): 333–341. URL: http://www.jstor.org/stable/25071669

Büthe, T., Djeffal, C., Lütge, C., Maasen, S. and Ingersleben-Seip N. V. 2022. Governing AI – attempting to Herd Cats? Introduction to the special issue on the Governance of Artificial Intelligence. *Journal of European Public Policy* 29 (11): 1721–1752. DOI: 10.1080/13501763.2022.2126515.

Cataleta, M. S. 2020. *Humane Artificial Intelligence: The Fragility of Human Rights Facing AI*. East-West Center. URL: http://www.jstor.org/stable/resrep25514.

Ganor, B. 2021. Artificial or Human: A New Era of Counterterrorism Intelligence? *Studies in Conflict and Terrorism* 44 (7): 605–624.

Hunter, L. Y., Albert, C. Rutland, J. and Hennigan, C. 2022. *The Fourth Industrial Revolution, Artificial Intelligence, and Domestic Conflict*. Global Society.

Johnson, J. 2018. *The US-China Military and Defense Relationship during the Obama Presidency*. New York: Palgrave Macmillan.

Johnson, J. 2019. Artificial Intelligence and Future Warfare: Implications for International Security. *Defense and Security Analysis* 35 (2): 147–169.

Kasapoğlu, C., and Kırdemir, B. 2019. *Wars of None: Artificial Intelligence and the Future of Conflict*. Centre for Economics and Foreign Policy Studies. URL: http://www.jstor.org/stable/resrep21050.

Khan, F. A., Li, G., Khan, A. N., Khan, Q. W., Hadjouni, M., and Elmannai, H. 2023. AI-Driven Counter-Terrorism: Enhancing Global Security through Advanced Predictive Analytics. *IEEE Access* 11 (1): 135864–135879. doi: 10.1109/ACCESS.2023.3336811.

Kissinger, H. 2018. How the Enlightenment Ends. *The Atlantic*, June. URL: https://www.theatlantic.com/magazine/archive/2018/06/henry-kissinger-ai-could-mean-the-end-of-human-history/559124/.

Marks, J. 2020. The CyberSecurity 202: A Russian Mega-Hack is Further Damaging Trump's Cybersecurity Legacy. *Washington Post*, December 14. URL: https://www.washingtonpost.com/politics/2020/12/14/cybersecurity-202-russian-mega-hack-is-further-damaging-trumps-cybersecurity-legacy/.

Norris, D. F., and Mateczun, L. K. 2023. Cyberattacks on Local Governments 2020: Findings from a Key Informant Survey. *Journal of Cyber Policy*. DOI: 10.1080/23738871.2023.2178319.

Pauwels, E. 2020. *Artificial Intelligence and Data Capture Technologies in Violence and Conflict Prevention*. Global Center on Cooperative Security. URL: https://www.jstor.org/stable/resrep27551.

Rojas, J. A. D. V. 2022. Propaganda and Authority in José Ricardo Morales' Play *Los Culpables* (1964): A Connection with the Chilean Context. *Canadian Journal of Latin American and Caribbean Studies / Revue canadienne des études latino-américaines et caraïbes* 47 (2): 261–279.

Rosenbach, A. V. 2021. Fighting Fear and the Future of Technology-Enabled Terrorism. *Atlantisch Perspectief* 45 (3): 31–35. URL: https://www.jstor.org/stable/48638243.

Tianjiao, J. 2019. The Impact of Military Artificial Intelligence on Warfare. In Saalman, L. (ed.), *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk: Volume II East Asian Perspectives*. Stockholm International Peace Research Institute. URL: http://www.jstor.org/stable/resrep24532.15.

Torres-Soriano, M. R. 2020. Jihadist Propaganda as a Threat Indicator: The Case of Spain. *Terrorism and Political Violence* 32 (2): 365–381.

Weimann, G., Pack, A. T., Sulciner, R., Scheinin, J., Rapaport, G., and Diaz, D. 2024. Generating Terror: The Risks of Generative AI Exploitation. *CTCSENTINEL* 17 (1): 17–24.