ANNALS OF THE "CONSTANTIN BRÂNCUȘI" UNIVERSITY OF TÂRGU JIU
LETTER AND SOCIAL SCIENCE SERIES

ISSN-P: 1844-6051 ~ ISSN-E: 2344-3677

1/2023 ***https://alss.utgjiu.ro***

CONSIDERATIONS ON THE IMPACT OF ARTIFICIAL INTELLIGENCE ON TERORISM

Cătălin PEPTAN

Lecturer PhD., „Constantin Brâncuși" University of Târgu Jiu

Cosmin GAVRILĂ

Master graduate on Global Security Studies, Faculty of Political Science, Philosophy and Communication Sciences, West University of Timisoara

Letiția SÎRBU

Master graduate on Global Security Studies, Faculty of Political Science, Philosophy and Communication Sciences, West University of Timisoara

Flavius Cristian MĂRCĂU

Lecturer PhD., „Constantin Brâncuși" University of Târgu Jiu

Abstract: *THE STUDY AIMS TO HIGHLIGHT THE IMPACT OF ARTIFICIAL INTELLIGENCE (AI) ON THE PHENOMENON OF TERRORISM, SEEN FROM THE PERSPECTIVE OF THE OPPORTUNITIES OFFERED BOTH TO TERRORIST ENTITIES, ON VARIOUS LEVELS OF THEIR CONCERNS, AND TO STRUCTURES SPECIALIZING IN KNOWLEDGE, PREVENTION AND COUNTERACTION.*
THE CURRENT LEVEL OF KNOWLEDGE SHOWS THAT THE USE OF AI CAN GENERATE SIGNIFICANT RISKS AND DANGERS TO INDIVIDUAL AND COLLECTIVE SECURITY AS A RESULT OF THE REDUCTION OF HUMAN CONTROL OVER ITS LETHAL FORCE AND, THEREFORE, THE ATTRIBUTION OF RESPONSIBILITY FOR POSSIBLE UNCONTROLLED ACTIONS TAKEN.
GIVEN THE ETHICAL AND LEGAL ISSUES RAISED BY THE USE OF AI, THERE IS A NEED FOR POLICY MAKERS AND EXPERTS IN THE FIELD TO DEVELOP EFFECTIVE STRATEGIES TO MITIGATE THE RISKS AND HARNESS THE POTENTIAL BENEFITS OF AI IN THE FIGHT AGAINST TERRORISM.

Keywords: ARTIFICIAL INTELLIGENCE, SECURITY, TERRORISM, RISK, THREAT, DANGER, OPPORTUNITY

Contact details of the author(s): Email: catalinpeptantm@gmail.com; soryn_g@yahoo.com; letty_sirbu07@yahoo.com; flaviusmarcau@yahoo.com

ISSN-P: 1844-6051 ~ ISSN-E: 2344-3677

1/2023 ***https://alss.utgjiu.ro***

1. INTRODUCTION

At the beginning of the third millennium, terrorism continues to be perceived as a premeditated action by an individual or collective entity, aimed at the intentional use of violence against categories of people, usually civilians and non-combatants, to create fear and exert pressure on powerful groups, including government decision-makers, in order to achieve certain political goals (Schmid, 2012, pp. 158-159). Over time, the forms of terrorism have diversified, from the simplest attacks with bladed weapons or improvised explosive devices to sophisticated cyber attacks (Peptan, 2019, pp. 132-134) that are operated through the facilities of Artificial Intelligence, abbreviated as AI (Uppal, 2022).

AI has exceptional potential to both alter and transform the way terrorist organizations operate today and the knowledge, prevention and countermeasure response of state and international authorities to such threats. Thus, on the one hand, terrorists can use AI to automate specific tasks such as information gathering, propaganda and recruitment, as well as to develop more sophisticated tools, funding and operational modalities or tactics. All of these are subsumed under the goal of increasing the performance of actions taken. On the other hand, state and international authorities with responsibilities in the field can use AI to ensure effective action possibilities to fight terrorism. Capturing/gathering and analyzing large amounts of data, from social networks and other online sources, through the use of AI, can lead to the identification of suspicious persons, physical locations suspected of being used by terrorist groups and the detection of action patterns of their members, contributing significantly to the early prevention of terrorist attacks, as well as to providing a pragmatic and effective response to terrorist threats (West & Allen, 2018).

In general, the use of AI by terrorists and/or by institutions specialised in knowledge, prevention and countermeasures is a complex and evolving issue that raises important ethical and legal questions, many of which are still unresolved (Bringsjord & Govindarajulu, 2018). As AI technology continues to advance, it will be important for policy makers and experts in the field to develop effective strategies to mitigate the risks and harness the potential benefits of AI in the fight against terrorism.

The motivation for choosing the topic is based on the desire to understand the functionality of AI, a rapidly developing technology with a significant impact on different areas of society, and its impact on the phenomenon of terrorism, in the context of the fact that it generates major threats to global security. The combination of these two issues, AI and terrorism, shows the importance of debate and awareness of the implications that AI can have on terrorist activities.

The research hypothesis starts from the fact that the use of AI for terrorist purposes has a significant impact on the way terrorist organisations recruit, plan and carry out attacks, increasing efficiency and causing significant risks and threats to global security. The use of AI for terrorist purposes can generate new risks and threats. It is important to explore and understand these risks in order to provide a set of data that could underpin the development of appropriate policies and solutions to prevent and combat terrorism by specialised institutions.

The research methodology is based on empirical research as follows: 1) Literature review - a stage in which rigorous literature searches were conducted to identify and analyse recent works and studies addressing the topic of the impact of AI on terrorism; 2) Data and information collection - a stage in which relevant data were obtained through documentary research, interviews with experts in the field and analysis of case studies. Data of interest was obtained on the use of AI by terrorist organisations, the technologies involved and the impact on malicious activities, as well as the opportunities offered to institutions specialised in combating the phenomenon; 3) Analysis and impact assessment of AI - a stage based on the analytical method, in order to assess how AI can be used by terrorist organisations and, in particular, its impact on terrorism in the process of recruitment, propaganda, planning and execution of attacks, etc.; 4) Assessment of ethical and legal risks and

implications - this stage analysed the possible consequences of the use of AI in terrorist activities on security, human rights, privacy, etc.

2. ASPECTS RELATING TO THE NATURE OF ARTIFICIAL INTELLIGENCE INFLUENCES ON TERRORISM

The impact of AI technology on terrorism is an important and topical issue, given the significant effects this technology can have on some of the vectors of global security threats. The use of AI technology by terrorist groups may amplify the threat they currently pose, making terrorist activity increasingly difficult for terrorist institutions to know, prevent and counter, despite the institutional efforts undertaken.

We believe that the analysis of the nature of AI influences on terrorism must be analyzed on two levels. The first level to be addressed in the context of the use of AI technology by terrorist groups is to fully understand the potential threats and additional risks that can be associated with this phenomenon, by the technology itself. In recent years, the use of AI technology has increased significantly, and this rapid development has raised a number of concerns regarding the effects on global security. Thus, in the context of the manifestation of the terrorist phenomenon, there is a concern that terrorist organisations could use AI technology to develop more sophisticated action tactics and weapons to use in future attacks (van der Veer, 2019). Beyond the facilities of AI in terms of information collection, propaganda, recruitment of followers or financing methods (which will be detailed in the next chapter), the opportunities offered to terrorism in terms of the operationalization of the actions undertaken are eloquent. Such is the case with autonomous robots or drones that can be used by terrorist organizations to carry weapons or detonate dangerous explosives within their perimeters (Uppal, 2022). One such organization is ISIS, which since 2014 has used autonomous drones to attack various targets in northern Iraq, seeing this technology as a new source causing casualties for apostates (Warrick, 2017).

On the other hand, the second level of analysis of the influences of AI on terrorism must re-focus on the use of AI technology in the fight against terrorism, which can bring a variety of benefits through its ability to quickly and efficiently collect, analyze and synthesize a large amount of data, to identify suspicious persons and their action patterns (Uppal, 2022), as well as to monitor in real time suspicious locations of terrorist entities (see the "Maven" project, designed by the US authorities, used to identify people and objects through automated processing of video images) (A.D., 2022) and act with particular precision to neutralise them. These opportunities are exploited by specialised intelligence analysis departments within intelligence structures (Peptan, 2021, pp. 91-104), which support the efforts of operational departments in the fight against the scourge of terrorism. AI technology can also be used to identify the degree of radicalisation of members of terrorist groups and the aggressive intentions of terrorist organisations, as well as to predict the incidence of terrorist attacks (McKendrick, 2019, p. 19). It should be noted that the use of AI technology in the process of countering terrorism raises numerous ethical and legal issues (Bringsjord & Govindarajulu, 2018) that require regulatory policies.

3. HOW TERRORISTS EXPLOIT ARTIFICIAL INTELLIGENCE

The facilities offered to terrorism by AI are at the root of terrorist entities' efforts to develop using the latest technological developments, the increasing availability of these technologies and the recognition of the potential benefits of AI across the spectrum of terrorist group activities, from securing human resources to the operationalization of terrorist attacks. In this context, terrorists are increasingly using AI technology to further their goals, from propaganda and recruitment to planning, financing and carrying out terrorist attacks (UNICRI, 2021).

In terms of propaganda, terrorist groups use AI technology to create and disseminate ideas and concepts that promote their ideology and goals. One such way is to use AI algorithms to analyse social media data or identify potential targets. These algorithms have the ability to create personalized content that is attractive and resonates with their targets in order to manipulate and persuade them (through misinformation, false perception, distraction, disorientation, etc.) to adhere to their ideology (Benkler, Roberts, 2018, pp. 30-39). In addition, AI technology can be used to manipulate images and videos, creating content that appears authentic but disseminates false or exaggerated information. In recent years, the internet has been taken by storm by "deep-fake" videos (technology based on deep learning to generate audio/video recordings with a real profile that do not actually exist), which have become increasingly sophisticated, so that internet users can be more easily manipulated by various entities with dangerous intentions. Therefore, the phenomenon of "deep-fake" videos has been called by experts "the most serious threat created by AI technology" (Greaves, 2020), as this phenomenon can spread very easily on social media platforms.

Terrorist groups also use AI technology to recruit new members from the most diverse geographical areas of the world. AI-based chatbots can be used to engage in various dialogues with potential recruits and answer their questions, influencing their behaviour. These chatbots can also analyse the content of conversations to identify potential motivational constellations of people likely to join the group. In addition, social media algorithms can be used to select people who have expressed interest in topics related to the group's ideology and target them with personalized messages (McLay, n.d, p. 4). Thus, terrorist groups have also started to use various social media platforms with end-to-end encryption, allowing them to communicate in a private and secure way (IBM, n.d-a), without being intercepted by authorities. In a recent study analyzing the Islamic State's activity on the social media platform called Telegram, it was found that between February 1 and September 30, 2021, the Islamic State had chatbots posting, on average, 176 messages each day, identifying three basic functions of chatbots: content distribution, group management (blocking spammers and deleting messages), and last but not least, gatekeeping, i.e. allowing users to join or share various links (Alrhmoun, Winter & Kertesz, 2023, pp. 7-9). From another point of view, terrorist organisations can exploit the advantages offered by AI in facial recognition to identify a potential victim, regardless of location or context, and subsequently recruit them for terrorist purposes. Through the use of algorithms, facial recognition technology enables the identification, selection and organisation of images, as well as the identification of behavioural patterns of the persons under surveillance (Mann & Smith, 2017, pp. 121-145), which contributes significantly to the efficiency of the recruitment process of new members. Therefore, we can see that AI technology provides terrorist groups with a powerful set of tools through which they are able to create and disseminate propaganda, but also to recruit new recruits in a much easier way that does not involve significant investment.

Terrorist organisations use AI technology assimilated with commercial systems and to plan and execute attacks in a more efficient and complex way, which poses a serious threat to global security (Brundage et. al., 2018, p. 27). AI-powered algorithms have the ability to analyse large amounts of data from different sources so that they can identify potential targets, including through facial recognition, and execute attacks without human intervention with a high success rate. It should be noted that, as facial recognition systems are not infallible and have certain limitations (Hamann & Smith, 2019, pp. 9-13), and can also produce false identifications, terrorist groups can also target innocent people. On the other hand, terrorists can intentionally manipulate this technology to mark targets or assign false identities, causing misinformation and confusion in society by producing innocent victims.

By predictively analysing data from social media platforms, online forums and other sources, terrorist groups can identify security vulnerabilities and develop strategies to exploit them. Also, by

analysing social media data, terrorist organisations can identify patterns and other relevant information, which may include important details about critical infrastructure, events or public places that may become potential targets for terrorist attacks.

In order to plan and execute terrorist attacks, terrorist organisations need funding. According to experts, the most common sources of funding for terrorism are through sponsorships, charitable donations, illegal activities (smuggling, extortion, fraud), as well as through legal activities (personal or credit-based loans) (Oftedal, 2014, pp. 11-12). In addition, in recent years, terrorist organisations have started to use AI technology to obtain funding through the use of cryptocurrencies, which poses a significant threat to global security. Cryptocurrencies are a decentralised payment method via a decentralised blockchain that is difficult to track, most of which are designed to eliminate the control, oversight and fees associated with traditional fiat currency transactions (Smith, 2023). In 2020, US counter-terrorism authorities uncovered a series of fundraising campaigns by terrorist groups such as the al-Qassam Brigades, Islamic State and al-Qaeda, through which they were able to obtain substantial cryptocurrency-based funding (Mines & Margolin, 2020). The introduction of AI algorithms into the cryptocurrency operating system, as is the case with blockchain networks, improves the performance and functionality of traditional cryptocurrencies, with the ability to conduct much faster transactions (IBM, n.d-b). The lack of adequate regulation and effective monitoring and control mechanisms over the cryptocurrency industry still allows terrorist organisations to use this method to finance their activities.

AI-powered algorithms also have the ability to assess the risk of a possible attack and develop strategies for deploying potential attacks, allowing terrorists to operationalise such precise and coordinated actions, thereby maximising damage and minimising their own losses. By automating terrorist attacks, perpetrators can make use of machine learning algorithms that allow them to identify vulnerable individuals or potential targets for terrorist attacks (UNICRI, 2021, pp. 22-25). The use of machine learning algorithms to mimic human behaviour also allows terrorist groups to create fake social media profiles that appear to be legitimate, making it more difficult for the relevant authorities to identify, track potential threats and take preventive or punitive action. Thus, terrorist groups develop deceptive techniques in order to conspire their actions and evade detection by the structures specialised in dealing with terrorist issues. On the other hand, terrorist groups may resort to the use of drones, unmanned aerial vehicles (UAVs), in precise and coordinated attacks, with AI playing a crucial role in extending their capabilities, allowing them to easily navigate to targets of interest and make decisions in a totally autonomous way (Mohsan et. al., 2022). Terrorist groups are up to speed with new technologies, with drones already becoming a weapon they find difficult to annihilate. In this sense, AI can be used by terrorists to coordinate and control swarms of drones or other devices within the operationalization of synchronized attacks, eloquent being the facilities offered by Swarm algorithms (Williams, 2018, p. 22), which allow the autonomous coordination of a large number of individual units, an aspect that can determine special effects on traditional defense mechanisms.

The use of AI technology by terrorist organisations in the operation of cyber attacks is a constant concern for these entities and a major global security threat. Today, these groups have the ability to develop malware and other advanced hacking tools that have become increasingly difficult for cyber security systems to detect and counter (ReadyNH, n.d). The most vulnerable critical infrastructures in the energy sector, transport, public sector services, telecommunications, as well as manufacturing industries, have become prime targets for terrorist groups (Allianz, 2016). In addition, using AI technologies, terrorist groups can carry out cyber attacks (cyber terrorism) on the information systems of public organisations and institutions, including governments of state entities and international bodies, allowing them to access confidential data that can destabilise the functioning of the institutions concerned or even the state.

Relationships between cross-border organized crime groups, paramilitary groups and terrorist groups may lead to increased opportunities for them to procure AI-based action capabilities, which will generate additional security threats. On the other hand, the operational and logistical support, from the state level, of some paramilitary groups involved in conflict zones in various geographical areas of the world map, considerably increase the risks of their involvement in activities circumscribed to the terrorist phenomenon, as well as the resulting maximization expected through the use of AI technology. The recent activities carried out by the Wagner Group in the interest of the Russian Federation in the conflict in Ukraine, and the military support given to the group by the Kremlin authorities, increase the risk of the use of AI technology in the actions taken by the group. Moreover, in specialized circles, the activities of the last decade carried out by the Wagner Group on the African continent are assimilated to terrorist actions, a fact that motivates the requests to include it on the list of terrorist groups (Edwards & Cotovio, 2023).

In conclusion, it can be said that the peculiarities of AI technologies (speed, accuracy and scalability) provide terrorist organisations with significant opportunities, enabling them to carry out their activities more efficiently and successfully. Thus, AI algorithms can process and analyse large amounts of data in a short time frame, enabling terrorist entities to quickly identify targets of interest, quickly plan attacks on them and take covert action in a short time. On the other hand, AI offers high accuracy in data analysis and can identify patterns of modus operandi and temporal trends with a high degree of accuracy, reducing the margin of error across the entire spectrum of terrorist group concerns, from propaganda and human resource recruitment to the operationalization of heinous attacks. Terrorist groups make use of the facilities offered by AI by rapidly expanding or reducing, depending on their needs and resources, the tools they use, which gives them a high degree of flexibility in any situation.

4. OPPORTUNITIES OFFERED BY ARTIFICIAL INTELLIGENCE IN THE FIGHT AGAINST TERRORISM

As AI is an emerging and rapidly evolving technology, it is important for institutions specialised in dealing with terrorist issues to be prepared for the future in order to anticipate potential threats and develop strategies to prevent and counter new threats that may arise as a result of the use of this technology by terrorist organisations. In this regard, mention should be made of the steps taken by the US authorities to use AI in the interests of national security (Executive Order 13859/2019 founding the American Artificial Intelligence Initiative programme) (Mocanu, 2020), and the recent actions of the Council of Europe, in 2023, which adopted a new counter-terrorism strategy for the period 2023-2027, setting out new tools and concrete responses to the challenges faced by European states as a result of the growing incidence of terrorism (Council of Europe, 2023). Also, on June 14, 2023, the European Parliament voted to adopt the first legislation regulating the use of AI technology at European Union (EU) level, ensuring that systems based on this technology are secure, transparent, traceable and non-discriminatory, are overseen by the human factor that created them, and EU citizens are protected from its negative effects - disinformation, promotion of violence, terrorism. (Nahoi, 2023).

Preventing and countering the actions of terrorist groups requires concerted action by specialised institutions (Peptan & Butnariu, 2020, pp. 65-77), which increasingly relies on the opportunities offered by AI technology.

First of all, the mentioned technologies offer a diverse range of applications that can be used in the fight against terrorism, such as people's access control systems or border point security. Generically, they are circumscribed to the eProfiler system - a system designed to secure areas or perimeters of interest through video surveillance -, based on the detection and identification of

people/objects, the detection of violence and the analysis of crowd behavior. (Ionescu, B., et. al., 2020, p. 57).

On another note, the capabilities offered by modern AI-based surveillance systems enable the monitoring of social networks and other online platforms in order to obtain, process and analyze data to identify and track potential terrorists through facial recognition tools and other technologies biometrics, as well as for detecting potential terrorist actions, or identifying the behavioral and action patterns of terrorists. Systems developed on these technologies can identify persons of interest, generate certain alarms in case of potential vulnerabilities or terrorist threats, and analyze video streams and photo images in real time (Krishan, Sharma & Kanchan, 2020, pp. 131-139; Jain, Ross & Prabhakar, 2004, pp. 4-20). Circumscribed to this type of opportunities, we also find the eSeeming system - based on the analysis of emotions and physiological signs -, which aims to detect covert behavior or the concealment of the truth (lie) from the interlocutor's speech, allowing to obtain important information, especially in the management of informative or judicial investigations. (Ionescu, B., et. al., 2020, p. 59).

Such technologies have been used by the US in recent decades, most notably the XKeyscore and PRISM software developed by the National Security Agency and used for population surveillance. Although the implementation of these programmes was intended to prevent future situations similar to the terrorist attacks of 11 September 2001, their use has provoked a worldwide political debate on the implications of population surveillance in the context of technological progress (Scheuerman, 2014, pp. 609-628).

Given the high degree of hermeticity of terrorist groups, which makes HUMINT intelligence gathering difficult, AI technologies offer counter-terrorism structures the greatest opportunities in the intelligence gathering/collection stages. Thus, in the exploitation of open sources (OSINT), increasing use is being made of Deep Web and Deep Learning algorithms, which offer outstanding visual identification and speech recognition facilities. Also, exploitation of SIGINT technical sources allows the exploitation of the electromagnetic spectrum to identify behavioural patterns in crisis situations, while IMINT sources allow information to be obtained from the analysis of images of interest (Mocanu, 2020). Generically, such activities are circumscribed to the eTalk system - based on the collection of information through the analysis of recorded audio and visual data -, which was designed to allow the management of critical scenarios, through the use of automatic speech transcription, search for spoken words, speaker identification and, last but not least, lip reading. (Ionescu, B., et. al., 2020, p. 58-59). The operational successes achieved using these technical sources against the Al-Qaeda terrorist group after the terrorist attacks of 11 September 2001 have confirmed their role and necessity in the arsenal of specialised counter-terrorism structures (Hayden, 2018, pp. 44-46).

Regarding the anticipatory dimension of terrorist actions through the capabilities offered by AI technology, Atin Basuchoudhary and James T. Bang credit the idea that if a variable cannot be used empirically to predict terrorism, then it is unlikely to have a causal relationship. However, AI's ability to rapidly collect and analyse large amounts of data gives it the ability to identify certain variables that can then be analysed in a causal context. The choice of variables must be based on theory, in particular on pre-existing data obtained through human, technical and information analysis sources, in which context AI can become an integral part of an iterative knowledge building process (Basuchoudhary & Bang, 2018, p. 7).

Special opportunities are offered to specialised counter-terrorism structures by AI technology and at the intelligence processing and analysis stage, allowing analysts to identify regional peculiarities, dialects, or suspicious individuals and their actions. Specialised software for meta-data mining of collected data/information, decryption of information or facilities at the intelligence analysis stage itself, add to the panoply of opportunities offered by AI technology (Mocanu, 2020).

Equally important are the opportunities offered by AI technology in the actions/operations undertaken by specialised structures against terrorist entities (supported by the intelligence gathering and analytical pillars), from identifying vulnerabilities in the systems used by terrorist entities and their modus operandi, to taking the necessary decisions to ensure the success of the operations undertaken. AI-based object detection and recognition algorithms that leverage computer vision techniques provide drones with the ability to identify and track specific objects or targets (terrorists, their locations, assets used to carry out attacks). At the same time, these facilities can be used by specialised counter-terrorism structures and for conducting specific surveillance, search and rescue operations of their own operational capabilities. The operations to eliminate the leaders of Al-Qaeda, Osama bin Laden (Cristea, 2015), in the year 2011, and Ayman al-Zawahiri (Șerban, 2022), in the year 2022, based on vast programs of investigation and surveillance with the help of means based on AI technology (satellites and drones capable of capture and transmit in real-time images and video recordings of operational interest), are some of the most successful actions in which a special role has been played by the effective combination of the roles of the human factor and modern AI technology.

5. ETHICAL AND LEGAL ASPECTS OF THE USE OF ARTIFICIAL INTELLIGENCE IN TERRORISM ISSUES

The use of AI technology by actors involved in the terrorist phenomenon - terrorist entities and institutions specialised in combating the phenomenon, raises particular challenges (computational limitations, regulation, type of use), but also numerous ethical and legal issues.

Since in the case of the first category of actors listed above, by the nature of the activities carried out by them, it is not possible to speak of compliance with regulatory rules in the field, awareness of action, responsibility and ethics in the steps taken, we shall now confine ourselves to a few brief comments on the ethical and legal problems caused by the use of AI by specialized institutions in the fight against terrorism.

The manifestations and developments of terrorism over the last three decades have led to the idea that it represents a deterritorialised, asymmetric war, which requires coherent measures to be carried out by specialised state or international structures, in the context of a real anti-terrorist war (Văduva, 2002, pp. 58-62). It is an atypical war, focusing on the dimensions of knowledge, prevention and counteraction, including the use of AI technologies.

Even under these circumstances, by extrapolation, we believe that the anti-terrorist war, waged against a form of "illegal violence", must comply with the provisions of the Geneva Conventions of 1949 and the additional protocols to these conventions of 1977 (which, by the way, prohibit terrorism in international armed conflicts). Thus, the specialized interventions limited to countering the activities of terrorist entities must not cause unnecessary destruction, avoid as much as possible the production of victims among the civilian population not involved in supporting terrorist activities and be limited to achieving the proposed objectives, respectively the destruction of the operational capabilities of the groups terrorist. On the other hand, the use of AI technology in the anti-terrorist war must be able to ensure compliance with the principles of proportionality and humanity of the intervention against exponents of terrorism, leading to the combating of the targeted targets from among the terrorist entity, without producing collateral victims.

In another vein, the use of AI technology in anticipating the actions of terrorist entities or in identifying and prosecuting the perpetrators of terrorist attacks - Regulated by the "European Ethical Charter on the Use of Artificial Intelligence in Legal Systems and their environment" (CEPEJ, 2018) - is a major issue and challenge due to the unique opportunities offered by this technology in identifying and facially recognising perpetrators, analysing and interpreting gunshot/explosive sounds

ISSN-P: 1844-6051 ~ ISSN-E: 2344-3677

1/2023 ***https://alss.utgjiu.ro***

to identify the type of weapon/explosive device used, or assessing the criminal or recidivism potential of perpetrators (Predescu, 2023).

On all levels of action of the specialised counter-terrorism structures, a possible irrational use of AI can also generate significant risks and dangers in terms of reducing human control over its lethal force and, implicitly, of assigning responsibility for the attacks undertaken. It is worth noting that autonomous weapons can be programmed to act and make decisions without direct human intervention, so there is a risk that the human factor may lose control over the actions taken by these advanced systems, which are susceptible to error.

Even if the war on terror is characterised by a value dimension conferred by well-defined rules, norms or procedures, examples of past good practice and even customary approaches imposed by the specificities of the targets, the theme of awareness of action and responsibility is the guiding principle of the actions taken. In these circumstances, the subject of AI's action consciousness - which can go beyond the control of the human factor, who created it and uses it for various purposes, including the fight against terrorism - is intensely debated, with scholarly studies pointing out that only its creator, i.e. man, can "decide whether the evolution of AI will at some point be marked by consciousness and then reflective consciousness." (Predescu, 2023)

The issue of criminal liability, as it relates to the use of AI technology, is far from a unified approach among experts. Thus, Tyler L. Jaynes raises the question of the responsibilities of the author of the code originally written by the human factor and the ability of AI technology to generate new code with additional instructions. Thus, a legal problem is generated when the computer becomes the author of its set of programmed instructions, the human factor being unable to determine whether the code owned by such a device was created by its command (Jaynes, 2019, pp. 342-356). Jacques Hartmann et al. draw attention to the fact that an additional legal problem is caused by the ability of AI to facilitate autonomous decision-making by drones and the way this ability is treated in the relevant legislation. It should be noted that with the increasing performance of AI, the legal system faces increasingly complex dilemmas in regulating the autonomous behaviour of AI applications. The 2019 report of the Expert Group on Liability and New Technologies, set up by the EU Commission, showed that the evolution of new emerging digital technologies is giving rise to increasingly complex ecosystems, making it difficult to establish a coherent liability framework with clarity (Hartmann, Jueptner, Matalonga & White, 2023, pp. 31-48). Dremliuga Roman and Prisekina Natalia believe that the field of AI needs to be legally regulated especially when its possession, use and distribution can become sufficiently dangerous. On the other hand, when AI technology is integrated into devices containing prohibited dangerous objects or substances, existing legislation in the field should be applied. In their view, where AI is used in a new dangerous device, the use of which is not legally regulated, the legislation on dangerous objects may apply (Roman & Natalia, 2019, pp. 342-346).

With regard to the ethical issues arising from the use of AI technology in counter-terrorism warfare, analysed from the perspective of the nature and outcome of the action, we are of the opinion that the approach must be based on and be in line with the general regulations established at the United Nations General Conference on Education, Science and Culture of 23 November 2021 - "Recommendation on the Ethics of Artificial Intelligence" (UNESCO, 2021) - concerning: Respect, protection and promotion of human rights, fundamental freedoms and human dignity; proportionality and prohibition of harm; safety and security; fairness and non-discrimination; transparency and explainability; privacy and data protection; accountability and responsibility (Predescu, 2023).

In the fight against terrorism, AI is considered a strategic technology, based on excellence and two-way interaction with the human factor, which must implement, through the development and strengthening of technological capabilities, the awareness of adopting an ethical conduct necessary to respect fundamental rights and values at the societal level (European Commission, 2020). Regardless

of the circumstances and the means of action to combat the scourge of terrorism - perceived as a real war on terror consciously and premeditated by certain individual and collective entities - compliance with ethical and legal rules is an imperative condition, even if these conditions sometimes lead to operational disadvantages compared to the actions of the adversary.

6. RESEARCH LIMITATIONS

Our research deals with a topical subject, circumscribed by an issue with a particular impact on the global security situation. As the work of some of the institutions responsible for detecting, preventing and countering the actions of terrorist entities is a state secret, the means and methods used are not accessible to the general public. Thus, the limitations of the research are inherent, which did not allow for the presentation of a diverse and complex case study. Also, the authors did not present possible concrete scenarios confirming the theoretical aspects of the possible use of AI by terrorist entities and/or counter-terrorism institutions, in order to avoid providing ethically questionable information.

7. CONCLUSION

The opportunities offered by the use of AI technologies in issues related to terrorism imply, on the one hand, the generation/increase of risks and dangers to global security and, on the other hand, the development of capabilities to act against this scourge of the global world.

The use of AI technology, in particular through the use of machine learning algorithms, allows terrorist groups to increase their ability to capture, analyse and process data, which gives them a particular operational capability to strengthen their human resources (recruitment, propaganda), to quickly identify potential targets and to develop more effective attack strategies. Terrorist groups may also use advanced technologies, such as drones and other autonomous weapons, which can be programmed to execute terrorist attacks with precision, increasing the ability to operationalise actions, making them more difficult to detect and counter, and reducing the risk of collateral damage. Thus, our research hypothesis, at least from a theoretical point of view, is confirmed.

On the other hand, AI technology also offers great opportunities for institutions specialising in terrorism management to anticipate potential threats and develop strategies to prevent and counter security threats from terrorist organisations.

In this context, both categories of actors involved in the terrorist phenomenon - terrorist groups and structures specialised in preventing and countering terrorism, are concerned to develop concerted actions in order to gain a competitive advantage by developing and implementing the latest AI technologies. The development race in AI technology may cause instability in international relations through increased competition between nations for the development and use of advanced technologies, and the proliferation of AI technologies by non-state actors, including terrorist groups, is a source of concern (McLay, n.d, p. 24).

Therefore, a global and coordinated approach is needed to manage the challenges posed by the use of AI technology in dealing with terrorism, with the international community tasked with developing appropriate regulations.

REFERENCES

A.D. (2022, October). Artificial intelligence. Real time information. *Intelligence.* Retrieved from https://intelligence.sri.ro/inteligenta-artificiala-informatii-timp-real/

Allianz. (2016, June). Cyberattacks on critical infrastructure. Retrieved from https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html

Alrhmoun, A., Winter, C. & Kertesz, J. (2023). Automating Terror: The Role and Impact of Telegram Bots in the Islamic State's Online Ecosystem. *Terrorism and political violence*

Basuchoudhary, A., & Bang, J. T. (2018). Predicting Terrorism with Machine Learning: Lessons from „Predicting Terrorism: A Machine Learning Approach." Peace Economics, *Peace Science and Public Policy, 24*(4)

Benkler, Y., Faris, R., & Roberts, H. (2018). *Network propaganda: Manipulation, disinformation, and radicalization in American politics*. Oxford University Press., pp. 30-39

Bringsjord, S. & Govindarajulu, N. S. (2018, July 18). Artificial Intelligence. *Stanford.* Retrieved from https://plato.stanford.edu/entries/artificial-intelligence/

Brundage, M. et al. (2018)., The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Retrieved from https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/1c6q2kc4v_50335.pdf

CEPEJ. (2018). Regulated by the „European Ethical Charter on the Use of Artificial Intelligence in Legal Systems and their environment". Retrieved from https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

Council of Europe. (2023, February 8). Council of Europe adopts new counter-terrorism strategy for 2023-2027. Retrieved from https://www.coe.int/en/web/portal/-/council-of-europe-adopts-new-counter-terrorism-strategy-for-2023-2027

Greaves, M. (2020, August 4). 'Deepfakes' ranked as most serious AI crime threat. *UCL*. Retrieved from https://www.ucl.ac.uk/news/2020/aug/deepfakes-ranked-most-serious-ai-crime-threat

Cristea, B. (2015). Taking down the most wanted terrorist: The moment social media mattered. *Playtech.* Retrieved from https://playtech.ro/2015/eliminarea-celui-mai-cautat-terorist-momentul-cand-retelele-sociale-au-contat/

Edwards, C & Cotovio, V . (2023, July 26). UK government is heavily criticized for underestimating Wagner group's actions around the world. *CNN*. Retrieved from https://edition.cnn.com/2023/07/26/europe/uk-government-wagner-group-report-intl-gbr/index.html

Harmann, K. & Smith, R. (2019). Facial recognition technology. *Criminal Justice*, *34*(1)

Hayden, M.V. (2018). *Pe muchie de cuțit. Serviciile secrete americane în epoca terorii.* Meteor Publishing.

IBM. (n.d-b). Blockchain and artificial intelligence (AI). Retrieved from https://www.ibm.com/topics/blockchain-ai

IBM. (n.d.-a). What end-to-end encryption means. Retrieved from https://www.ibm.com/topics/end-to-end-encryption

Ionescu, B., et. al., Artificial Intelligence Fights Crime and Terrorism at a New Level, în *IEEE Multi Media,* 2020, Vol. 27, No. 2

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, *14*(1)

Jaynes, T. L. (2019). Legal personhood for artificial intelligence: citizenship as the exception to the rule. *AI & SOCIETY*

Krishan, K. P., Sharma, S.K. & Kanchan, T. (2020). Facial-recognition algorithms: A literature review. *Medicine, Science and the Law*, *60*(2)

Mann, M. & Smith, M. (2017). Automated facial recognition technology: Recent developments and approaches to oversight. *University of New South Wales Law Journal, 40*(1)

McKendrick, K. (2019, August 7). Artificial Intelligence Prediction and Counterterrorism. *Clatham House.* Retrieved from https://www.chathamhouse.org/sites/default/files/2019-08-07-AICounterterrorism.pdf

McLay, R. (n.d.). Managing the rise of Artificial Intelligence. *Tech.humanrights.gov*. Retrieved from https://tech.humanrights.gov.au/sites/default/files/inline-files/100%20-%20Ron%20McLay.pdf

Mines, A. & Margolin, D. (2020, August 26). Cryptocurrency and the Dismantling of Terrorism Financing Campaigns. *Lawfare.* Retrieved from https://www.lawfareblog.com/cryptocurrency-and-dismantling-terrorism-financing-campaigns

Mocanu, M. (2020, February 11). Artificial intelligence in intelligence and beyond. *Monitorul Apărării*. Retrieved from https://monitorulapararii.ro/inteligenta-artificiala-in-intelligence-si-nu-numai-1-28414

Mohsan, S. et al. (2022). Towards the Unmanned Aerial Vehicles (UAVs): A Comprehensive Review. *Drones* 2022, *6*(6): 147

Oftedal, E. (2014). The financing of jihadi terrorist cells in Europe. *FFI-Report.* Retrieved from https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/1103/14-02234.pdf

Nahoi, O. (12 mai 2023). A challenge before the EU: regulating artificial intelligence, Retrieved from https://www.rfi.ro/politica-social-155762-provocare-fata-ue-reglementare-inteligenta-artificiala

Peptan, C. & Butnariu, A. (2020). Considerations on preventing and combating the terrorist phenomenon. *Research and Science Today, 2*

Peptan, C. (2019). Terrorism-Security threat in the context of globalization. *Annals of the „Constantin Brancusi" of Targu-Jiu, Letter and Social Science, 2*

Peptan, C. (2021). A plea for intelligence analysis. *Annals of the „Constantin Brancusi" of Targu-Jiu, Letter and Social Science, 1*

Predescu, O. (2023, January 6). Implications of Artificial Intelligence in the legal field and beyond. *Juridice.* Retrieved from https://www.juridice.ro/essentials/6349/implicatiile-inteligentei-artificiale-in-domeniul-juridic-si-nu-numai

ReadyNH. (n.d.). Cybercrime and Cyber Terrorism. Retrieved from https://www.readynh.gov/disasters/cyber.htm

Roman, D., & Natalia, P. (2019). Artificial Intelligence Legal Policy. *Proceedings of the 2019 8th International Conference on Software and Computer Applications - ICSCA '19*.

Scheuerman, W. E. (2014). Whistleblowing as civil disobedience. *Philosophy & Social Criticism, 40*(7)

Schmid, A. (2012). The Revised Academic Consensus Definition of Terrorism., *Perspectives on terrorism, 6*(2)

Smith, A. (2023, March 23). Funding Tomorrow's Terrorists and Criminals: Cryptocurrency's Impact on the World Stage. *Georgetown Security Studies.* Retrieved from https://georgetownsecuritystudiesreview.org/2023/03/23/funding-tomorrows-terrorists-and-criminals-cryptocurrencys-impact-on-the-world-stage/

Șerban, V. (2022). How Al Qaeda leader Ayman al-Zawahiri was hunted and killed. "Every time he recorded a video, there was the chain of custody". *Ziare.com.* Retrieved from https://ziare.com/al-qaida/lider-al-qaeda-ucis-atac-cu-drone-statele-unite-afganistan-1754337

UNESCO. (2021). *Recommendation regarding the ethics of Intelligence Artificially.* Retrieved from https://www.cnr-unesco.ro/uploads/media/f1077_recomandari-unesco-ai-site.pdf

UNICRI. (2021). Algorithms and terrorism: The malicious use of artificial intelligence for terrorist purposes. Retrieved from https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf

Uppal, R. (2022, January 18). Artificial Intelligence (AI) is the future of terrorism and counterterrorism. *IDSTCH.* Retrieved from https://idstch.com/security/artificial-intelligence-ai-is-the-future-of-terrorism-and-counterterrorism/

Van der Veer, R. (2019). Terrorism in the age of technology. *Clingendael.* Retrieved from https://www.clingendael.org/pub/2019/strategic-monitor-2019-2020/terrorism-in-the-age-of-technology

Văduva, G. (n.d). *Terrorism. Geopolitic and geostrategic dimenssion. Terrorist War. War against terrorism*. Retrieved from https://cssas.unap.ro/ro/pdf_studii/terorismul.pdf

Warrick, J. (2017, February 21). Use of weaponized drones by ISIS spurs terrorism fears. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html

West, D. M. & Allen, J. R. (2018, April 24). How artificial intelligence is transforming the world. *Brookings.* Retrieved from https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/

Williams, S., M. (2018), Swarm Weapons: Demonstrating a Swarm Intelligent Algorithm for Parallel Attack, p. 22, School of Advanced Military Studies US Army Command and General Staff College Fort Leavenworth, Kansas, Retrieved from https://apps.dtic.mil/sti/pdfs/AD1071535.pdf