Terörizm ve Radikalleşme Araştırmaları Dergisi
Journal of Terrorism and Radicalization Studies

Haziran 2025, Cilt: 4, Sayı: 2, ss. 266-287

June 2025, Volume: 4, Issue: 2, pp. 266-287

ISSN 2792-0518 (Basılı/Print) **ISSN 2822-2334 (Çevrimiçi/Online)**

Makaleye ait Bilgiler / Article Information

Araştırma Makalesi / Research Article

Makale Başvuru Tarihi / Application Date : 05 Mayıs 2025 / 05 May 2025

Makale Kabul Tarihi / Acceptance Date : 18 Mayıs 2025 / 18 May 2025

Makalenin Başlığı / Article Title

The Predictive Tactical Advantages and Disadvantages of Artificial Intelligence in the Field of Counterterrorism

Terörizmle Mücadele Alanında Yapay Zekânın Öngörücü Taktik Avantajları ve Dezavantajları

Yazar(lar) / Writer(s)

Hatice VAROL DAĞDELEN

Atıf Bilgisi / Citation:

Dağdelen Varol, H. (2025). The Predictive Tactical Advantages and Disadvantages of Artificial Intelligence in the Field of Counterterrorism. *Journal of Terrorism and Radicalization Studies*, 4(2), pp. 266-287. DOI: 10.61314/traddergi.1691794

Dağdelen Varol, H. (2025). Terörizmle Mücadele Alanında Yapay Zekânın Öngörücü Taktik Avantajları ve Dezavantajları. *Terörizm ve Radikalleşme Araştırmaları Dergisi*, 4(2), ss. 266-287. DOI: 10.61314/traddergi.1691794

Terörizm ve Radikalleşme ile Mücadele Araştırma Merkezi Derneği

Research Center for Defense Against Terrorism and Radicalization Association

Adres/Address: Beytepe Mah. Kanuni Sultan Süleyman Bulvarı

5387. Cadde No:15A D:58

06800 Çankaya/Ankara

www.tradergisi.com

e-posta/e-mail: editortrad@teram.org

Terörizm ve Radikalleşme Araştırmaları Dergisi-TRAD, 2025, 4(2) :266-287 Araştırma Makalesi
Journal of Terrorism and Radicalization Studies-TRAD, 2025, 4(2): 266-287 Research Article
DOI: 10.61314/traddergi.1691794

THE PREDICTIVE TACTICAL ADVANTAGES AND DISADVANTAGES OF ARTIFICIAL INTELLIGENCE IN THE FIELD OF COUNTERTERRORISM

Hatice VAROL DAĞDELEN*

ABSTRACT

The study examines the evolving predictive tactical approaches of states to counter terrorism by utilizing emerging artificial intelligence technologies in a multidimensional manner. The subject under scrutiny in the present study is the development of artificial intelligence in general, and which methods are most prominent in the field of counterterrorism. In this context, firstly the concept of artificial intelligence is discussed, and then the historical development of the concept is focused upon. In the following discussion, the subset of artificial intelligence that is applicable to counterterrorism is analyzed, and the predictive tactical advantages of these subsets are explained. The study delineates a predictive tactical approach to the terrorism threat, accompanied by illustrative applications of technology. The methodological approach employed is qualitative and interpretive. The findings obtained at the conclusion of the study indicate that, despite the success achieved in the field of security by artificial intelligence technologies, there is a necessity for a strict control mechanism with regard to ethical and moral responsibility. It is imperative that the effective and beneficial use of artificial intelligence in the field of security is predicated on the establishment of moral and legal use, transparency, accountability, and systems determined by national and international standards.

Keywords: *Artificial intelligence, Terrorism, Counterterrorism, Machine Learning, Predictive Detection*

TERÖRİZMLE MÜCADELE ALANINDA YAPAY ZEKANIN ÖNGÖRÜCÜ TAKTİK AVANTAJLARI VE DEZAVANTAJLARI

ÖZET

Çalışma, devletlerin gelişen yapay zekâ teknolojilerini kullanarak terörizmle mücadeleye yönelik değişen öngörüsel *(predictive)* taktik yaklaşımlarını çok boyutlu bir şekilde ele almaktadır. Çalışmada incelenen konu genel olarak yapay zekanın gelişimi ve terörizmle mücadele alanında en çok hangi yöntemlerinin öne çıktığıdır. Bu kapsamda öncelikle yapay zekâ kavramı ele alınmış ardından kavramın tarihsel gelişimine odaklanılmıştır. Sonrasında yapay zekanın terörizmle mücadele için kullanılabilecek alt kümelerine yer verilmekte ve bu alt kümelerin öngörüsel taktik avantajları anlatılmıştır. Çalışmada anlatılan terörizm tehdidine yönelik öngörüsel taktik yaklaşım teknolojinin kullanıldığı örnek uygulamalar yer almaktadır. Kullanılan yöntem niteliksel ve yorumlayıcı analizdir. Çalışma sonunda elde edilen bulgular yapay zekâ teknolojileri sayesinde güvenlik alanında başarı elde edilmesine karşın etik ve ahlaki sorumluluğun sıkı bir kontrol mekanizmasına muhtaç olduğu yönündedir. Sonuç olarak yapay zekanın güvenlik alanında etkin ve faydalı kullanımı için gerekli olan şeyler ahlaki ve hukuki kullanım, şeffaflık, hesap verilebilir, ulusal ve uluslararası standartlarda belirlenmiş sistemler kurulmasıyla mümkündür.

Anahtar Kelimeler: *Yapay Zekâ, Terörizm, Terörizmle Mücadele, Makine Öğrenimi, Öngörüsel Tespit.*

* PhD Candidate, TERAM Researcher, hvarol28@gmail.com, ORCID: 0000-0002-3668-3048

INTRODUCTION

The contemporary world is witnessing profound shifts in the security landscape, precipitated by the rapid evolution of threat concepts, technological advancements, and the proliferation of hybrid actors. The field of terrorism is one in which this shift is particularly pronounced. Terrorism is becoming increasingly dispersed, virtual, and unpredictable. These changes in the realm of terrorism have consequently precipitated alterations in this field, particularly due to the inadequacy of the security measures implemented in the period preceding September 11. In a globalized and digitalized world, security measures taken against terrorism have started to be carried out not only in the military field but also in the technological field. Simon, 2011, pp. 47-50: As posited by Ballard et al. (2002, pp. 2-7).

Despite the integration of technology into the security sector having occurred in parallel with weapon technologies, it is the advent of artificial intelligence (AI) and deep learning methods, developed in conjunction with AI, that has primarily driven the advancement of technology in the field of security. AI is defined as a set of systems that can systematically analyze scattered and complex data sets to produce logical results, identify certain patterns, make predictions for tomorrow with yesterday's data, and detect things that are wrong or different from normal (Kaplan, 2019, p. 2).Thanks to its wide usage area and capacity to process big data quickly, AI is not only a post-incident tool for the security field, but also contributes to the development of proactive and preventive strategies with profiling, patterning, face recognition methods and word analysis on social media. For instance, the United States' Defense Advanced Research Projects Agency (DARPA) and the Israeli Internal Security Organization (Shin Bet, Shabak, or Shin Bet) are institutions that utilize AI tools to predict terrorist activities. The operational capabilities of AI are revealed by the features. As Weimann (2016, pp. 1-5) and Russell & Norvig (2016, pp. 1-3) argue.

It is evident that there are numerous technical and tactical advantages inherent in the utilization of artificial intelligence within the domain of security. However, it is imperative to acknowledge that the implementation of this technology transcends the confines of the technical and tactical dimensions. Furthermore, while the operational characteristics of AI are beneficial, there are also ethical, social, cultural and legal debates concerning the development and utilization of the technology system based on AI. In her

seminal work, Shoshana Zuboff conceptualizes the term "surveillance capitalism", as employed in her book The Age of Surveillance Capitalism (2019), as a system in which the use of individual data is of paramount importance in the emerging capitalist system (pp. 203-213). Concerns regarding invasion of privacy, including unauthorized use of personal data, distrust of institutions, and technological biases, have led to questions regarding the use of AI.

Nevertheless, the threat posed by the use of this technology by terrorist organisations is indisputable. It is evident that organisations have the capacity to utilise this technology for a variety of purposes, including the recruitment of new members, the concealment of existing members' identities, the destruction of reputations, and the deceit of security forces through the presentation of false images of their activities. It is imperative to acknowledge that all of these threats have the potential to engender significant security concerns.

The main question of this study is how countries use artificial intelligence technologies in the fight against terrorism. The primary objective of this study is to provide a comprehensive, overarching review of the utilization of artificial intelligence as a method for the early detection of terrorism. The objective of the present study is twofold: firstly, to discuss the challenges currently being faced in this field, and secondly, to provide a perspective on future opportunities for those who are committed to the detection of terrorism using AI. The objective of the present study is to investigate the tactical advantages and disadvantages of AI-enabled technology in the prediction and early detection of terrorist threats. The assumption that is being made in the context of this question is that AI technologies have ethical and social risks as well as tactical advantages by transforming traditional intelligence. The present study offers suggestions for the ethical and social aspects of AI in the fight against terrorism. These suggestions are based on an analysis of the tactical usage of AI in this context. While preparing the recommendations, disadvantageous situations caused by AI are first identified. After the identification of these situations, recommendations are presented for each topic. The primary objective of these recommendations is to enhance the efficacy of AI utilization in the counterterrorism effort.

1. CONCEPTUAL FRAMEWORK AND HISTORICAL DEVELOPMENT

AI is open to diverse interpretations. Russell and Norvig (2016) posit that AI can be defined as a set of systems that are capable of perceiving their environment, making goal-oriented decisions, and undergoing constant development (p. 233). Michael Haenlein and Andreas Kaplan (2019) define AI as a field that encompasses a multitude of processes for the analysis of complex data, with the capability to sub-analyze its constituent elements, and to extend itself to autonomous decision-making processes (p. 2). According to Cole Stryker (2024), the concept refers to the comprehension of human learning by computers, the realization of problem solutions, and the development of creative and autonomous simulations. According to Kathleen McKendrick (2019), the primary objective of AI is not the emulation of the human brain, but rather its transcendence (p. 6). In the NATO terminology dictionary, created by NATO, AI is defined as the field of computer science that enables the analysis of large data sets to perform functions similar to human intelligence, such as reasoning or learning (NATO Term, 2005). In summary, the term 'AI' is a general designation for cognitive programs that possess the capacity for both deep learning and analysis.

Despite the pervasiveness of the notion of AI in contemporary discourse over the past decade, the field traces its origins and definitions to the previous century. It is important to acknowledge that AI has undergone various phases throughout its extensive history, from its inception to the present day. These stages are referred to as the spring, summer, fall and winter of AI (Haenlein & Kaplan, 2019, pp. 2-4).

The genesis of AI can be traced back to the 1940s, a period which bore witness to seminal contributions from both Alan Turing, with his formulation of the Turing Test, and Isaac Asimov, with his robotics stories. The concept transitioned from the domain of science fiction to that of academia in 1956. The initial conceptualization of the notion was undertaken by Marvin Minsky and John McCarthy in 1955. McCarthy, Marvin Minsky, Claude Shannon and Nathaniel Rochester were responsible for the preparation of a working paper for an eight-week congress at Dartmouth College about machine learning. The paper's underlying assumption is that machines should be designed to simulate human learning and intelligence

processes. Consequently, the resultant product will comprise not only a programming language but also a machine language, thereby elucidating the fundamental principles of intelligence. However, it is evident that the existing computers were not deemed adequate for these predictions. Notwithstanding the successful resolution of the hardware issue, it is imperative to consider the absence of efficacious software programs to facilitate the initiation of the project. Consequently, the primary recommendation of the authors of this paper is to comprehend and formulate methodologies for the development of machine learning processes. As demonstrated on pages 12 to 14.

The "Logic Theorist" (LT), developed by Allen Newell and Herbert Simon between 1955 and 1956, was conceived as the inaugural instance of AI. It is evident that, because of LT, machines have now been developed which are capable of emulating human problem-solving skills. In 1961, the pair developed a new program known as "General Problem Solver" (GPS). The GPS system was designed to address more complex objectives than LT, but this process was interrupted due to an incident (Neapolitan & Jiang, 2018, p. 1). The summer period utilized by AI was of a relatively limited duration.

In the late 1970s, the British mathematician James Lighthill published a report on the subject. In his report, Lighthill expressed a negative perspective on the prevailing positive outlook towards AI, characterizing machines as amateurs who have gained experience. According to the author, machines will never be able to compete with human intelligence (Haenlein & Kaplan, 2019, pp. 2-4). The seminal report by Lighthill initiated the winter period of AI technology.

After the five-year winter period of AI, a decline, or stagnation period, ensued until the 1990s. The initial programming that fostered the field, coupled with the critiques directed towards AI, prompted investors to withhold their financial support. Furthermore, the fact that data could not be entered automatically in the initial examples rendered analysis particularly challenging. The manual preparation of data sets has been identified as a contributing factor to the challenges encountered in determining the duration of the studies to be implemented (Haenlein and Kaplan, 2019, pp. 2-4).

In 1997, the world chess championship was won by IBM's Deep Blue, a supercomputer, over the then-current world champion, Kasparov. This event led to a resurgence of interest in the field of AI studies (IBM). After this, the development of Google Translate, search engines and other AI-supported technologies commenced. In the early 2000s, methods such as "decision tree" (DT) for AI classification gained popularity.

The rapid development of AI technology since the 2000s has led to its integration into various fields, including economics, informatics, and security strategies employed by states. The analysis of large data sets, the utilization of decision support systems, the capacity for linguistic analysis and the ability to process information in real-time, all of which are enabled by artificial intelligence (AI)-supported technologies, have collectively created the conditions for the emergence of anticipatory and predictive approaches within the domain of security. The methods employed in the domain of traditional security comprise post-incident intervention techniques. However, with the advent of AI, a change in thinking has occurred, allowing for the prediction of such events in advance.

The utilization of AI technology in the domain of security was initiated by institutions such as DARPA and IARPA, which were established in the USA in 1958. While the benefits provided by these institutions were limited in the early periods, their effectiveness increased with the development of AI technology. As demonstrated in the seminal works of Waibel (2019, pp. 1-12) and DARPA (2023).

The integration of AI technology, which is now prevalent across diverse sectors, into the realm of terrorism prevention signifies a paradigm shift towards a more comprehensive and nuanced approach to security assurance. The implementation of pattern recognition and anomaly detection tasks on large and complex data sets is facilitated by artificial intelligence (AI)-supported applications, which offer high processing power and rapid execution.

2. PREDICTING TERRORISM WITH AI

Terrorism is an area of study which, like any other discipline, is characterized by its low level of predictability. This is because it is a subject which depends on the human factor. The strategic stealth techniques and

self-development capacities of terrorist organizations or radicalized individuals pose a significant security threat that is challenging to analyze.

The application of classical intelligence methods for the early detection of terrorism, which is difficult to analyze, has not always yielded the desired results. In a world that is undergoing rapid change and becoming increasingly virtualized, there is a growing imperative to utilize cutting-edge technologies that are predicated on the analysis of digital traces for the purpose of detecting terrorism in its early stages. The utilization of artificial intelligence facilitates the processing of information derived from disparate and voluminous data layers, culminating in the classification of threats. Within the framework of categorized threats, states establish a prioritized ranking system for their own nations.

It is evident that there are various subsets of AI, with distinct application methods, including DT and random forest (RF). The primary categories encompass supervised learning, unsupervised learning, reinforcement learning, discriminative, generative, narrow or strong AI. Despite the heterogeneity of AI subsets, the process known as deep learning or machine learning occupies a central role in the classification, prediction, clustering, pattern recognition and decision-making stages that it applies to data. Machine learning employs deep neural networks (DNNs), which emulate the complex processes of the human brain.

DNNs are a system of interconnected artificial neurons that have the capacity to learn complex patterns from large data sets (Paris and Donovan, 2019, p. 12). DNNs are composed of multiple layers of artificial neural networks. The multiplicity of these layers is commensurate with the complexity of the data. Each layer processes the data it receives through a series of elementary calculations and then passes it on to the next layer. In order to reduce the error rate of the final version of the data, processes known as back propagation between layers are repeated, thereby characterizing the repetition of the process. Through repetition or back propagation, the network improves over time and increases in accuracy (Zhang et al., 2016, pp. 1-4). It is evident that this learning and development process has enabled the execution of functions such as classification, prediction, clustering, pattern recognition and decision making on a wide variety of data sources.

The utilization of AI classification models, such as DT and RF, is of paramount importance in the realm of terrorism prevention, given their capacity to facilitate both classification and prediction. DT and RF facilitate the identification of terrorist threats, the classification of suspicious behavior and the calculation of risk scores in large and multivariate data sets. As asserted by Lamptey et al. (2023, pp. 1-2). The DT method employs a branching model of the data, analogous to the branching structure of a tree. After each node, the conditions under scrutiny are catalogued in succession. The DT method facilitates the meaningful classification of data, including social media posts, IP mobility, digital footprints, and geographical locations of individuals with whom a suspicious person interacts. The merits of this approach are twofold: firstly, it is comprehensible and secondly, it lends itself to straightforward interpretation. However, DT, which is known to produce clearer results in small data sets, is unable to reach a sufficient level in complex data. As posited by Ali et al. (2012, p. 272), the RF method may be delineated as a forest version of the DT method, which is fundamentally designed as a single tree. In the RF method, each tree is trained using a random subset of the data set, thus creating a model that allows generalization. This method has been demonstrated to produce more reliable and accurate results in comparison with DT. However, the utilization of RF is considerably more challenging than that of DT about processing power and training level (Fratello and Tagliaferri, 2018, p. 374).

The classification structure of AI technologies is generally multidimensional, and is divided into areas such as machine learning, image recognition and processing, deep learning, and language processing. The accuracy rates of these systems, which are derived from supervised and unsupervised learning types, are quite high (Russell & Norvig, 2020, pp. 5). These technologies, which offer innovations in many fields from education to health, have also found a place in the field of security. In the context of counter-terrorism efforts, states employ artificial intelligence (AI) to collect extensive data concerning the interactions of digital content users with each other, their preferences, and other relevant information. However, the digital realm is not solely a medium for ordinary individuals to socialize; it is also a space in which malevolent ideologies are propagated. Weimann (2016) posits that a considerable proportion of radicalization occurs within the digital domain. It is imperative to comprehend, analyze and interpret the language employed in this domain. Digital communication strategies, social

media and online forums, especially popularized by DAESH and used extensively by terrorist organizations, have rendered these areas part and parcel of radicalization, propaganda, organization and intelligence gathering activities. The process of identifying radicalized individuals within social media or digital environments by means of reverse engineering is facilitated by the utilization of AI-supported technology.

To comprehend radicalization in so-called online environments, deep learning-based natural language processing (NLP) techniques are imperative in detecting the ideological language patterns of terrorist organizations. The utilization of NLP facilitates the categorization of social media articles as positive, neutral, or negative, thereby enabling the discernment of the public's stance on the subject matter. The utilisation of NLP facilitates the classification of tweets concerning a particular subject as either "positive", "neutral", or "negative". The objective is to ascertain public sentiment regarding the specified topic. This method is widely used in the commercial sector, for example, The effectiveness of marketing campaigns can be measured by monitoring brand mentions on social media. NLP is a branch of AI that uses machine learning methods to analyse and comprehend natural language. Its utilisation is pervasive, encompassing domains such as marketing, finance, and healthcare. NLP employs machine learning methodologies to analyse the natural language found on social media. The tool is a potent instrument for comprehending and analysing textual material, as well as for formulating decisions based on that comprehension. (Bural, 2021, p. 116).

One of the most significant features of AI technologies in the field of terrorism is the capacity for prediction of behavior. Behavior prediction is predicated on an examination of an individual's past actions, which allows for the prediction of how they will behave in the future. This method facilitates the identification of individuals who sympathize with terrorism or consume radical content, thereby enabling the early prevention of future criminal activity (Pfaff, 2025, p.5). As Helbing et al. (2017) emphasizes the ability of AI to analyze complex data sets quickly and in real time is of paramount importance. It is asserted that the utilization of AI technology will ensure the identification of any details or errors that may be overlooked by human workers.

AI-based image processing systems are utilized for the analysis of images obtained from security cameras or satellite images. In particular, facial recognition technologies have great importance in detecting suspicious individuals in crowds, monitoring illegal crossings and locating wanted persons. These systems have the capacity to be integrated with biometric data, thereby becoming real-time threat detection systems (Garcia-Sanchez et al., 2018). In addition to the aforementioned, data from security cameras employed in the targeting systems of autonomous aircraft is also analyzed by computers that possess deep learning capabilities.

In summary, the advantages of this system can be encapsulated as follows: classification and clustering of data, creation of ideological language patterns through data, behavioral predictions, creation of patterns, fast and real-time analysis of complex and large data, detection of fugitive or criminal individuals, and the capacity to recognize images obtained from autonomous vehicles (see Table 1). The advent of AI-enabled technologies has rendered the analysis of terrorism's logistical sources, individual or organizational connections, radicalization methods, smuggling activities and ideological language patterns a relatively straightforward task.

Table 1. Predictive Tactical Advantages of Artificial Intelligence in Terrorism

Classification and forecasting of big data
Creating ideological language patterns
Behavior prediction
Pattern recognition
Fast and real-time prediction of complex datasets
Recognition of illegal crossings or criminal individuals
Detection of threat elements by analyzing the images obtained by autonomous technology

3. THE DARK SIDE OF PREDICTIVE AI

Although it is recognized that artificial intelligence (AI) offers numerous advantages in numerous domains, there are approaches within the

counterterrorism literature that demonstrate a degree of caution about these technologies, and in some cases, even express criticism. The utilization of AI is not merely a technical concern; it is also a legal, human, social and moral issue. In this section, the primary challenges arising from the utilization of AI in the security sector are examined through the lens of five distinct categories. The categories encompass technical errors, privacy violations, algorithmic bias, democratic oversight and economic problems (see Table 2).

Table 2. Predictive Tactical Disadvantages of Artificial Intelligence in Terrorism

Vulnerability to technical errors
Privacy violations and ethical concerns
Algorithmic biases
Lack of democratic control
Economic problems

It is evident that technical criticisms of AI technologies are derived from the inherent characteristics of AI itself. The technology in question is predicated on the utilization of computers and cyber systems. While analyzing data, there is a possibility of integrating with various applications. In such circumstances, AI itself will be vulnerable to cyber-attacks. Of particular concern is the vulnerability of national security domains, such as the counterterrorism efforts, to potential threats. (PFAFF, 2025, p.10) One of the potential technical errors that can occur is the prediction of future behavior based on past data. Nevertheless, it should be noted that the accuracy of this prediction is questionable in dynamic and non-patterned fields, such as the social sciences.

In instances of so-called 'false positives', systems have the capacity to erroneously identify innocent individuals as suspects, a process which they subsequently deem to be of risk according to their proprietary algorithms. This phenomenon has the potential to not only compromise an individual's reputation but also hinder the apprehension of genuine lawbreakers (Wagner, 2018). Ethical concerns have been identified as a significant critique of AI (see Pfaff, 2025, p. 10; Pauwels, 2020, p. 16). Zuboff (2019) contends that AI surveillance systems have the potential to compromise privacy, autonomy

and freedom. He emphasizes that there is a risk of these systems falling into the hands of authoritarian governments and leading to social insecurity.

Another salient issue in relation to ethical concerns pertains to the equilibrium between security and freedom. The development of AI technologies for the early detection of terrorism has the potential to identify individuals deemed to be at risk. However, this process may also infringe upon individuals' rights and freedoms. It is emphasized that AI technology may become a part of preemptive security practices, which may result in a conflict with liberal legal norms (Amoore, 2013).

The training of artificial intelligence systems is contingent upon the data sets on which they are based. The algorithms may be influenced by historical, cultural or social biases inherent in the datasets. For instance, certain ethnic, religious or regional groups that have been associated with more terrorist links in the past may be classified as high-risk by the systems. This suggests that the automation of discriminatory practices is being encouraged, thereby reinforcing systemic bias (Noble, 2018).

The concept of constant surveillance, as depicted by George Orwell in his renowned work 1984 and as described by Michel Foucault as the metaphor of the panopticon[2], can be considered a form of self-censorship that leads to the internalization of specific behaviors. This state of affairs, particularly within democratic societies, gives rise to significant debates concerning the security-freedom balance. The development of AI technologies for the early prevention of terrorism has the potential to identify individuals deemed to be at risk. However, this identification process may also result in the infringement of individuals' rights and freedoms. It is emphasized that AI technology may become a part of preemptive security practices, which may result in a conflict with liberal legal norms (Amoore, 2013).

Most AI technologies associated with security and terrorism are characterized as 'black boxes'. In the context of a black box system, the general public is unable to ascertain the mechanisms by which processes

[2] The panopticon, invented in the 1700s by Jeremy Bentham. It is a design of a prison building with cells arranged in a circle around a central guard tower. This way, the inmates would never know when the guard was looking their way, and would have to behave as if they were being watched at all times. (Bentham, 2012, pp.13-15)

operate or the rationale underpinning the decisions that are made. Consequently, the system is perceived to be deficient in terms of transparency and accountability. One of the aspects of AI that has been the subject of considerable criticism is the paucity of information, particularly in the realm of trust-based areas such as security. (Pauwels, 2020, p. 19)

Another criticism level in the field is the replacement of systems based on human intelligence with those reliant on artificial intelligence (AI) technologies. Individuals who are no longer required are compelled to face economic instability and unemployment. The threat of unemployment will not only have economic consequences. Individuals facing challenges in meeting their fundamental needs may potentially engender novel security concerns if they are unable to address these needs through legitimate channels. (Pfaff, 2025, p.10)

In conclusion, the disadvantages of predictive tactics offered by AI technologies in the field of terrorism are manifold. However, it should be noted that only the technical and algorithmic elements of these disadvantages pertain to the nature of AI. The remaining aspects are associated with legal, social and ethical domains. Consequently, an inclusive perspective should underpin the beneficial use of this technology.

4. FORECASTING TERRORISM: AI IN ACTION

The utilization of AI in the prevention and combating of terrorism is a prevalent phenomenon. The cases under discussion in this study are drawn from a range of geographical locations. The case studies under consideration herein describe the practices of the United States of America (USA), Israel, China and the European Union, respectively. The units/institutions under discussion are analyzed in only the most general terms.

DARPA was established in 1958 by the United States government with the objective of developing military technology to counter the Soviet Union. It is evident that DARPA has a pioneering and innovative role in AI-enabled threat analysis. The institution has developed programs such as "Total Information Awareness" and "Insight", with the objective of identifying potential threats in advance by analyzing the behavioral patterns of individuals with data taken from the digital environment. It is evident that the areas of work undertaken by DARPA, in addition to those pertaining to artificial intelligence, encompass a range of disciplines including

autonomous systems, cybersecurity, quantum information systems, biotechnology and the advanced weapons industry. As demonstrated in the seminal works of Waibel (2019, pp. 1-12) and DARPA (2023),

The Intelligence Advanced Research Projects Activity (IARPA) was established in 2006. This organization operates in conditions that are more challenging than those faced by DARPA. However, IARPA has developed systems that enable it to analyze radicalization trends on social media. Quantum computing and natural language processing are two examples of AI techniques utilized by IARPA. It is evident that IARPA's notable domains of operation extend beyond the realm of artificial intelligence, encompassing such disciplines as crypto analysis, cyber intelligence, behavior prediction, open-source intelligence, and quantum computing. As demonstrated in the research by Bonvillian (2018, pp. 14–15) and IARPA (2023),

The Israel Internal Security Agency (Shin Bet or Shabak) is an institution that was established in the aftermath of the establishment of the State of Israel. The primary responsibilities of the organisation include the identification and prevention of internal threats, the gathering of intelligence from the region (primarily from Palestine), the protection of high-ranking bureaucrats, and the assurance of the security of critical infrastructure.

The Shin Bet utilizes AI in two primary domains: intelligence collection from Palestine (Gross, 2020; Goldman and Jamieson, 2017) and airport security (Wrobel, 2025; Leichman, 2024). The agency is also engaged in the development of algorithms for the analysis of content shared on social media, with a view to the prevention of potential threats.

The Social Credit System (SCS) of the People's Republic of China is a rating application that evaluates the behavior of individuals, institutions and companies. The evaluation process is informed by "trustworthiness scores." The overarching objective of this system is to enhance national allegiance, curtail criminal activity, and oversee economic management. To illustrate this point, it is noteworthy that individuals who violate traffic regulations experience a decline in their credit scores. Conversely, those who receive social assistance have been observed to see an increase in their credit scores. Furthermore, individuals engaging in protest activities against the state have been documented to face blacklisting, while debtors have been reported to be

subjected to bans from utilizing public transportation. As demonstrated in Creemers (2018, pp. 1-29) and Carbone (2019),

Another system utilized in China is known as Facial Recognition (FR). The development of this system has been primarily focused on leveraging technological advancements that facilitate the identification of individuals through biometric means. It is vital to emphasize that FR is of paramount importance to public safety in China. The system encompasses a broad spectrum of locations, including educational institutions, metropolitan transportation networks, urban centers, and dining establishments. The system has been developed to facilitate the identification of criminal elements by law enforcement agencies.

The utilization of FR technology in the Xinjiang Uyghur Autonomous Region has been the subject of considerable criticism. According to a report by Human Rights Watch (2019), the reverse engineering of a mobile application that enables the use of FR technology in the aforementioned region revealed that Chinese law enforcement agencies were collecting personal data on individuals, targeting them, and sending those arrested to political education camps or other facilities.

The European Police Office (Europol), an organization operating within the European Union (EU), has described AI technologies as an area that will completely transform police institutions in its 2024 report titled "AI and Policing." Europol, an organization which has integrated AI technologies, states that it has made progress in the areas of big data analysis and the identification of potential criminals (Reuters, 2025).

The European Internet Referral Unit (EU IRU) is responsible for the identification and removal of terrorist content in the digital environment. Following the identification of radical content circulating in the digital environment, the EU IRU reports it to the relevant platforms (Aunion, 2025).

5. AI AND THE FUTURE OF TERRORISM PREDICTION

The utilization of AI for the early detection of terrorism, or for counterterrorism purposes, gives rise to a number of changes. These changes are not only operational in nature, but also legal, ethical, social, and institutional. The efficacy of these changes is evident in the positive outcomes observed in state applications. Nevertheless, the pivotal element in guaranteeing the perpetuation of these favorable advancements is the

efficacious and commensurate utilization of AI governance. This section delineates a series of anticipations for the enhancement of the predictive capabilities of AI technologies in the future.

The visions to be developed in the field of AI have the potential to enhance the future applications of existing AI technologies. It is imperative that the vision presented encompasses not only application strategies but also normative elements. This will assist states in ensuring their security while protecting the rights of individuals.

The disadvantages of using AI in the field of terrorism have been discussed in detail in the previous sections of this study. The initial disadvantage pertains to technical errors. Even though AI technology can perform activities that exceed human capacity in many areas, it is essentially a machine learning process. To circumvent technical malfunctions during this process, it is projected that human-supported hybrid AI units will be developed. In contrast to a system that is entirely devoid of human involvement, structures founded upon human-machine collaboration are likely to demonstrate a high degree of success and a low probability of error as the control process unfolds. The system has been designed to transform disadvantages caused by technical errors into advantages.

It is an irrefutable fact that AI technologies are vulnerable to cyberattacks. There are established methods that can be applied to counteract this disadvantage. To illustrate, the following measures may be adopted in order to mitigate the risk of cyber-attacks: firstly, the number of individuals granted access to the system should be limited; secondly, multiple approval processes should be required for team members to gain access to the system; and thirdly, robust firewalls should be constructed.

The second disadvantage that has been discussed in the literature is that of privacy violations. The utilization of democratic control methodologies has been demonstrated to be advantageous in the resolution of privacy violations. Another recommendation is that judicial processes should be maintained to allow for the possibility of injustice, even in circumstances where all security data is not disclosed to individuals. Furthermore, it is imperative that teams utilizing AI technologies in the analysis of data be subject to rigorous oversight and control mechanisms. Access to data will be permitted only in situations where a high level of risk is identified, and

assessments will be conducted within the parameters of the identified risk. The imposition of severe penalties on individuals or institutions responsible for crimes in cases where risk-independent data is used can be considered a factor that increases trust in AI technologies.

As evidenced by the examples of SCS and FR applications supported by AI in China, AI technologies have the potential to be used for malicious purposes in societies where democracy is not fully established. In order to circumvent this issue, it is incumbent upon states to act in accordance with ethical principles, to maintain a balance between security and freedom, and to prefer to preserve their legitimacy in the eyes of the public by conducting transparent processes, thereby increasing their chances of achieving more positive results.

However, it is important to note that the utilization of AI technologies by states should be subject to general rules in international legal circles. The resolution of the aforementioned problem is predicated on the assumption that each state will regulate its AI security units in accordance with international standards and, if necessary, submit annual reports to an international organization to be established. Examples of work conducted in this area include the European Commission's Ethical Guidelines on High-Risk AI Applications (AI HLEG, 2019) and the European Union's Artificial Intelligence Act (AI Act). Despite the pioneering nature of these documents, their scope is somewhat restricted. It is anticipated that in the future, more comprehensive documents will be prepared, and that compliance with these documents by states will have a positive impact on ensuring security.

Another expectation is that institutional capacity will be increased to facilitate the storage and processing of large data sets so that AI technologies can be used more effectively in the future. This will facilitate the sustainable and reusable storage of data. It is imperative that capacity increases be realized at both the technical and institutional levels. Furthermore, it is imperative that personnel engaged in data management undergo periodic training to ensure proficiency and maintain data integrity. This will enable them to learn about ethical concerns, understand the limitations of algorithms, become experts in crisis management, and develop critical approaches to decision support units. About the training of personnel, the relevant security units of each state should prepare modular training programmers in accordance with the AI curriculum. The training provided

here should focus on legal, ethical, sociological, cultural, language skills, and technical issues.

It is important to note that not all data obtained in the field of intelligence is of the same quality. To facilitate the analysis of data with AI-supported technologies, it is essential that the data sets utilized are contemporary, precise, varied, and meticulously prepared with a emphasis on outcomes. It is imperative that the algorithms employed are secure. Furthermore, it is imperative that a uniform standard is adhered to by all institutions involved in the transfer and sharing of data. In order to ensure effective cooperation in the fight against terrorism, the establishment of national and international data pools is imperative. The transfer of data to these pools should be subject to regular monitoring by independent organizations.

In a manner analogous to Asimov's three laws of robotics, which stipulate that robots must not harm humans, the following eight principles can be enumerated. The disadvantages caused by AI technologies may, in the future, be transmuted into advantages. The following steps are recommended to facilitate the enhancement of AI technologies:

- The utilization of human-robot hybrid methodologies is imperative in contemporary research endeavors.
- The utilization of multi-security approval systems is imperative for the access of data.
- The implementation of data collection and analysis processes is to be conducted in a transparent manner.
- It is imperative that national and international legal regulations are revised in order to ensure compatibility with contemporary technological advancements.
- It is imperative to ensure an increase in institutional capacity.
- The preparation of regular and comprehensive training programmers for responsible personnel is of paramount importance.
- The enhancement of data quality is of paramount importance.
- The establishment of national and international data pools is contingent upon effective cooperation.

CONCLUSION

The evolving technological landscape is precipitating profound changes and transformations within the domain of security. In particular, the rapid

advancements in AI technologies, which have been increasing exponentially in recent years and are expanding their areas of application on a daily basis, are bringing about profound changes. AI technologies are being used in a variety of fields. These include the creation of large data clusters in the digital realm that can be understood by humans. They also include tracking and prevention of radicalization processes. In addition, they are used for the identification of fugitives or criminals through biometric identification. They are also used for the detection of abnormal behaviors, the making of behavior predictions and the creation of language patterns.. AI technologies can analyze past events and utilizing behavior prediction and pattern recognition methods to predict crimes that are likely to occur. It is evident that these features underpin a proactive and preventive paradigm shift in the field of terrorism, as represented by AI technologies.

However, as with any innovation, this technological advancement gives rise to controversial issues. Even though AI technologies are planned to reach or even surpass human intelligence, these systems have the potential to make technical errors. Furthermore, individuals have ethical concerns regarding the collection and analysis of data. These ethical concerns, termed privacy violations, are substantiated by the example of China.

It is impossible to predict the analyses produced by AI technologies due to the openness of their learning processes to intervention. This is one of the factors that could lead to individuals being discriminated against or suffering unjust loss of reputation. The absence of democratic oversight in data collection and analysis processes gives rise to concerns regarding the reliability of the system. While it is reasonable that data should not be disclosed to the public due to its confidentiality, it is important that the institutional system to be established is subject to regular monitoring. Another problem posed by AI technologies is the unemployment problem seen in every technological innovation. The utilization of AI in data analysis can facilitate the preparation of data sets that would otherwise require months of analysis to complete within a matter of hours.

In conclusion, it is evident that AI is a powerful and transformative tool for the early detection and prevention of terrorism. Nevertheless, it is imperative that this power is utilized in a more proactive manner, with a view to generating social benefits. The cornerstone of this transformation is the balance between freedom and security. It is imperative that the security

environment provided by technology does not impede personal freedoms. In this context, the utilization of artificial intelligence within the domain of security should be regarded as a political decision and an issue of values, as opposed to a mere technical advancement. Consequently, governance models should be constructed in accordance with this perspective.

REFERENCES

Aldrich, D. P. (2021). *Black wave: The Saudi-Iran wars on terror*. Oxford University Press.

Ali, J., Khan, R., Ahmad, N., & Maqsood, I. (2012). Random forests and decision trees. *International Journal of Computer Science Issues (IJCSI), 9*(5), 272.

Aunion, J. A. (February 28, 2025). *Aunque la víctima sea artificial, el crimen es real: 25 detenidos en una operación internacional contra la pornografía infantil creada con IA.* El País. Access date: 25.04.2025. https://elpais.com/sociedad/2025-02-28/aunque-la-victima-sea-artificial-el-crimen-es-real-25-detenidos-en-una-operacion-internacional-contra-la-pornografia-infantil-creada-con-ia.html

Ballard, J. D., Hornik, J. G., & McKenzie, D. (2002). Technological facilitation of terrorism: Definitional, legal, and policy issues. *American Behavioral Scientist, 45*(6), 989-1016.

Bentham, J. (2012). The Panopticon. In *Offenders or Citizens?* Antony Duff (Ed.) (pp. 13-15). Routledge.

Bural, E. B. (2021). *Sosyal Medya İstihbaratı*. Yeditepe Akademi Yayınları

Bonvillian, W. B. (2018). DARPA and its ARPA-E and IARPA clones: A unique innovation organization model. *Industrial and Corporate Change, 27*(5): 897–914.

Carbone, C. (February 22, 2019). *China bans 23 million from traveling as part of citizen report card system*. Fox News. Access date: 24.04.2025. https://www.foxnews.com/world/china-bans-23-million-from-buying-travel-tickets-as-part-of-social-credit-scoring-system

Creemers, R. (2018). *China's social credit system: An evolving practice of control*. SSRN.

DARPA. (2023). *Defense Advanced Research Projects Agency*. Access date: 30.03.2025. https://www.darpa.mil

Fratello, M., & Tagliaferri, R. (2018). Decision trees and random forests. In *Encyclopedia of bioinformatics and computational biology: ABC of bioinformatics* 1: 374.

Goldman, P., & Jamieson, A. (January 30, 2017). *Hamas used fake social media accounts to hack Israeli soldiers' phones: IDF*. NBC News. Access date: 20.03.2025. https://www.nbcnews.com/news/world/hamas-used-fake-social-media-accounts-hack-israeli-soldiers-phones-n706036

Gross, J. A. (February 17, 2020). *IDF: Hamas again tries to 'catfish' soldiers with fake women on social media.* Times of Israel. Access date: 20.03.2025. https://www.timesofisrael.com/idf-hamas-again-tries-to-catfish-soldiers-with-fake-women-on-social-media/

Haenlein, M., & Kaplan, A. (2019). A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. *California Management Review, 61*(4): 5–14.

Human Rights Watch. (May 1, 2019). *China's algorithms of repression: Reverse engineering a Xinjiang police mass surveillance app*. Access date: 20.03.2025. https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass

IARPA. (2023). *Intelligence advanced research projects activity*. Access date:10.03.2025. https://www.iarpa.gov

IBM. (n.d.). *Deep blue*. Access date: 25.04.2025. https://www.ibm.com/history/deep-blue

Lamptey, O., Gegov, A., Ouelhadj, D., Hopgood, A., & Da Deppo, S. (2023, June). Neural Network Based Identification of Terrorist Groups Using Explainable Artificial Intelligence. In *2023 IEEE Conference on Artificial Intelligence (CAI)* (pp. 191-192). IEEE.

McKendrick, K. (2019). *Artificial intelligence prediction and counterterrorism*. Chatham House.

NATOTerm. (n.d.). NATO Terminology Database. Access date: 10.03.2025. https://nso.nato.int/natoterm/Web.mvc

Paris, B., & Donovan, J. (2019). *Deepfakes and cheap fakes: The manipulation of audio and visual evidence.* Data & Society Research Institute, 12.

Reuters. (18 Mart 2025). Europol warns of AI-driven crime threats. Access date: 13.04.2025. https://www.reuters.com/world/europe/europol-warns-ai-driven-crime-threats-2025-03-18/

Russell, S., & Norvig, P. (2016). *Artificial intelligence: A modern approach* (3rd ed.). Pearson Education.

Simon, J. D. (2011). Technological and lone operator terrorism: Prospects for a fifth wave of global terrorism. In *Terrorism, identity and legitimacy: The four waves theory and political violence*. Jean E. Rosenfeld (Ed.). (pp.44-66) Routledge.

Wagner, B. (2018). Ethics as an escape from regulation: From ethics-washing to ethics-shopping? In *Being profiling*. Amsterdam University Press.

Waibel, A. (2019). *What is DARPA? How to design successful technology disruption.* Access date: 13.04.2025. https://isl.iar.kit.edu/downloads/WhatIsDarpa.Waibel.pdf

Weimann, G. (2016). *Terrorism in cyberspace: The next generation*. Columbia University Press.

Wirtz, B. W., & Müller, W. M. (2019). Artificial intelligence and the public sector—Applications and challenges. *International Journal of Public Administration*, *42*(7): 596–615.

Zhang, J., Zheng, Y., Qi, D., Li, R., & Yi, X. (November 2016). DNN-based prediction model for spatio-temporal data. In *Proceedings of the 24th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*. 1–4.

Zuboff, S. (2019). The age of surveillance capitalism. In *Social theory re-wired*. Longhofer, W., & Winchester, D. (Ed.) (pp.203-213) Routledge.