Artificial Intelligence in Crime Prevention and Counter-Terrorism

Mesterséges intelligencia a bűnmegelőzésben és a terrorizmus elleni védekezésben

BAUMGARTNER Helga[1] – ŐSZI Arnold[2]

Abstract

The integration of artificial intelligence and facial recognition technologies into modern security frameworks significantly enhance our ability to identify threats, to take preventive measures, and to improve public safety and security. As threats posed by criminals and suspected terrorists continue to evolve, increasingly sophisticated countermeasures are required to combat the risks posed by such threats. By analysing vast amounts of data in real-time, artificial intelligence can detect patterns that suggest illegal activities, while face recognition can identify individuals of interest without them suspecting surveillance. Furthermore, with rapid evolution and broad applicability within both physical and cybersecurity, these technologies enable continuous improvement, ensuring that security measures follow the recent technological advancement. Artificial intelligence and face recognition play crucial roles in mitigating security risks and in countering terrorism, making them an important component of the global effort to maintain safety in our complex and digital world.

Keywords

artificial intelligence, counter-terrorism, face recognition, cybersecurity

Absztrakt

A mesterséges intelligencia és az arcfelismerő technológiák integrálása a biztonsági rendszerekbe jelentős előrelépést jelent a fenyegetések azonosítására, a megelőző intézkedések megtételére és a biztonság fokozására. Ahogy a bűnözők és a feltételezett terroristák által jelentett fenyegetések egyre fejlődnek, egyre kifinomultabb ellenintézkedések szükségesek ezek leküzdésére. A valós idejű adatelemzés révén a mesterséges intelligencia képes felismerni az illegális tevékenységekre utaló mintázatokat, míg az arcfelismerő rendszerek képesek azonosítani a célszemélyeket természetes közegükben. Gyors fejlődésük és széleskörű alkalmazhatóságuk révén, biztosítják, hogy a fizikai és kiberbiztonsági intézkedések lépést tudjanak tartani a legújabb technológiai fejlesztésekkel. A mesterséges intelligencia és az arcfelismerés kulcsszerepet játszanak a biztonsági kockázatok mérséklésében és hatékony eszközt nyújtanak a terrorizmus elleni globális küzdelemben az összetett és digitális világunkban.

Kulcsszavak

mesterséges intelligencia, terrorizmus elleni védekezés, arcfelismerés, kiberbiztonság

[1] baumgartner.helga@phd.uni-obuda.hu | ORCID: 0009-0003-7938-7614 | PhD Student, Doctoral School for Safety and Security Sciences Óbuda University |Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] oszi.arnold@bgk.uni-obuda.hu | ORCID: 0000-0001-5988-0143 | adjunct professor, Óbuda University, Bánki Donát Faculty of Mechanical and Security Technology Engineering |adjunktus, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

ARTIFICIAL INTELLIGENCE

Artificial intelligence is one of the most critical technologies today, playing a significant role in our daily lives. In the past decade, it has undergone significant evolution — the rapid growth of the internet has led to an exponential increase in the volume of data produced, which is a key component in artificial intelligence development. Artificial intelligence is a complex interdisciplinary field, which integrates elements – apart from computer science, mathematics and statistics, engineering – from biology and medicine, psychology, sociology, communication and linguistics, amongst others. With the increase in computing power and the improvement of algorithms that enable the addressing of more complex problems, processing this ever-growing amount of data has become faster and more efficient in response. Moreover, increased financial investment in artificial intelligence has resulted in its rapid spread across various sectors. This widespread adoption is transforming industries. In healthcare, artificial intelligence assists in diagnosing diseases and personalizing treatment plans. In the automotive industry, it advances the development of autonomous vehicles. In national defence it helps analyse the allied and enemy forces' strategy and provides support in military operations. In the financial sector artificial intelligence is used for fraud detection and investment analysis. In education it tailors the learning path based on the individual's learning experience. Smart cities also utilize artificial intelligence to develop a more liveable space by improving traffic management, energy, water and waste management, and infrastructure management. With the help of artificial intelligence, farmers can optimize field usage for better food production, manage natural resources and minimize environmental impact. Furthermore, artificial intelligence-driven chatbots are enhancing customer service. As a result, artificial intelligence is not only changing technology, but also impacting society, leading to new innovations, and making life more efficient, leading to innovation and efficiency: starting a new era where technology and daily life work better together. [1] [2]

Artificial intelligence has become an integral part of our everyday life, aiming to make it easier and more convenient. Despite its undeniable presence and effects, oftentimes we are not truly aware of the way it works, or the potentials it has. The evolution and spread of artificial intelligence have outpaced the public awareness, which can lead to either underestimating the possibilities that artificial intelligence holds or overestimating its capabilities — either way we may fail to explore the potential benefits. As we continue to integrate artificial intelligence into our lives, we must focus on understanding its benefits while simultaneously paying attention to its misuse.

Artificial intelligence has multiple subfields, each representing different technologies, and often they are referred to collectively as artificial intelligence, which, although not necessarily inaccurate, understanding the characteristics of these subfields and their potential applications improves our ability to utilise their strengths effectively across the different sectors and functions. The primary subfield of artificial intelligence is machine learning, which enables machines to learn autonomously and to improve from experience without being specifically programmed to do so. By analysing vast amounts of data, it can identify patterns and trends with more precision and higher effectiveness than a human. This capability allows machine learning to be applied across various industries, leading to significant improvements in efficiency, accuracy, and decision-making processes. Another subfield is deep learning, which employs neural networks inspired by the human brain's structure and function to process high-dimensional, unstructured data, effectively mimicking human intuition but at a scale and speed that exceeds human capability. Deep learning is able to understand data hierarchy, allowing machines to understand texts, pictures or even sounds, which is a significant progress in areas such as autonomous vehicles, speech recognition, and predictive analytics, revolutionising how machines understand and interact with the world. [1] [3]

This paper focuses on the technical and operational aspects of facial recognition technology and counter-terrorism. While facial recognition technology raises significant concerns regarding privacy, data protection, human rights, and ethics, these are beyond the scope of this study, and therefore, not discussed.

ARTIFICIAL INTELLIGENCE IN SAFETY AND SECURITY

Artificial intelligence has also gained ground in the safety and security sector, where it is applied across various fields, such as in physical security, including access control, fire protection, hazard detection, disaster response and management, as well as in information security, data protection and cybersecurity. These artificial intelligence-driven solutions are used not only by consumers seeking to make everyday life safer and more comfortable, but also by government bodies to enhance national security, and to efficiently identify and assess threats and to mitigate the risks posed criminal activities. These advanced technologies enable a more proactive approach in identifying threats, protecting infrastructure, managing emergencies, facilitating better coordination and response strategies at local, national, and international levels, allowing for a much more effective and efficient allocation of both human and material resources. [4]

In physical safety and security, artificial intelligence can be applied to Closed-Circuit Television Systems (CCTV) where it can enhance their functions and enable proactive monitoring and response, rather than merely reactive actions. Traditional CCTV requires constant human oversight to detect and respond to anomalies. By integrating artificial intelligence into CCTV systems, it can reduce the need for human resources that would perform the same function, decrease overall response time, and increase the efficiency of these systems, overall leading to enhanced safety and security for both people and infrastructure. [5]

Artificial intelligence enhanced CCTV can improve security measures by performing object recognition, which can identify unattended bags in public areas; crucial in restricted areas such as airports, stadiums, or densely populated streets, preventing possible terrorist attack. Object recognition can also be used to identify weapons or other specific items, allowing security personnel for fast reaction. By monitoring the crowd, it is also possible to determine the number of attendees, assess density, and to determine if the headcount reaches a potentially dangerous level. When evacuation is required, artificial intelligence can advise through dynamic exit signs about the optimal evacuation route as the conditions change. [6]

Artificial intelligence is also used in plate number recognition, which is widely applied, especially to manage access to parking lots, ensuring only authorised vehicles can access restricted areas. It is also utilised by law enforcement agencies to monitor traffic for potential violations and to identify and locate stolen or suspicious vehicles.

Another method of utilising artificial intelligence is in motion detection, which can enhance intrusion detection and perimeter security by differentiating between the movements of humans and animals. Traditional motion sensors often react to any kind of movement, disregarding the size of the body detected. By applying artificial intelligence, the system can differentiate whether the motion comes from a human – and therefore a potential intruder – or an animal, and therefore reduce false alarms.

Fire safety can also benefit from the use of artificial intelligence. One known application is in CCTV systems with flame and smoke detection function where visual changes indicating fire can be identified. During firefighting, real-time visual monitoring can inform firefighters of potential flashover, enabling them to leave the building, before it is too late. Artificial intelligence can also be trained to identify the type of burning material or fluid without personnel being exposed to potential harm. Furthermore, artificial intelligence can also be applied to simulations of the spread of smoke and fire in buildings, and with that, evacuation and firefighting plans can be updated, and the ideal location of sprinklers and other fire protection and firefighting devices can be identified for optimal performance. [7]

During a disaster, the primary focus is on minimising the impact of such events as much as possible. Disasters can arise from health crises, natural causes, human negligence, or even acts of terror. Effective disaster management includes prediction, prevention, preparation, mitigation, response and recovery. Of these, prediction plays a crucial role, for which artificial intelligence serves as a powerful tool. By analysing historical data and current measurements, artificial intelligence can predict natural disasters such as floods, volcanic eruptions, or hurricanes, and can advise on effective rebuilding strategies for resource allocation.

Disasters occurring due to human negligence, such as industrial accidents or nuclear disasters, can also be mitigated using artificial intelligence by predicting equipment failure, recognising signs of human negligence and advising on the safety distance for evacuation in case of nuclear disaster based on level of radiation to minimize exposure. Ultimately, artificial intelligence can be applied to all elements of disaster management. [8] [9]

ARTIFICIAL INTELLIGENCE AND CYBERSECURITY

Cybercrime and cyberterrorism pose a great threat nowadays, affecting everyone and every sector from individuals to governmental, private, and public sectors. These activities range from stealing personal data to causing financial fraud or attacking critical infrastructure to a level where cyber criminals or cyberterrorists are capable of shutting down communication and navigation systems, disrupting businesses or government operations.

On one hand, artificial intelligence can be used by malicious actors to identify vulnerable targets or refine their methods to seem more authentic. However, artificial intelligence can also detect threats and offer response solutions to mitigate risk, therefore enhance cybersecurity and reduce potential damage. Machine learning models can analyse and learn the pattern of the users' normal behaviour, and can detect when irregular activities occur, that indicate cyberattack.

Ransomware is also often employed by cybercriminals and cyberterrorists, who block access to systems of individuals or organizations within the private or public sector to demand ransom. Machine learning models can be applied to make ransomwares more sophisticated by learning how the security measures developed against them work, and adapting accordingly, making them more difficult to detect, therefore posing greater threat to its victims. However, artificial intelligence can also predict potential ransomware attacks based on historical data, foresee future threats and suggest preventive measures based on the profile of the organization. During an attack, artificial intelligence can initiate immediate incident response, such as isolating elements of the system, or shutting down the whole system and therefore minimizing the impact, while informing respective individuals and authorities about the attack. Furthermore, artificial intelligence can be utilized to reconstruct the elements of the attack for further investigations, helping to understand the utilized methods for the attack, and to develop an adequate cyber-defence strategy. [1] [10]

The spread of crypto assets – including crypto currency – has been convenient in the financing of terrorism due to their anonymity and quick transferability across borders. Terrorist groups can receive fundings in crypto currency – ransoms are also often demanded in the form of crypto currency – which then can be used to purchase firearms and explosives, launder money, and to commit further crime or acts of (cyber)terrorism.

The internet and social media serve as a tool for radicalisation of individuals, recruiting potential terrorists, and financing terrorist operations including transactions of weapons.

The adoption of end-to-end encryption in popular messaging platforms enables suspected terrorists to communicate in such way that is almost impossible for law enforcement agencies to detect. Additionally, they often use the dark web to conduct their illegal activities while remaining anonymous and protected by the encryption and anonymity features of the dark web.

ARTIFICIAL INTELLIGENCE AND COUNTER-TERRORISM

Terrorism does not have a universally accepted definition, and the same applies to cyberterrorism, however, the key distinction between "traditional" terrorism and cyberterrorism is that cyberterrorism often does not involve physical harm or direct casualties. Instead, cyberterrorism focuses on disrupting services and causing serious consequences for critical infrastructure, resulting in chaos and significant economic damage.

With the widespread availability of the internet and modern technology, access to the internet has become more available for the many. As such, suspected terrorists as well are adopting new technologies and are shifting their theatre into cyberspace, allowing criminals and suspected terrorists to operate across borders with minimum risk of exposure, spreading terrorist content – including propaganda –, recruiting individuals, and learning about the latest technology for malicious purposes. While the two concepts are similar, they are not the same. [11]

To prevent cyberterrorist attacks, it is crucial to protect online infrastructure adequately by implementing security controls; predictive measures must be in place. Artificial intelligence can quickly and accurately process and analyse vast amounts of data – such as communications metadata, financial transactions, travel patterns, and web browsing activities. artificial intelligence in the context of counter-terrorism could serve multiple purposes, including identifying patterns of terrorist threat, including their intent, capabilities, and opportunity. In turn, a better understanding of the threat would allow counter-terrorism authorities to deploy measures to mitigate the associated risks.

The total data production in 2024 is estimated to reach 147 zettabytes per day, increasing to 181 zettabytes per day in 2025. This includes the creation and collection of digital information across the internet, including, but not limited to social media content, communication, scientific research, and data from Internet of Things (IoT), among others. From a technology and research perspective such growth of available data is welcomed, as it enhances various aspects of human life, however, managing such quantity of data is impossible to be controlled by humans alone, and therefore calls for advanced data management. [12]

To effectively manage this data, employing artificial intelligence to monitor online content in real-time is essential. This approach ensures the timely detection and flagging of terrorist content for removal, thereby preventing its spread and promoting a safer internet environment. However, this method requires a balanced application of technology and human judgment, as utilising this approach for monitoring individuals requires such a large amount of data per person to be effective, which is almost impossible to collect, and also raises significant human rights concerns regarding privacy, discrimination, and the potential for mass surveillance. [1]

It is undeniably easier to analyse written content, however, videos are more commonly used to share information. Advanced algorithms are required to monitor the content of videos, which can be utilised not only for analysing the content – such as speech, sound, images, surroundings.

Numerous tools are available to identify online terrorist content, which can be districted into two main groups: matching and classification. Matching compares new content to existing content that has been previously classified as terrorist content. In this case the content is converted into a fixed-length string of data, or so-called hash value, allowing comparison of whether the newly generated hash value matches any of the existing hash values generated from confirmed terrorist content. When using cryptographic hashing, the same content will always generate the same hash value, which is both a strength and a weakness of this technique. Any alteration of the original content results in a different hash value. Alternatively, perceptual hashing can also be utilized, as this technique can identify visually similar content and patterns despite minor modification. However, matching does not always classify as artificial intelligence, only when machine learning is applied to learn, adapt, and improve over time. [13]

To adequately monitor content on the internet, artificial intelligence tools based on computer vision, speech recognition and audio analysis and Natural Language Processing (NLP) techniques must be applied to sift through texts, images, videos, audios available online, identifying potential terrorist material or connections that can indicate the presence of terrorist groups. NLP is a subfield of artificial intelligence that applies machine learning, and often deep learning as well to analyse texts, and to understand their content and semantics. However, content moderation and classification also heavily rely on computer vision for image and video analysis, as well as speech recognition and audio analysis for processing audio content. matching technique, classification-based content moderation offers a more sophisticated approach.

A sophisticated NLP technology can differentiate between an article about terrorism, and potential terrorist content, preventing the misleading of officials. While these technologies can identify possible terrorist content, they require human assessment and final decision. No matter how advanced artificial intelligence is, it may identify harmless content as terrorist content, and vice versa. Automated content moderation is used by many well-known social media platforms to identify and filter content that meets pre-defined criteria, helping to prevent spread of terrorist propaganda and radicalisation, however, due to the stylistic nuances of a language, it may fail to adequately recognise the intended message and, therefore, should not be fully automated without human supervision. [3]

One significant limitation of applying artificial intelligence to detect and remove online terrorist content is the lack of available relevant data needed to adequately train the algorithms. While different online platforms provide a large amount of data that has already been identified and removed, this data might not be sufficient to train the algorithms to identify all types of terrorist content, or it might be biased, due to specific event, terminology appearing in the training data, as well as the lack of accepted definition of terrorism. To overcome this limitation, generative artificial intelligence can be used to generate content for training purposes that is similar to already existing, real-world example. This new content is then similar in style, terminology, and characteristics of previous examples, with the aim of filling the gap of lack of sufficient training data. [13]

ARTIFICIAL INTELLIGENCE AND FACE RECOGNITION

Of all the possible applications of artificial intelligence in the field of counter-terrorism, artificial intelligence enhanced face recognition is particularly crucial.

Face recognition in crime prevention was utilised long before the digital era. Historically, until the mid-1900s, identification relied on manual comparison of photographs in documents such as identification cards or early passport versions where photos could be easily falsified, or replaced, and the comparison relied significantly on human intuition. Relying solely on the expertise of law enforcement personnel, it has been, and still is, a liability, as errors may occur due to potential misjudgement and lack of experience of the personnel in charge of the verification of these documents.

When digital pictures replaced analogue, face recognition underwent a significant evaluation. Firstly, as falsification of photographs within identification documents became much more challenging and secondly as sophisticated facial recognition technologies became available.

The origins of face recognition dates back to the 1960s, when a semi-automatic face recognition system was developed by Woody Bledsoe, along with Helen Chan Wolf and Charles Bisson, where the characteristic reference points on the image of a human face were manually marked on a graphic tablet, and then the computer would use these points to recognise faces. In the 1970s, a semi-automated facial recognition system was created by A. Jay Goldstein, Leon D. Harmon and Ann B. Lesk, by establishing 21 marker points on the face, which were then systematically compared by computers. In the late 1980s, face recognition underwent significant development, when Michael Kirby and Lawrence Sirovich, began to apply a method based on linear algebra, which later served as the foundation of the Eigenface technique. The concept is that the positions of reference points on the face relative to each other can be described by vectors, and less than one hundred values are necessary to numerically describe a face for identification purposes. In the early 1990's this method was adopted and further developed by Matthew Turk and Alex Pentland, who created an average face from all the faces in their database. By subtracting this average face from each individual face and describing the difference with vectors, the characteristic eigenvector, or personal vector, for each face is obtained. [14] [15]

In the mid 1990s, Peter N. Belhumeur, João P. Hespanha, and David J. Kriegman developed a method called Fisherface to address some of the limitations of the Eigenface technique. This method enhances the accuracy of recognition by better distinguishing features of different individuals and reducing unnecessary variations, such as changes in expression or lighting within the same person's images. [16]

From the 1990s onwards, the civilian sector has played a significant role in developing face detection and recognition systems, mostly encouraged by governmental bodies. Among these initiatives are the Facial Recognition Technology Database (FERET) initiated by the Defense Advanced Research Projects Agency (DARPA), or the Face Recognition Vendor Tests (FRVT) launched by the National Institute of Standards and Technology (NIST) in the 2000s. In 2001 Paul Viola and Michael Jones developed a face and object detection system using Haar-like features. This method was capable of analysing a large number of images in real-time to determine whether they contained an image of a face. The Haar-like features scan images, searching for patterns characteristic of faces based on the intensity of contrasts and edges due to facial features. [14] [17]

The methods listed so far worked primarily on basic algorithms, without the use of artificial intelligence.

In the 2010s, as artificial intelligence became more widespread, so did artificial intelligence enhanced face recognition, integrating deep learning to improve its accuracy. These systems began to incorporate deep learning techniques, which use neural networks with multiple layers to analyse various forms of data. This integration marked a pivotal shift in how facial recognition technologies functioned, enabling these systems to achieve unprecedented levels of accuracy and efficiency.

Deep learning models, especially Convolutional Neural Networks (CNNs), learn to detect and differentiate between facial features automatically and accurately. As these systems are fed more data, their ability to recognise faces under varied conditions and from different angles improves. Sophisticated models are also able to differentiate and recognize various facial expressions, coming from different emotions, and categorise people based on that, which allows among others personalised targeting in marketing, other purposes like enhanced security measures, where facial emotions can indicate intent or state of mind.

FACE RECOGNITION AND COUNTER-TERRORISM

The events of 9/11 brought a significant change in safety and security, especially within the aspect of travel and border management. This incident catalysed significant advancements in security measures – countries became more protective, strengthened their borders as well as their entry policies, and travel regulations became unprecedentedly strict. This event also accelerated the integration of biometric data into Machine Readable Travel Documents (MRTDs), and therefore facial recognition technology became a significant tool in countering terrorism. As a result of that, nowadays more than 140 countries issue MRTDs, with integrated biometric data. Integrating facial recognition technology into travel security has revolutionised border control and screening procedures at both land crossings and airports. This helps prevent suspected terrorists from crossing borders or boarding flights, resulting in enhanced security measures and a significant improvement in safety protocols. [18]

When leaving or entering a country, travellers must present their travel documents to passport control officer, who then verifies the identity of the traveller, checks the validity of the document, and that the individual is not on any watchlist, including known or suspected criminals and terrorists among other entities. Automated Border Control Gates (ABC Gate) operate in a similar way as traditional passport control but replace the passport control official with facial recognition software. Travellers present their travel document – only those with integrated biometrics data – to the ABC gate, which scans and verifies the document, ensures that person is the rightful owner, and checks that they are not wanted by authorities. [19]

Facial recognition technology enhances safety and security in both physical and cyberspace. By integrating it into CCTV systems in public spaces, authorities can improve their situational awareness, enabling them to monitor these areas more effectively, and detect and respond to suspicious activities. These systems can be deployed in crowded places, such as airports, stadiums, train stations and streets. Facial recognition systems are capable of monitoring crowds in real time, searching for potential matches against watchlists. During investigations for criminal cases including terrorist attempts or attacks, reviewing CCTV footage, extracting facial images of the potential perpetrators and using artificial intelligence enhanced facial recognition systems to search for and possibly identify criminals and suspected terrorists are crucial for the success of investigation.

In cyberspace, facial recognition systems can be employed to monitor online content, identifying individuals in terrorist propaganda, or extracting their facial images, similarly to how they operate in physical space. By analysing the content together with the metadata, such as geolocation, time stamp and other technical information, law enforcement agencies have better chance to capture known or suspected criminals and terrorists. [1]

SUMMARY

Artificial intelligence undeniably plays an increasingly significant role in our everyday life – unless we specifically attempt to avoid it – there is hardly a day when we do not meet it in our daily routines. Applying artificial intelligence to safety and security, and especially to crime prevention and counter-terrorism, could immensely enhance global safety and security.

Applying artificial intelligence in these areas is complex; from real-time CCTV with enhanced capabilities to complex data analysis that predicts potential threats before they materialise. These systems are capable of identifying individuals on watchlists in real-time, providing law enforcement agencies with essential information that can prevent terrorist actions. Facial recognition technology, when integrated with extensive surveillance networks, enables continuous monitoring of public spaces, therefore enhancing the detection and response to potential threats.

Artificial intelligence is capable of analysing vast amounts of data, allowing it to identify patterns and connections that human analysts may miss. This includes forecasting potential terrorist attacks by analysing communication, financial transactions, and travel data. Law enforcement agencies can extract actionable information from this data, preventing possible crime and terrorist acts.

Integrating artificial intelligence into counter-terrorism strategies becomes imperative, this not only ensures a higher level of public safety but also supports a more proactive approach to global security challenges. In a world where threats are becoming more complex and harder to detect, artificial intelligence offers a powerful tool in the arsenal of national security, enhancing international cooperation and coordination for safety and security.

Facial recognition technology supports various aspects of counter-terrorism efforts, including prevention, investigation, surveillance, and monitoring of online environments. As threats continue to evolve, the strategic application of facial recognition technology remains crucial in safeguarding the public and enhancing global security measures.

REFERENCES

[1] United Nations Office of Counter-Terrorism – Counter-Terrorism Centre (UNCCT) – United Nations Interregional Crime and Justice Research Institute (UNICRI) – *Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes – A Joint Report by UNICRI and UNCCT*, 2021, [Online] link

[2] KOLLÁR, Csaba – A mesterséges intelligencia és a kapcsolódó technológiák bemutatása a biztonságtudomány fókuszában – Kiberbiztonság – Cybersecurity 2. – Biztonságtudományi Doktori Iskola, Budapest, 2019, ISBN:9789634491859 [Online] link

[3] United Nations Office of Counter-Terrorism – Counter-Terrorism Centre (UNCCT) – United Nations Interregional Crime and Justice Research Institute (UNICRI) – *Countering Terrorism Online with Artificial Intelligence – An Overview for Law Enforcement and Counter-Terrorism Agencies in South Asia and South-East Asia – A Joint Report by UNICRI and UNCCT*, 2021, [Online] link

[4] NECZ, Dániel – *A mesterséges intelligencia belügyi és biztonsági célú alkalmazása* – SCIENTIA ET SECURITAS 1 : 1 pp. 49-53., 5 p. (2020), , [Online] link

[5] LAHIFF, Mike – *How AI is Disrupting the Business of Physical Security* – Forbes Technology Council, 2023, , [Online] link

[6] ROMAN, Jesse – *Applications of AI* – National Fire Protection Association (NFPA) Journal, 2024 [Online] link

[7] ROMAN, Jesse – *Our AI Future* – National Fire Protection Association (NFPA) Journal, 2024 [Online] link

[8] SAHOTA, Neil – *AI in Disaster Management: AI's Role in Disaster Risk Reduction, 2023,* [Online] link

[9] BARI, Lazima Faiah, AHMED Iftekhar, AHMED Rayhan, ZIHAN Tawhid Ahmed, SHARMIN Sabrina, PRANTO Abir Hasan, and Md. ISLAM Rabiul – *Potential Use of Artificial Intelligence (AI) in Disaster Risk and Emergency Health Management: A Critical Appraisal on Environmental Health* – Sage Journals, 2023 [Online] link

[10] PAUL, Anthony Lawrence – *The Role of Artificial Intelligence in Enhancing Data Security* – May 2024 [Online] link

[11] NADIJA, Madaoui – *The role of artificial intelligence in combating cyber terrorism – El Papel de la Inteligencia Artificial en la Lucha Contra el Ciberterrorismo*, IUS ET SCIENTIA, 2023 Vol. 9 Nº 2, [Online] link

[12] TAYLOR Petroc – *Amount of data created, consumed, and stored 2010-2020, with forecasts to 2025* – Statista, 2023 [Online] link

[13] MACDONALD, Stuart, MATTHEIS, Ashley, WELLS, David – *Using Artificial Intelligence and Machine Learning to Identify Terrorist Content Online* - Tech Against Terrorism Europe - 15 January 2024 [Online] link

[14] NEC New Zealand Limited – *A brief history of Facial Recognition* –2022, [Online] link

[15] Dr. U, Chandni – *The Tale of Facial Recognition Technology* –2022, [Online] link

[16] BELHUMEUR, Peter N., HESPANHA, Joao P., KRIEGMAN, David J – *Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection* – IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol. 19, No. 7, July 1997, [Online] link

[17] MAUSS, Ben – *Haar-like Features: Seeing in Black and White, An Introduction to Computer Vision, Part II,* 2021 [Online] link

[18] BAUMGARTNER, Helga – *Biometrikus adatok a géppel olvasható úti okmányokban – Az ICAO Doc 9303,* Safety and Security Sciences Review 6 : 1 pp. 1-8. , 8 p. (2024), [Online] link

[19] Dr. BALLA, József – *A biometrikus adatokat tartalmazó úti és személyazonosító okmányok biztonságnövelő hatása a határ- és közbiztonság alakulására* – Doctoral dissertation, 2019, [Online] link