

The Effectiveness of Artificial Intelligence Systems in Combating Electronic Terrorism Crimes

Dr. BAAZIZ Amel*

Lecturer "B", Algiers 3 University, (Algeria)

baaziz.amel@yahoo.fr

Received: 15/07 /2024

Accepted: 18/11 /2024

Published 15/01/2025

Abstract: This study aims to demonstrate the effectiveness of artificial intelligence systems in combating electronic terrorism crimes. AI applications are leveraged to process data on terrorists and high-risk suspects, with the objective of preempting criminal activities. Terrorist organizations have significantly enhanced their technological infrastructures, exploiting extensive datasets to conduct real-time analyses that support their operations and recruitment efforts via digital platforms. This study provides a detailed examination of AI's characteristics and the legal constructs surrounding electronic terrorism, alongside an in-depth analysis of how AI systems can be strategically employed to counteract cyber-terrorism. The paper concludes with key findings and actionable recommendation

Keywords: Electronic Terrorism Crime; Cyberspace; Artificial Intelligence.

ملخص: تبيان مدى فعالية أنظمة الذكاء الاصطناعي في التصدي لجرائم الإرهاب الإلكتروني، حيث تخضع بيانات الإرهابيين و المتهمين الخطيرين لتطبيقات الذكاء الاصطناعي التي تضطلع لكشف الجرائم قبل ارتكابها، فقد طورت التنظيمات الإرهابية قدراتها التكنولوجية بما سمح لها باستخدام بيانات ضخمة و تحليلها عبر الانترنت بغرض تسهيل عملياتها الإرهابية و التجنيد الإلكتروني للشباب عبر شبكة الانترنت، واشتملت الدراسة على بيان ماهية الذكاء الاصطناعي و التنظيم القانوني للجرائم الإرهابية الإلكترونية ، و كذلك بيان دور أنظمة الذكاء الاصطناعي في مواجهة الجريمة الإرهابية الإلكترونية و خلصنا في الأخير إلى نتائج و توصيات.

الكلمات المفتاحية : جريمة الإرهاب الإلكتروني، الفضاء السيبراني، الذكاء الاصطناعي.

*Corresponding author

1. Introduction:

Artificial intelligence technologies represent a paradigm shift in the technological landscape, heralding a new era in human history with their innovative applications across various life domains. The evolution of AI has been marked by substantial advancements, notably in the development of artificial neural networks that mimic cerebral functions. AI has become indispensable in numerous sectors, including law enforcement and crime prevention, where it plays a pivotal role in investigating and thwarting criminal activities. This is particularly relevant as AI may inadvertently facilitate the commission of crimes, such as cybercrimes, if not properly managed.

Moreover, the advent of novel criminal behaviors, especially those perpetrated via the internet like electronic terrorism, poses a grave security risk to global peace. These crimes are exacerbated by terrorist groups' adept use of cutting-edge technologies for coordination, operational planning, and cyber espionage. It is imperative, therefore, that investigative bodies harness AI's predictive capabilities to not only recognize and thwart such threats but also pinpoint the culprits behind them.

Given this backdrop, the core question this research addresses is:

- How effective are artificial intelligence systems in combating electronic terrorism crimes?

This paper will delve into two critical areas to address the research question. The first will define the essence of artificial intelligence and the characteristics of electronic terrorism crimes. The second will discuss the instrumental role of AI systems in combating these modern threats.

2. The Nature of Artificial Intelligence and Electronic Terrorism

Artificial intelligence represents a dual-edged sword. On one hand, it provides significant benefits, such as the ability to track and trace crimes and criminals efficiently. On the other hand, it poses substantial risks as terrorists exploit AI systems to orchestrate their nefarious activities. These systems enable them to harness vast amounts of data, which they analyze over the internet to streamline their operations and

enhance their recruitment efforts among the youth through digital channels.

This research paper explores the dual aspects encompassed by the concepts of artificial intelligence (first requirement) and electronic terrorism (second requirement).

2.1 The Concept of Artificial Intelligence:

The present study delineates the definition, characteristics, and classifications of artificial intelligence.

2.1.1 Definition of Artificial Intelligence:

Artificial intelligence (AI) is a subdivision of computer science. The definitions attributed to AI are varied, primarily because they aim to emphasize the diverse capabilities and potential applications that are cultivated within these systems to emulate human intelligence¹. Technologically, AI is advantageous as it facilitates smart devices in functioning adeptly and judiciously, by enabling them to assess and react to their environments effectively.”²

Marvin Lee Minsky³ a pioneer in the field, described AI as the process of creating computer programs dedicated to performing tasks that, until now, have been competently executed by humans. These tasks require sophisticated mental capacities such as cognitive learning, organized thinking, and memory retention. Furthermore, AI is viewed as a modern approach aimed at enhancing cognitive and mental operations in synthetic machines, equipping them with the capabilities to think, perceive, and make informed decisions.⁴

¹ Yasmine Abdel-Monim Abdel-Hamid, International Legal Challenges for the Regulation of Artificial Intelligence, Legal Journal, No. 3, British University, Egypt, (BSN), p. 3134.

² Nils J Nilson, The Quest of Artificial Intelligence: a history of Ideas and Achievements, Cambridge University Press, London,2010, p13.

³ Marvin Lee Minsky, Steps Towards Artificial Intelligence, Proceedings of the IRE, January,1961, pp 8-30.

⁴ As an example of this automated robot "Ross" manufactured by IBM, which was purchased by the renowned US law firm Baker & Hostetlers in 2017 where this robot quickly inspects millions of files in a single second as well as its

Practically, the concept of artificial intelligence leverages general-purpose technology with the goal of automating and enhancing the precision and breadth of decision-making processes in machines. It involves identifying obscure patterns and forecasting them within complex environments to resolve issues traditionally handled by humans, thereby augmenting their efficiency in specific tasks.⁵

Other definitions characterize artificial intelligence as an information system endowed with intellectual capabilities akin to those of humans, or as a computer application or machine that undertakes tasks typically performed by human beings.

It is also characterized as a method for controlling a computer or robot through a program that processes thoughts in a manner akin to intelligent human beings.⁶

From the definitions cited above, it becomes apparent that artificial intelligence is a branch of computer sciences that devises sophisticated strategies to program machines or robots. These programs enable machines to perform actions and generate outcomes similar to those achieved by human intelligence.

By comprehending the intricate mental processes conducted by the human brain during thought and translating these into analogous computational strategies, robots are empowered to tackle complex problems effectively.

2.2.2 Characteristics of Artificial Intelligence:

Artificial intelligence is characterized by several distinct features, including:

- The capability to process and analyze vast quantities of data.
- The aptitude to symbolically represent knowledge.

ability to familiarize itself with legislative developments and court rulings periodically.

⁵ Matthijs Maas, International Law does not compute: Artificial intelligence and the development, Displacement or destruction of the Global Legal Order, Melbourne, Journal of International Law, Vol 20, No1, 2019, p 2.

⁶ Artificial Intelligence consists in having a machine perform operations that we do with our intelligence, See: NEVEJANS (Nathalie), Treaty of Ethics of Civil Robotics; LEH Edition, 2017, p31.

- Employing a problem-solving approach analogous to that of human beings.
- The capacity for learning and adaptation.
- The ability to swiftly and accurately address assumptions.
- Handling incomplete or ambiguous information effectively.
- Solving intricate and multifaceted problems.
- Exhibiting evolution, creativity, and the capacity for understanding visual matters and perception.
- Making autonomous decisions without human intervention, based on the accumulated data.
- Utilizing experiences from the past and applying them to new, unseen scenarios.
- Employing logical reasoning to solve problems.⁷

2.2.3 Artificial Intelligence Types:

Artificial intelligence can be categorized based on its capacity and functionality.

A. Based on its Capacity: It is divided to three types:

➤ Limited or Narrow Artificial Intelligence:

This form of artificial intelligence is currently the most prevalent. It is designed to perform specific tasks, such as operating autonomous vehicles, recognizing speech and images, or playing chess as seen in various smart devices.

➤ General Artificial Intelligence:

This category embodies AI that possesses capabilities akin to human intelligence, enabling machines to think and plan independently, much like humans. Examples include artificial neural networks which simulate human cognitive processes.

➤ Superintelligent Artificial Intelligence:

This type of AI surpasses human capabilities, performing tasks more efficiently than humans specialized in those areas. It encompasses abilities such as advanced understanding, strategic planning, autonomous communication, and sophisticated judgment-making.

⁷ Laila Fighter, Haniya Hasan, Artificial Intelligence and Educational Applications for Educational Development, Human and Community Magazine, vol. 10, Issue 4, 2021, p. 114

Currently, this level of AI remains a theoretical concept without tangible realization.⁸

B. Based on its Functions:

- **Interactive Machines:** This is the most basic form of artificial intelligence, which does not possess the capability to learn from past experiences. Instead, it interacts with ongoing experiences to optimize performance.
- **Limited Memory:** These systems can store information from past interactions for a brief period, with autonomous driving systems being prime examples of this type.
- **Theory of Mind:** AI systems under this category are designed to understand human emotions and interactions, although practical applications of such technology are yet to be seen in the real world.
- **Self-awareness:** This advanced type of AI can predict future events and possesses a higher level of consciousness and awareness compared to humans. Currently, it is the subject of ongoing research and has not yet been actualized.⁹

2.3 Legal Organization of Electronic Terrorism Crimes:

In this section, the researcher endeavors to elucidate the nature of electronic terrorism crimes, delineate their constitutive elements, and exemplify various manifestations of such crimes.

2.3.1 Defining Electronic Terrorism Crimes:

Electronic terrorism is acknowledged within the framework of international agreements. The Shanghai Cooperation Organization Agreement on Information Security characterizes electronic terrorism as "the use or threat of using information resources for terrorist purposes." This threat primarily emanates from terrorist organizations engaging in unlawful activities. Notably, this definition emphasizes the exploitation of

⁸ Abdul Razak Mukhtar, Applications of Artificial Intelligence, International Journal of Educational Research, vol. 3, No. 4, 2020, p. 184-185.

⁹ Artificial intelligence, its most important applications, an article published on the website: <http://www.annajah.net/site/contact/>

information networks by these organizations to conduct terrorist acts and recruit new adherents.¹⁰

Furthermore, the Arab Agreement on Combating Information Technology Crimes addresses this phenomenon under Article 15. It defines electronic terrorism as "crimes associated with terrorism that are perpetrated through information technology." This includes the propagation of ideologies and principles of terrorist groups, advocating for these groups, financing terrorist operations, training, facilitating communication between terrorist organizations, and disseminating methodologies for manufacturing explosives used in terrorist operations.¹¹

2.3.2 Electronic Terrorism Crimes Elements:

The elements constituting electronic terrorism crimes distinguish themselves from those of traditional crimes, particularly in terms of the tools used for committing these crimes. Thus, the presence of both material and moral elements is essential, along with a specific condition: the crime must be committed using information technology means.

This condition is imperative, and its absence negates the criminal nature of the act, rendering the crime non-existent due to the absence of a criminal act. If another criminal description arises, the elements of such a crime are discussed as follows:

A. Material Element:

The material element in electronic terrorism crimes refers to the actions of the perpetrator that result in damage or harm to the external world, which is punishable by law. This element is bifurcated into two behaviors: positive and negative.

¹⁰ Agreement on cooperation in Ensuring International Information Security between the Member States of the SCO, (June 2022), available at: <http://eng.sectsc.org/load/207508/> accessed 20 April 2021.

¹¹ Baji Abdel Nour, Malik Naseema, Cyberterrorism: Between the Globalization of Crime and the Necessity of Combating, *Journal of Legal Studies and Research*, vol. 7, No. 2, 2022, p. 69

Positive behavior occurs when the individual refrains from an action commanded by the law, while **negative behavior** involves committing an act prohibited by the law. The outcome of these behaviors is significant in crimes that have consequential effects. Importantly, in assessing the material element of electronic terrorism crimes, the law does not take into account the means -whether tangible or intangible- used in committing the criminal act. The material element comprises three crucial components: the criminal behavior, the criminal outcome, and the causal link between them.

➤ **Criminal Behavior:**

Criminal behavior in the context of electronic terrorism crimes is characterized as the overt physical actions undertaken by the perpetrator to achieve a criminal outcome that is punishable by law. This behavior can be categorized as either positive or negative. Positive behavior involves deliberate actions where the perpetrator utilizes their physical faculties to produce tangible effects externally, thus constituting the crime and causing harm or presenting an external danger.

A key aspect of electronic terrorism crimes is the mandatory use of a device or computer with internet connectivity. Without such devices, the activity cannot be classified as an electronic crime. In these crimes, the perpetrator engages in technical activities within a digital environment, such as using remote control technology for remote detonation or employing applications like Google Earth to track and monitor the movements of potential victims.¹²

➤ **Criminal Outcomes:**

The legal consequences stemming from the criminal behavior define the criminal outcome. Electronic terrorism crimes are particularly severe in terms of their outcomes. The law presumes the danger posed by these outcomes, which may include enabling communication among the leaders and members of terrorist organizations, promoting terrorist ideologies, funding these activities, spreading training methodologies, or providing instructions for the production of incendiary or explosive devices.

¹² Zayn al-Abidin Awad Kazem al-Kurdi, *Information Terrorism Crimes, Comparative Study*, T1, Al-Halabi Rights Publications, Beirut, 2018, p. 88.

An electronic terrorism crime can be considered complete without the achievement of its intended outcome. For instance, the mere creation of websites intended to facilitate communication among members and leaders of a terrorist organization constitutes a crime, irrespective of whether the communication actually occurs, whether the network has users, or whether the website is accessed or not. The act of establishing the website is punishable by law, regardless of the fulfillment of its intended purpose.

➤ **Causal Relationship:**

The relationship between criminal behavior and the criminal outcome is a pivotal element for the completion of the material aspect of a crime. A causal relationship must exist between the criminal behavior and the resulting outcome for criminal responsibility to be established. However, in the context of electronic terrorism crimes, the necessity for a causal relationship between criminal behavior and its outcome is waived.

Given the gravity of these offenses, criminal responsibility is asserted as soon as an action is taken, such as creating a website or personal page with the intent of promoting terrorist ideologies or facilitating communication among members of terrorist organizations. For example, in cases of electronic espionage, merely unauthorized access to a website or information system through the internet or a computing device to acquire data that could compromise national security or impact the nation's economy is deemed a punishable criminal act.¹³

2.3.4 Forms of Electronic Terrorism Crimes:

The various forms of electronic terrorism crimes have multiplied due to the immense advancement in information technology. Terrorist groups utilize websites and electronic platforms to communicate with their members and leaders, recruit youth and teenagers, spread their ideologies, and finance their terrorist operations. Below are some of the most common forms of terrorism crimes:

¹³ Mohammed Ali Swilam, Crimes of Terrorism and Cyber Terrorism, Comparative Study, T1, Egyptian Publishing and Distribution, Cairo, 2018, p. 45.

A. The Crime of Youth Recruitment by Terrorist Organizations:

Terrorist organizations capitalize on the expansive reach of the internet to recruit and allure youth into their ranks, representing one of the most perilous forms of electronic terrorism. They harness the power of social media platforms to engage with individuals who express interest in joining their ranks, persuading them to embrace their ideologies, facilitating their relocation from current locations to conflict zones, propagating extremist rhetoric, and inciting them to acts of violence.

Terrorists strategically employ social media to propagate and broadcast their ideologies across various societal segments, particularly targeting economically disadvantaged and unemployed youth.¹⁴

B. The Crime of Promoting Terrorist Activities:

Terrorist organizations increasingly turn to the internet to foster a culture of terrorism and enhance their promotional efforts. They aim to attract and convert as many individuals as possible, encouraging them to adopt terrorist ideologies and integrate into their ranks.

This crime is often perpetrated through the dissemination of emails or messages via social media platforms, which are used to facilitate communication among terrorists, exchange pivotal information, and spread it among those engaged in terrorist schemes. Their primary goal is to maximize recruitment and ideological adoption.¹⁵

C. The Crime of Financing Terrorist Organizations:

Terrorist groups exploit the internet as a tool to finance their operations. This involves collecting donations under the facade of charitable activities. They establish counterfeit companies masquerading as charitable organizations, which are purportedly aimed at collecting

¹⁴ Ben Salem Iman, *Crime of Electronic Recruitment of Terrorism According to Algerian Law*, T1, Arab Democratic Center for Strategic, Political and Economic Studies, Berlin, 2018, p. 37.

¹⁵ Khaled Hassan Lutfi, *Cyber Terrorism, the Scourge of the Age, and the Legal Mechanisms to Confront It*, T1, Dar al-Thawr University, Egypt, 2018, P.215

funds for a noble cause, but instead, funnel these resources to support terrorist activities.¹⁶

D. The crime of electronic espionage:

Terrorist entities utilize the internet to conduct espionage against countries, organizations, and both international and national institutions. As espionage techniques have evolved from traditional to electronic methods with the advent of the information network, espionage now extends beyond national boundaries to encompass military sites and armament systems that are critical to national security. These sites can be accessed using spy satellites and satellite broadcasting technologies.

The information targeted by electronic espionage does not necessarily need to be classified; it suffices if it pertains to the internal or external security of the state or impacts its national economy. Electronic espionage often employs various communication means, with email serving as one of the most prevalent methods.¹⁷

2.4 Means of Electronic Terrorism:

Terrorist organizations employ a variety of methods and tools to achieve their goals, which include facilitating communication between the leaders and members of terrorist groups, as well as recruiting individuals and enticing them to join. One of the most prevalent techniques is the use of email to spread their ideologies and recruit members. Additionally, they create dedicated websites for these purposes. The following will explore these methods in greater detail.

2.4.1 Exchange Terrorist Data via the Internet:

Terrorist groups exploit the internet's capabilities for secure and rapid communication to exchange information among themselves. This is facilitated through various digital platforms such as websites, emails, forums, and online chat rooms. These channels enable several

¹⁶ Abdullah Saad al-Mahdi, Criminal Responsibility for the Crime of Electronic Finance of Terrorist Groups, Master's Thesis, University of Isra, 2018, p. 66.

¹⁷ Abdullah Mohammed Al-Nawaisa, Mamdouh Hassan Al-Adwan, Crimes of Cyber Espionage in Jordanian Legislation, Analytical Study, Journal of Law, and Sharia Studies, Majlid46, issue 1, p. 467.

individuals to meet virtually in multiple locations simultaneously, engaging in discussions and disseminating terrorist propaganda.

This propaganda often utilizes threats and intimidation to orchestrate or publicize specific terrorist acts. The overarching aim is to instill fear among individuals and governments alike, coercing them into acquiescing to the demands of these terrorist groups.¹⁸

2.4.2 Creating Terrorist Electronic Websites:

Terrorist organizations actively create and manage websites to spread their ideologies, recruit new members, and provide training. These websites offer detailed instructions on email hacking, website penetration, overcoming digital barriers, distributing viruses, and other electronic sabotage techniques. Such platforms often serve as virtual training camps, disseminating information on manufacturing bombs, preparing explosive devices, and offering training through electronic manuals or videotapes available on their platforms.¹⁹

2.4.3 Destruction of Websites and Information Systems:

Terrorist groups also engage in the destruction of digital infrastructure by executing cyber-terrorist attacks. These attacks aim to damage or completely disable information networks, causing significant harm to information infrastructure. Strategies include rendering websites inoperable, shutting down essential online services, and compromising command, control, and communication systems critical to national security.²⁰

3. The Role of Artificial Intelligence in Combating Electronic Terrorism Crime

In the realm of criminal justice, particularly in the modern era, the synergy between technology and law has become critically essential. This involves both the theoretical frameworks of law and the practical application of cutting-edge technologies such as artificial intelligence.

¹⁸ Osama Jaber al-Doh, *Crime of Cyberterrorism in Jordanian Legislation*, Master's Thesis, Al-Jerash University, 2016, p. 72

¹⁹ Mahmoud Saleh Al-Adali, *op. cit.*, p. 183.

²⁰ Hamza Mohammed Abu Issa, *IT Crimes, Comparative Study in Arab Legislation*, T2, Wael Publishing & Distribution House, Amman, 2019, p. 190.

There is a pressing need for criminal legislation to evolve in step with technological advances, particularly in applying legal norms to artificial intelligence systems.

AI plays a pivotal role in investigating and analyzing electronic terrorism crimes, as terrorist organizations increasingly adopt sophisticated and innovative technological methods. Thus, integrating artificial intelligence technologies into the digital forensic investigation of electronic crimes, including predicting and intercepting electronic terrorism activities, is imperative.

3.1 Digital Criminal Investigation in Electronic Terrorism

Digital criminal investigations of electronic terrorism involve leveraging digital technologies, cloud computing, data analysis, artificial intelligence, and various investigative tools and software. These resources aid investigative authorities in identifying, collecting, analyzing, and documenting crimes committed via online platforms or digital devices. The ultimate goal of these investigations is to gather digital evidence that can be used to prosecute suspects and secure convictions, thereby upholding justice.

3.1.1 Definition of Digital Criminal Investigation and its Importance:

Digital criminal investigation is defined as the process of probing crimes that are executed using electronic devices such as computers, smartphones, tablets, digital cameras, or any data storage devices. The primary objective of a digital criminal investigation is to preserve, identify, acquire, and document digital evidence that will be utilized in court to substantiate allegations of crimes committed with these electronic devices.

This investigative process extends to crimes perpetrated by terrorists through the use of electronic devices and the internet. Artificial intelligence systems play a pivotal role in these investigations by aiding criminal investigation agencies to determine the identity of the perpetrator through details such as usernames, email messages, or phone numbers collected during the investigation process. These systems have become instrumental in criminal evidence collection by extracting data

and information, which can serve as compelling evidence against the perpetrators involved.²¹

3.1.2 Methods of Digital Criminal Investigation in Electronic Terrorism:

The methodologies employed in the digital criminal investigation of electronic terrorism brain activity to detect and investigate information, avoiding the induction of nervous pressure. This technique aims to verify the presence or absence of crime-related information, thereby confirming or refuting the occurrence of the crime, with the brain as the central focus of the investigation.²²

3.2 Prediction of the Electronic Terrorism and Objection of Electronic Messages

The prediction of electronic terrorism crimes and the interception of electronic messages involve distinct but interrelated approaches. In the first part, the researcher discusses the application of artificial intelligence to predict electronic terrorism activities. In the second part, the focus shifts to explaining how electronic messages are intercepted.

3.2.1 Applications of Artificial Intelligence in Order to predict Electronic Terrorism Crimes:

Artificial Intelligence (AI) plays a pivotal role in preemptively detecting crimes, particularly those related to electronic terrorism. This preventive capacity is facilitated through the comprehensive analysis of big data, employing correlations between diverse data points to yield predictive insights, a technique referred to as "algorithmic crime prediction."²³

²¹ Mahmoud Salama Sharif, Legal Nature of AI Crime Prediction and Legitimacy, Arab Journal of Forensic and Forensic Sciences, Nayef Arab University of Security Sciences, Vol. 3, No. 2, 346.

²² Mahmoud Salama Sharif, op. cit., p. 350-351.

²³ Algorithms: They are defined as a set of sequential and sequential mathematical pathways and steps needed to solve a problem and the equipment programmatically to give a certain result based on the data and inputs you feed into.

Algorithms are instrumental in this process, utilizing extensive datasets to filter, scan, sort, analyze, understand, and process information. The vastness of the data enhances the accuracy of predictions, thereby improving decision-making processes.

Technological resources, such as networks of tracking devices including satellite imaging and data from mobile phones and GPS systems, are crucial in gathering this data. Additionally, behavioral data, such as frequency of internet access for information on bomb-making or visits to suspicious websites, play a significant role. Social media platforms like Twitter and Facebook, where individuals might post comments inciting violence against the state, also serve as valuable data sources for these predictive algorithms.

One notable AI application in this field is "PredPol," which identifies high-risk areas and potential perpetrators by analyzing a compilation of data, images, and videos. This system evaluates information related to individuals' activities on social media, along with personal addresses and criminal history, to assess the likelihood of someone committing a crime.²⁴

Another innovative AI application is the "Terahertz" system, designed to detect suicide bombers by identifying explosives concealed under clothing. This tool utilizes Terahertz radiation technology to scan and image hidden weapons, aiming to identify and intercept potential threats posed by individuals carrying concealed weapons.

3.2.2 Interception of Electronic Messages:

The interception of calls and electronic messages is a sophisticated technological strategy that requires advanced AI systems to effectively determine a suspect's involvement in criminal activities. Interception involves the monitoring of electronic communications by capturing electrical waves, collecting the transmitted data, converting it into readable formats, or recording it for further analysis. This process includes all transmitted data, which is then processed and converted to

²⁴ Abir Mohammed Asaad, Artificial Intelligence, Dar al-Bayda ', T1, 2017, P.18

reveal its content, subsequently serving as evidence against the suspected individual.²⁵

Legal frameworks often permit the interception of electronic messages and correspondences if it is deemed crucial for the investigation. This encompasses all forms of communications, including messages, emails, and phone calls, all of which are integral for uncovering the facts related to the commission of terrorist crimes.

4. Conclusion:

This study has underscored the efficacy of artificial intelligence (AI) techniques in combating electronic terrorism crimes. Algorithms, as fundamental components of AI, play a crucial role in analyzing extensive datasets related to criminal activities. This analysis is vital for producing effective predictions about the likelihood of future electronic terrorism incidents.

Terrorist organizations harness the power of the internet to disseminate their ideologies and recruit individuals, making use of various electronic platforms to engage and indoctrinate potential members. Thus, the establishment of robust legal frameworks is essential to shield individuals from the threats posed by electronic terrorism. The study has led to several key conclusions and actionable recommendations.

5. Results:

- ✓ Artificial intelligence is a dual-natured tool; it is invaluable in tracking crimes and criminals but also can be exploited by terrorist groups to perpetrate their offenses.
- ✓ AI significantly contributes to the reduction of electronic terrorism crimes.
- ✓ AI's effectiveness hinges on algorithms that manage data collection and analysis, enabling it to emulate cognitive functions such as thinking, decision-making, and executing plans.
- ✓ AI applications are instrumental in detecting potential electronic terrorism activities well in advance, providing

²⁵ Wijih Mohammed Suleiman, Artificial Intelligence in Crime Investigation, Al-Mezan Journal of Islamic Studies, University of Islamic Sciences of the World, Journal 3, Issue 3, 2022, p. 466.

authorities with a crucial window to counteract and prevent these crimes.

- ✓ Electronic terrorism crimes typically involve the use of information technology, which constitutes a core element of this crime type.
- ✓ Terrorist groups utilize the internet for communication, coordination, and information exchange among their members, employing platforms like email, forums, chat rooms, and internet meetings.
- ✓ The spectrum of electronic terrorism crimes is broad, with significant risks arising from terrorists' use of the internet to recruit members, spread propaganda, orchestrate terrorist activities, and fund their operations through online channels.

6. Recommendations:

Based on the insights garnered from this study, the following recommendations are put forth:

- ✓ Vigilant monitoring and blocking of suspicious websites that promote terrorism and extremist ideologies are imperative.
- ✓ There is an urgent need to enhance societal and internet user awareness regarding the dangers of electronic terrorism, including its various forms and the means to combat it.
- ✓ Educational institutions such as families, schools, universities, as well as media outlets and social media platforms, should actively participate in preventing electronic terrorism. This involves promoting awareness about the threats posed by such activities to individuals, society, and the state at large, and emphasizing the cultivation of strong ethical and religious values.

7. References:

- Abdel Ilah Muhammad Al-Nuwaysa, Mamdouh Hassan Al-Adwan, Electronic Espionage Crimes in Jordanian Legislation: An Analytical Study, Journal of Legal and Sharia Studies, Volume 46, Issue 1.
- Abdel Razzaq Mukhtar, Artificial Intelligence Applications, International Journal of Educational Research, Volume 3, Issue 4, 2020.
- Artificial Intelligence, Its Most Important Applications, an article published on the website: <http://www.annajah.net/site/contact>.

-Bayaji Abdounour, Malek Nsima, Electronic Terrorism: Between Globalization of Crime and the Necessity of Combatting it, Journal of Legal Studies and Research, Volume 7, Issue 2, 2022.

-Ben Salem Iman, The Crime of Electronic Recruitment for Terrorism According to Algerian Law, 1st edition, Arab Democratic Center for Strategic, Political, and Economic Studies, Berlin, 2018.

-Hamza Mohammad Abu Issa, Information Technology Crimes: A Comparative Study in Arab Legislation, 2nd edition, Wael Publishing and Distribution House, Amman, 2019.

-Khaled Hassan Latifi, Electronic Terrorism: A Contemporary Menace and Legal Mechanisms to Combat it, 1st edition, Dar Al-Fikr Al-Jamee, Egypt, 2018.

-Leila Moqatel, Hania Hassan, Artificial Intelligence and its Educational Applications for Developing the Educational Process, Journal of Humanity and Society, Volume 10, Issue 4, 2021.

-Marvin Lee Minsky, Steps Towards Artificial Intelligence, Proceedings of the IRE, January 1961.

-Matthias Maas, International Law does not compute: Artificial intelligence and the development, Displacement or destruction of the Global Legal Order, Melbourne, Journal of International Law, Vol 20, No 1, 2019.

-Mohammed Ali Suleim, Terrorism and Electronic Terrorism: A Comparative Study, 1st edition, Egyptian Publishing and Distribution, Cairo, 2018.

-Nathalie Nevejans, Treaty on Civil Robotics Law, and Ethics; LEH Edition, 2017.

-Nils J. Nilson, The Quest of Artificial Intelligence: A History of Ideas and Achievements, Cambridge University Press, London, 2010.

-Osama Jaber Al-Dawh, Electronic Terrorism in Jordanian Legislation, master's Thesis, Jerash University, 2016.

-Yasmin Abdel Moneim Abdel Hamid, International Legal Challenges of Regulating Artificial Intelligence, Legal Journal, Issue 3, British University, Egypt.

-Zain Al-Abidin Awad Kazem Al-Kurdi, Information Terrorism Crimes: A Comparative Study, 1st edition, Al-Halabi Legal Publications, Beirut, 2018.