International Journal of Religion
2024
Volume: 5| Number 11 | pp. 975 – 985
ISSN: 2633-352X (Print) | ISSN: 2633-3538 (Online)
ijor.co.uk
DOI: https://doi.org/10.61707/7hj3ys81

Artificial Intelligence and Nurturing Electronic Terrorism

Monther Abed-Alrazzaq Musleh Al-Amaireh [1]

Abstract

The purpose of the study was to review and analyze the techniques and tools used by cyber terrorists in exploiting artificial intelligence, and to understand how artificial intelligence contributes to enhancing the capabilities and effectiveness of cyber terrorism.the importance of this study is to understand the effects of using artificial intel ligence on fueling cyber terrorism and increasing its effectiveness, and identify the challenges facing counter-terrorism operations. the study followed the descriptive analytical approach to describe the legal framework for artificial intelligence and fueling cyber terrorism, and analyzing legal texts.

Keywords: *Artificial Intelligence, Electronic Terrorism, Nurturing.*

INTRODUCTION

The modern era is witnessing rapid advancements in technology, and among the emerging technologies that humanity is actively exploring and applying is the field of artificial intelligence. Artificial intelligence is considered a multidisciplinary field aimed at enabling computer systems to learn, think, and make decisions in a manner similar to human intelligence. Artificial intelligence has revolutionized various fields such as medicine, industry, commerce, and even the daily lives of individuals.

However, rapid technological development brings new and complex challenges, one of which is the use of artificial intelligence to fuel cyberterrorism. The world faces increasing threats from extremist and terrorist groups that exploit modern technologies to promote their violent ideas and disseminate terrorist content online. This is where artificial intelligence may potentially play a role in enhancing and facilitating such harmful activities.

The use of artificial intelligence in generating and widely disseminating terrorist content poses a serious challenge to global cybersecurity. Artificial intelligence can learn from online data and interactions, producing extremist content faster and more efficiently, thereby promoting the spread of extremist ideas and increasing the recruitment of extremists. The main challenge is how to identify and effectively monitor this extremist content and address it.

Combating the use of artificial intelligence to fuel cyberterrorism requires a multidisciplinary approach that combines legal, technological, and security fields. Tools and techniques capable of automatically detecting and analyzing extremist content must be developed. The identification of models and patterns used by extremists in promoting their ideas is also essential. Additionally, challenges arising from the use of artificial intelligence in cyberterrorism must be addressed. We must be aware of the delicate balance between freedom of expression and the need to protect societies from extremist and violent ideas. Efforts should be made to develop effective policies and a legal framework to combat cyberterrorism, including regulating the use of artificial intelligence and implementing necessary measures to prevent its exploitation in terrorist activities.

In addition, we must work on developing pattern recognition and big data analysis techniques to detect and combat potential terrorist activities. Artificial intelligence can play a crucial role in improving our ability to quickly and accurately identify suspicious patterns, thus enabling us to more effectively counter electronic terrorist threats.

In this research, we will explore the relationship between artificial intelligence and the promotion of cyberterrorism. We will analyze the challenges we face in combating this type of harmful activity and explore

[1] Middle East University, Faculty of Law, Jordan, E-mail: montheram@hotmail.com

the potential applications of artificial intelligence in addressing these threats. We will also discuss the ethical and legal aspects associated with the use of artificial intelligence in this context.

Understanding this complex relationship between artificial intelligence and the promotion of cyberterrorism contributes to directing our efforts towards developing effective strategies and tools to combat this growing threat by responsibly and positively utilizing technology. We can enhance our cybersecurity and maintain safe and thriving communities in the age of artificial intelligence.

Research Problem: The research problem revolves around understanding how artificial intelligence is used to fuel and enhance cyberterrorism, and how to develop effective strategies and solutions to tackle this complex challenge. It involves analyzing the methods and tools that can be employed in generating extremist content, studying mechanisms for its identification and monitoring, and developing robust tools and solutions to combat this increasing phenomenon.

Research Questions

What is meant by artificial intelligence and cyberterrorism?

What are the techniques and tools used by cyberterrorists to exploit artificial intelligence?

How can artificial intelligence contribute to enhancing the capabilities and effectiveness of cyberterrorism?

What impact can the use of artificial intelligence have on increasing cyberterrorism threats?

What are the primary security and ethical challenges associated with the evolution of artificial intelligence and the promotion of cyberterrorism, and what are the ways to combat them?

What are the possible methods for identifying and monitoring artificial intelligence-supported terrorist activities?

Research Objectives

Clarify the concepts of artificial intelligence and cyberterrorism, providing precise and comprehensive definitions for both.

Review and analyze the techniques and tools used by cyberterrorists to exploit artificial intelligence.

Understand how artificial intelligence can contribute to enhancing the capabilities and effectiveness of cyberterrorism.

Evaluate the impact that the use of artificial intelligence can have on increasing cyberterrorism threats and identify the security and ethical challenges associated with this.

Review international efforts and initiatives by institutions in combating the use of artificial intelligence in promoting cyberterrorism and identify the challenges they face.

Identify possible methods for identifying and monitoring terrorist activities supported by artificial intelligence.

Research Significance

The significance of the research lies in understanding the effects of using artificial intelligence on the promotion of cyberterrorism and its increased effectiveness. It also helps identify the challenges facing efforts to combat cyberterrorism. Furthermore, the research raises public awareness about the potential threats that the use of artificial intelligence in fueling cyberterrorism can pose.

RESEARCH METHODOLOGY

Analytical Approach: This approach will be adopted to analyze relevant legal texts and to examine the jurisprudential opinions related to the subject of the study.

Descriptive Approach: This approach will describe the legal framework of artificial intelligence and cyberterrorism.

Previous Studies

Study by Farida Ben Amrouche, "Cyberterrorism: A Study on the Conceptual and Dimensional Issues," Algerian Journal of Social and Human Sciences, University of Ibrahim Sultan Chibout, Algeria, Vol. 8, No. 2, 2020.

The technological revolution and advancement in our contemporary era have transformed the way of life worldwide. Modern information technology is increasingly integrated into various aspects of economic, political, and social life. Computers have become integral to financial institutions, public facilities, education, and security. However, it is impossible to ignore the negative uses of these modern technologies. One of the manifestations of these negative uses is cyberterrorism, which has become a global concern, frightening the world exposed to online terrorist attacks.

Cyberterrorists conduct their criminal activities from anywhere in the world behind their electronic screens. These risks are intensifying every day because modern technology alone cannot protect people from cyberterrorism operations, which have caused significant harm to individuals, organizations, and nations. Many countries and international organizations have sought to take the necessary measures to combat cyberterrorism. Still, these efforts have proven insufficient to address this dangerous weapon.

Study by Reem Abdel Mageed, "Applications of Artificial Intelligence and the Phenomenon of Terrorism," Diplomatic Affairs Journal, British Libyan University - Institute of Diplomatic Studies, Vol. 7, No. 4, Libya, 2020.

With the rapid pace of technological advancement in general and artificial intelligence with its various applications, especially in the military context, concerns have been raised about the risks of this development on national, regional, and global security. There are growing fears regarding the use of these technologies by terrorist groups. In this context, the research question for this study is: What is the impact of the development of artificial intelligence applications on the phenomenon of terrorism? The study concluded that these applications facilitate the spread of the terrorism phenomenon due to the advantages they provide to terrorist groups. Furthermore, artificial intelligence can also be used to combat terrorism and attempt to limit its spread.

RESEARCH STRUCTURE

Chapter 1: The Nature of Artificial Intelligence and Cyberterrorism.

Requirement 1: Definition of Artificial Intelligence and Cyberterrorism.

Requirement 2: Causes, Characteristics, and Objectives of Cyberterrorism.

Chapter 2: The Impact of Using Artificial Intelligence in Increasing Cyberterrorism Threats

Requirement 1: Analyzing the impact of using artificial intelligence in enhancing terrorists' ability to carry out cyberattacks.

Requirement 2: The risks associated with the development of artificial intelligence and fueling electronic terrorism, and combating them.

CHAPTER 1

The Nature of Artificial Intelligence and Cyberterrorism

In the modern era, technology is undergoing rapid and exponential advancement, giving rise to a new challenge concerning artificial intelligence and its impact on various aspects of life, including cybersecurity and counterterrorism. Cyberterrorism is considered one of the emerging threats that involve the use of technology and artificial intelligence for malicious purposes.

Cyberterrorism can be defined as the utilization of technology and computer systems to carry out terrorist acts or cause significant harm in the digital world. This includes electronic hacking, cyber fraud, electronic espionage, cyberattacks on the critical infrastructure of a country or organization, and influencing the global economy and vital systems.

The First Requirement

Definition of Artificial Intelligence

Section 1: Definition of Artificial Intelligence

Artificial intelligence can be defined as a field that focuses on the development of systems and technologies capable of executing tasks deemed intelligent in a manner resembling human behavior. The goal of artificial intelligence is to design and construct systems that can process information, make decisions, and solve problems in a manner that resembles or approximates human performance.

When researchers talk about making machines behave like those in science fiction movies, it refers to the ambition of developing systems with extraordinary capabilities, including self-learning, artificial thinking, communication, and intelligent interaction with the environment and humans. While significant progress has been made in these fields, there are still substantial challenges in achieving a similar level of human-like intelligence.

Today's computers have the ability to process numbers and solve complex mathematical problems quickly and accurately. However, there are other aspects of human intelligence, such as communication, social interaction, creative thinking, and deep learning, which pose challenges for artificial intelligence. The human mind consists of a complex network of millions of interconnected nerve cells, and researchers suggest that replicating this level of complexity currently exceeds human capabilities.

Section 2: Definition of Cyberterrorism

The definition of terrorism has been diverse and varied due to the multiplicity of its forms, patterns, methods, and objectives, as well as the differences in international perspectives, political directions, and the various beliefs and ideologies held by different countries. What some parties consider as terrorism may be seen as a legitimate act by others.

Article 147 of the Jordanian Penal Code No. 10 of 2022 defines terrorism as any act aimed at creating a state of panic and is committed using explosive, inflammable, and toxic substances, or epidemiological and bacterial agents that pose a public threat. In the Egyptian law, terrorism is defined as the use of force, violence, threat, or intimidation with the intent of disrupting public order or jeopardizing the safety and security of society. This includes harming individuals, causing terror among them, endangering their lives, freedoms, and security, as well as causing harm to the environment, public and private facilities, hindering or obstructing the exercise of public authorities, religious institutions, educational institutions, or impeding the application of the constitution, laws, or regulations.

Within the framework of the Arab Convention for the Suppression of Terrorism, terrorism is defined as any act of violence or threat thereof, regardless of its motives or objectives, aimed at causing fear, intimidation, or harm to the environment, public or private facilities, or exposing national resources to danger.

Based on these definitions, cyberterrorism can be broadly defined as aggression, intimidation, or physical or moral threats against individuals in their religion, themselves, their property, using computing and electronic network technologies, with the aim of disabling computer systems, stealing sensitive information and data, intimidating individuals and groups in the digital world. Cyberterrorism includes activities such as forced hacking of computer systems, spreading viruses and spyware, electronic fraud, threats via email and social media, electronic piracy, offensive cyber hacking, online defamation, and sabotage or disruption of websites, government, and commercial systems.

The Second Requirement

Causes, Characteristics, and Objectives of Cyber Terrorism

Section One: Causes and Motives of Cyber Terrorism

The reasons and motives for cyber terrorism vary based on numerous factors, and among these reasons are:

Potential General Reasons for Cyber Terrorism

Revenge and Anger: Cyber terrorism may be a response to anger and a desire for revenge against specific entities, whether they are countries, organizations, or specific individuals. Individuals or groups can use cyberattacks as a means of seeking retribution for perceived injustices or to have an impact on a specific target.

Political and Social Influence: Extremists and terrorist groups may use cyberattacks as a means to achieve political or social goals. Government structures, governmental institutions, and other political targets can be targeted to disrupt or undermine their authority.

Extremist Ideology: Extremist ideology can play a significant role in driving individuals to commit acts of cyber terrorism. Individuals or groups may promote extremist ideas, whether religious or ideological extremism, and consider cyberattacks a means to achieve their goals and propagate their extremist visions.

Financial Support and Financing: Cyber terrorists may resort to conducting attacks to generate funds and finance their activities. This can include stealing financial information, attacking financial institutions, or using encrypted digital currencies to fund their terrorist activities.

Weaknesses in Cybersecurity: Attackers may exploit vulnerabilities in electronic security systems to carry out terrorist attacks. If cybersecurity structures are weak or lack necessary protection, it may become easier for attackers to exploit these vulnerabilities to access sensitive information or disrupt critical infrastructure.

Intellectual Motivations

Intellectual motivations for terrorism play a significant role in encouraging individuals to commit acts of terrorism. These motivations include:

Ignorance and Misinterpretation of Religion: Ignorance and the misinterpretation of religion can play a significant role in driving individuals toward terrorism. Some individuals may exploit ignorance and misinformation to promote extremist ideas and provide a distorted interpretation of religious teachings, pushing individuals to commit violent or terrorist acts.

Intellectual Divisions: Intellectual divisions and differences between various ideological currents can encourage individuals to resort to terrorism. Intellectual divisions may arise due to differences in political, social, cultural, and religious visions, and some groups exploit these divisions to recruit individuals and incite them to violence.

Extremism: Extremism is a serious factor in driving individuals toward terrorism. Extremism involves adopting radical ideas, rigid views, and a rejection of peaceful coexistence, dialogue, and tolerance. Extremism may be exploited to justify violence and terrorism and incite individuals to commit violent acts targeting communities and other individuals.

Political Motivations

Political motivations play a significant role in the phenomenon of terrorism, including:

Social Injustice and Inequality: The absence of social justice and inequality in the distribution of wealth, services, and economic opportunities can be a motivation for terrorism. When individuals and communities feel they are suffering from injustice and are not receiving their basic rights and opportunities to improve their living conditions, they may resort to violence and terrorism as a means to express their anger and achieve their demands.

Political Persecution and Oppression: Political persecution and oppression by governments or authoritarian entities can be a motivation for terrorism. When individuals and communities suffer from political persecution and violations of their basic rights and freedoms, they may turn to organized violence and terrorism to resist and confront oppressive regimes.

Violation of International Laws and Agreements: Violating international laws and agreements, colonial control, and the plunder of natural resources can be a motivation for terrorism. When some communities and peoples experience economic and political exploitation and injustice by global powers, a sense of anger and resentment may arise, driving some individuals to resort to violence and terrorism as a means of resistance and achieving just demands.

The Jordanian Penal Code criminalizes terrorism, indicates its forms and means of use, and specifies the penalties that apply to its perpetrators. Article (147) stipulates that: 1 - Terrorism means, if its motives and purposes are, the use of violence by any means or the threat of its use, i.e. an individual or collective criminal project aimed at endangering terrorism. The safety and security of society is at risk if in implementation of this, those who do so create terror among people, intimidate them, endanger their lives, cause damage to the environment, public facilities and property, private property, international facilities, or diplomatic missions, or by occupying or seizing any of them, or exposing national resources to danger, or Forcing any government or any international or regional organization to carry out any action or to abstain from it. The article in the first paragraph defines terrorism and clarifies its elements, which we have previously explained.

Section Two: Characteristics of Cyber Terrorism and Its Goals

Cyber terrorism has a set of characteristics that distinguish it from other criminal activities. Cyber terrorism seeks to achieve illegal goals and is often associated with the digital sphere and the use of modern technology.

First: Characteristics of Cyber Terrorism

There are several features and characteristics that distinguish cyber terrorism, such as:

Non-Reliance on Violence: Cyber terrorism is characterized by not relying on physical violence or bodily force. Instead, it only requires the presence of a computer connected to the network and specific software.

Crossing Borders: Cyber terrorism is a crime that transcends geographical boundaries, extending beyond countries and continents. It is not limited to a specific regional scope.

Difficulty of Detection: Security and judicial systems face challenges in detecting cyber terrorism crimes due to a lack of expertise in dealing with these crimes.

Difficulty of Proof: It is challenging to prove cyber terrorism crimes since digital evidence can be quickly destroyed or erased, making the process of collecting evidence a significant challenge.

Multi-Party Collaboration: Cyber terrorism is executed through the collaboration of several individuals working together to carry out criminal activities over the network.

Technical Expertise: Perpetrators of cyber terrorism are typically well-versed in information technology or possess knowledge and experience in dealing with computer systems and networks.

Second: Objectives of Cyber Terrorism

Cyber terrorism aims to achieve several illegitimate objectives. The primary objectives can be summarized as follows:

Spreading Fear and Terror: Cyber terrorism seeks to create an atmosphere of fear and terror among individuals, nations, and societies by executing criminal acts over the internet. This can lead to a disruption of public safety and instability.

Infrastructural Destruction: Cyber terrorism aims to cause harm and destruction to information technology infrastructure. It targets the disabling and destruction of communication systems, information technology, and causes damage to public and private property and facilities.

Fund Collection: Cyber terrorism utilizes its means to gather the necessary funds for financing terrorist operations. This can be accomplished through fraudulent operations and penetration of financial systems or through deceptive activities on the internet, contributing to funding the activities of terrorist groups.

CHAPTER TWO

The Impact of Using Artificial Intelligence in Increasing Cyber Terrorism Threats

The evolution of communication methods and the availability of information on the internet have led to the emergence of a new form of terrorism known as "cyber terrorism." Cyber terrorism employs computer devices, scientific, and technological techniques to execute terrorist acts that may be challenging to carry out in physical reality. These acts can be executed by an individual with the competence and the ability to utilize information technology.

The term "cyber terrorism" was introduced in the 1980s by Colin Barry. He defined it as an electronic attack aimed at either threatening governments or assaulting them with the intention of achieving political, religious, or ideological goals. James Lewis pointed out that computer network tools are used to destroy or disrupt vital national infrastructure, such as energy, transportation, and government operations, or to intimidate governments or civilians.

The First Requirement

Analysis of the Impact of Using Artificial Intelligence in Increasing the Capability of Terrorists to Execute Cyber Attacks

Cyberterrorism is closely linked to ongoing scientific and technological advancements, as the more technology and information systems progress, the greater the risks of cyberterrorism become. Consequently, there is an interactive relationship between technological advancement and the increased threat of cyberterrorism.

Advanced technologies like artificial intelligence offer a multitude of capabilities, enabling machines to simulate human intelligence. When humans engage with events and situations, they sense and comprehend what's happening around them, make decisions based on that knowledge, and act accordingly. Similarly, smart devices equipped with artificial intelligence technologies behave in the initial stages based on human-like behaviors.

The phenomenon of terrorism, in particular, evolved with the emergence of the internet and social networks. These technologies have become essential tools for terrorist groups. By using the internet and social media, terrorists can expand their recruitment, purchase weapons, disseminate hate messages, promote educational programs, and more. Additionally, these technologies have been employed to develop tools for targeting specific groups by identifying them and carrying out attacks against them.

Terrorist groups have increasingly relied on artificial intelligence technology to expand their reach and expedite their activities. Artificial intelligence allows these groups to widen the scope of their operations, aiding them in recruitment and planning for their operations.

A report by the United Nations Office of Counter-Terrorism highlights the use of artificial intelligence by terrorist groups. The report suggests that terrorists are typically among the early adopters of new technology, especially when the technology is relatively unregulated and widely available. Consequently, while we witness technological advancements that contribute to our progress and development as humans and help preserve our existence, terrorists are also acquiring new tools they can use as weapons to spread fear, with artificial intelligence being no exception.

The potential malicious uses of artificial intelligence include enhancing cyberattacks, such as Distributed Denial of Service (DDoS) attacks, utilizing artificial intelligence to develop malicious software, deploying it in ransomware programs, facilitating password guessing operations, bypassing CAPTCHA security, using self-

driving vehicles in terrorist attacks, employing drones equipped with facial recognition capabilities, and developing genetically targeted biological weapons.

On the other hand, artificial intelligence can be used for big data analysis to identify new targets for terrorist attacks, directing terrorist groups in planning and executing their operations more effectively and tactically.

It is clear that this advancement in the use of technology and artificial intelligence in terrorism poses a significant challenge to global efforts to combat terrorism. Addressing this evolving threat requires international cooperation and effective information sharing among countries, security organizations, and intelligence agencies.

Globally, governments, international organizations, and technology companies are working on developing tools and techniques to detect and counter the use of artificial intelligence in terrorism. Governments and institutions must take necessary measures to enhance cybersecurity and raise awareness among citizens about potential terrorist threats associated with artificial intelligence.

Furthermore, international organizations should enhance international cooperation in the fight against terrorism, including information and expertise sharing. International platforms such as the United Nations, the European Union, and INTERPOL can play a vital role in facilitating this cooperation and developing effective strategies to combat the use of artificial intelligence in terrorism.

There should also be a focus on developing defensive technology to counter the use of artificial intelligence in terrorism. Researchers and technology engineers should work on developing automatic analysis and anomaly detection systems and tackling cyberattacks utilizing artificial intelligence.

In general, combating the use of artificial intelligence in terrorism requires multi-faceted and integrated efforts that combine legal, technological, intelligence, and international cooperation aspects.

Therefore, the relationship between artificial intelligence and cyberterrorism is complex and continually evolving. Artificial intelligence can contribute to the spread of extremist content that incites terrorism. Terrorists and extremists use artificial intelligence for recruitment purposes and disseminate extremist ideas. They can use algorithms supported by artificial intelligence to identify individuals who may be vulnerable to their ideology, such as those dealing with depression, loneliness, or showing interest in violence and adventure. They may also target non-religious individuals and seekers of belonging. Thus, artificial intelligence can be used to create and disseminate extremist content more rapidly and effectively. Natural language processing algorithms can be used to create lifelike virtual personas, and through simulation techniques using fake voices and images of fictitious characters, extremist content can be distributed and promoted as authentic posts on social media platforms, websites, messaging applications, and more. The use of chatbots and other automated systems allows this material to spread quickly and reach a larger audience with less effort.

While the Jordanian law includes general mechanisms for combating cyberterrorism, as mentioned earlier, it does not specifically address the use of artificial intelligence in cyberterrorism. There are no provisions in the Jordanian Penal Code or the Cybercrime Law that specifically deal with the use of artificial intelligence in cyberterrorism or incitement to cyberterrorism through artificial intelligence applications. Here, the researcher emphasizes the need for new legislation that includes penalties for cyberterrorism, whether it involves the use of artificial intelligence for terrorist purposes or incitement to terrorism through artificial intelligence applications or other means.

The Second Requirement

Risks Associated with the Advancement of Artificial Intelligence and Nourishing Electronic Terrorism, and How to Combat It

Technology and the development of artificial intelligence have made significant progress in recent decades, which raises genuine concerns about the negative use of this technology in fostering electronic terrorism. Electronic terrorism is a matter that requires immediate attention and action, as it can pose a threat to the

security of countries, institutions, and individuals. The development of artificial intelligence provides terrorists with new opportunities for planning, executing, and promoting their terrorist activities.

The First Subsection: Risks Associated with the Advancement of Artificial Intelligence and Nourishing Electronic Terrorism

Spread of Terrorist Propaganda: Artificial intelligence can be used to produce and distribute terrorist content on a wide scale, increasing the ability of terrorist groups to recruit extremists and influence them.

Cyber Attacks: Terrorists can use artificial intelligence to execute advanced cyber-attacks on critical infrastructure and government institutions, leading to service disruptions and the theft of sensitive information.

Manipulation of information: Artificial intelligence can be used to produce and distribute misleading and fake information, affecting public opinion and undermining social and political stability.

Development of smart weapons: Artificial intelligence can be used to develop advanced smart weapons, such as drones and combat robots, increasing the terrorists' capability to carry out deadly and destructive attacks.

Second Subsection: Measures to Combat Risks

These measures include:

Enhancing international cooperation: Countries should enhance cooperation and information sharing to combat cyberterrorism, including the sharing of intelligence data and collaboration in developing security technologies.

Strengthening legal frameworks: Countries should establish strict laws and regulations to combat cyberterrorism and the unlawful use of artificial intelligence for terrorist purposes. These laws should include deterrent penalties for individuals and entities that use technology in illegal ways.

Development of security technologies: Technology companies and security organizations should work on developing advanced security technologies to detect and combat online terrorist activities. This includes the use of artificial intelligence and machine learning to identify terrorist behavior patterns and counteract them.

Enhancing Awareness and Education: Institutions and governments should promote awareness and education regarding the risks of cyberterrorism and its negative impact. Training and resources should be provided to the public and organizations to recognize attack patterns and establish strong security practices.

Collaboration with the Private Sector: Governments and security agencies should collaborate with private companies and organizations to exchange information and expertise and develop effective solutions to combat cyberterrorism.

Combating cyberterrorism poses a significant challenge for countries and institutions. Addressing it requires international cooperation, the development of appropriate laws and regulations, and the enhancement of technological and security capabilities to counter these threats. Many countries and international organizations are working on establishing a legal and technical framework to combat cyberterrorism while promoting awareness and training in this field.

It's worth noting that digital freedom and individuals' rights online are also important aspects of the dialogue on combating cyberterrorism. Efforts to combat cyberterrorism should be conducted in a way that simultaneously preserves individuals' rights to privacy, freedom of expression, and access to information.

CONCLUSION

The issue of feeding cyberterrorism through artificial intelligence poses a significant challenge in the modern age. Artificial intelligence provides terrorist organizations, extremist groups, and their associated individuals with new opportunities to carry out more sophisticated and destructive cyberattacks. Through this research, we have reviewed the key issues related to the utilization of smart technology to fuel cyberterrorism, providing a

comprehensive analysis of the causes and challenges. Artificial intelligence represents an advanced field aimed at designing systems capable of performing intelligent tasks that approach human capabilities. Despite advancements in this field, there are substantial challenges that require sustainable solutions. Cyberterrorism encompasses various activities, including electronic penetration, fraud, espionage, and cyberattacks.

RESULTS

Artificial intelligence can increase the complexity and effectiveness of cyberterrorist attacks while reducing their detection.

Terrorist organizations benefit from artificial intelligence to develop advanced tools and software for launching cyberattacks.

Challenges are associated with the difficulty of detecting and punishing cyberattack perpetrators due to the complex nature of technology and the attackers' adept disguises.

Cyberterrorism is driven by various motivations, including revenge, anger, extremist ideologies, political motives, and personal gain.

Cyberterrorism is characterized by unique attributes such as the absence of physical violence and the ability to transcend geographical boundaries.

Cyberterrorism aims to achieve unlawful objectives, such as spreading fear, causing infrastructure damage, and raising funds to finance terrorist activities.

RECOMMENDATIONS

Enhance International Cooperation: Expand cooperation among countries to share information and develop common strategies to combat the feeding of cyberterrorism using artificial intelligence.

Strengthen Training and Education: Provide specialized training for security and technical personnel to enhance their understanding of emerging threats related to artificial intelligence and cyberterrorism.

Develop Legislation: Update and develop legislation and laws to be more effective in combating the feeding of cyberterrorism and holding perpetrators accountable.

Enhance Cybersecurity: Improve cybersecurity at both government and corporate levels to mitigate electronic threats.

REFERENCES

Legal Books

Abdul Aziz bin Ibrahim Al-Shabal, Electronic Initiation: A Jurisprudential Study, Zahra of Sevilla Publishing and Distribution House, First Edition, 2012.

Adel Abdel Sadek, Electronic Terrorism: A New Pattern and Different Challenges in International Relations, First Edition, Al-Ahram Center for Political and Strategic Studies, Cairo, 2009.

Adel Abdulnour, An Introduction to the World of Artificial Intelligence, Publications of King Abdulaziz University, 2005.

Ahmed Hussein Al-Suwaidan, International Terrorism in Light of International Changes, Beirut, Al-Jebli Legal Publications, 2005.

Ali Adnan Al-Fayyad, Electronic Crime: A Comparative Study, Zain Legal Publications, First Edition, 2011.

Dr. Jameel Abdul Baqi Al-Sagheer, Confronting the Criminality of Hacking Paid Television Programs, Dar Al-Nahda Al-Arabiya, 2002.

Mustafa Mohammed Musa, Cyberterrorism: A Legal, Security, and Social Study, Jordan: Dar Al-Easar for Publishing and Distribution, 2015.

Mustafa Yousef Kafi, Maher Odeh, Mahmoud Ezzat Al-Lahham, Media and Electronic Terrorism, Jordan: Dar Al-Easar for Publishing and Distribution, 2015.

Nabil Ahmed Helmy, International Terrorism According to the Rules of International Public Law, Dar Al-Nahda Al-Arabiya, Cairo, 1988.

Nooran Shafik, The Impact of Electronic Threats on International Relations, Cairo, The Arab Office for Knowledge, 2015.

Ziad Abdul Karim Al-Qadi, An Introduction to Artificial Intelligence, First Edition, Safaa Printing, Publishing, and Distribution House, 2010.

Laws and Regulations:

Jordanian Penal Code No. 10 of 2022.

Agreements:

The Arab Convention for Combating Terrorism, Entry Date 28/9/2023.

Published Research:

Mohamed Moanes Mahboub El-Din, Regional Terrorism, Security Strategies, Research presented within the 50th Scientific Conference Legislation to Combat Terrorism in the Arab World held in Sudan 7-1998/12/9.

Abdullah bin Abdulaziz bin Fahd Al-Ajlan, Cyberterrorism in the Information Age, Research presented at the First International Conference on Information Security and Privacy in Internet Law, held in Cairo from 2-4 July 2008.

Yousef Haggag, Electronic Crime: The Problem of Procedural Rules, Legal Articles, the Legal Library, 2015.

Mahmoud Abdel Hamid Abdel Motaleb, Crimes of Using the World Wide Web (Internet Crime), From a Security Perspective, Research presented at the Law and Internet Conference organized by the College of Sharia and Law in cooperation with the Emirates Center for Strategic Studies and Research and the Information Technology Center at the United Arab Emirates University during the period of 2000/5/31.

Abdullah bin Abdulaziz bin Fahd Al-Ajlan, Cyberterrorism in the Information Age, a research paper presented at the First International Conference on the Protection of Information Security and Privacy in Internet Law, held in Cairo from 2-4 July 2008.

Mohammed Al-Alfi, Anti-Cyberterrorism Legislation: Substantive Provisions and Patterns, Working Paper presented at the Scientific Conference on Arab and International Laws in Combating Terrorism held in Riyadh during the period from 15 to 17 April 2013.

Aysar Muhammad Atiya, The Role of Modern Mechanisms in Combating Emerging Crimes: Cyberterrorism and Ways to Confront It, Paper presented at the Scientific Conference on Emerging Crimes in Light of Regional and International Changes, Oman, during the period 04-02 September 2014.

Theses:

Mohamed Ali Al-Aryan, Cyber Crimes, Doctoral Thesis, Faculty of Law, Alexandria University, New University Publishing House, Alexandria, 2004.

Mashab Nasser Mohammed Al-Ziran, Websites and Their Role in Disseminating Religious Extremism and Ways to Confront It from the Experts' Perspective, Master's Thesis, Naif Arab University for Security Sciences, Riyadh, 2011, p. 19.

Legal Journals:

Mouza Al-Mazrouei, Electronic Intrusions: A Danger - How to Confront It, Economic Horizons Magazine, United Arab Emirates, Issue 9, 2008.

Sohair Hegazi, Procedural Threats to E-Commerce, Research and Studies Center, Dubai Police, United Arab Emirates, Issue 91.