IUS ET SCIENTIA
2023 • Vol. 9 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

The role of artificial intelligence in combating cyber terrorism

EL PAPEL DE LA INTELIGENCIA ARTIFICIAL EN LA LUCHA CONTRA EL CIBERTERRORISMO

Madaoui Nadjia
Lounici Ali, University of Blida2, Algeria
madaoui.nadjia99@yahoo.com 0009-0005-1096-211X

Recibido: 29 de octubre de 2023 | Aceptado: 08 de diciembre de 2023

ABSTRACT

This study aims at identifying the effects of technology on crime, as it is a double-edged sword, in which it can help in committing crimes, however it also contributes to preventing, detecting and suppressing them. Besides, technological development has had two prominent effects, one of them is negative, which was manifested in the dangers that threaten the security of states and individuals, particularly the phenomenon of terrorism, whose danger has steadily increased with technological and technical progress.

Therefore, the method of managing terrorism has become more sophisticated, as terrorist groups using cyberspace to launch attacks using the Internet and complex programs, thus terrorism has shifted from traditional based on hard power to cyber terrorism based on soft power. As for the positive impact of technological development, it is represented in the artificial intelligence technology used in the prevention and control of crimes, including cyber terrorism crimes.

KEYWORDS

Cyber terrorism
Artificial intelligence
technology
Combating
Prevention

RESUMEN

Este estudio tiene como objetivo identificar los efectos de la tecnología en la delincuencia, ya que es un arma de doble filo, en la que puede ayudar en la comisión de delitos, sin embargo, también contribuye a prevenirlos, detectarlos y reprimirlos. Además, el desarrollo tecnológico ha tenido dos efectos destacados, uno de ellos negativo, que se manifestó en los peligros que amenazan la seguridad de los Estados y de los individuos, en particular el fenómeno del terrorismo, cuyo peligro se ha incrementado constantemente con la tecnología.

Por lo tanto, el método de gestión del terrorismo se ha vuelto más sofisticado, ya que los grupos terroristas utilizan el ciberespacio para lanzar ataques utilizando Internet y programas complejos, por lo que el terrorismo ha pasado de ser tradicional basado en el poder duro al ciberterrorismo basado en

PALABRAS CLAVE

Ciberterrorismo
Tecnología de inteligencia artificial
Lucha contra la prevención
Prevención

el poder blando. En cuanto al impacto positivo del desarrollo tecnológico, está representado en la tecnología de inteligencia artificial utilizada en la prevención y control de delitos, incluidos los delitos de ciberterrorismo.

1. Introduction

Cyberspace has become of great significance in the international system, as it affects the nature of that system after the increasing reliance on technology. Besides, it helped to end the monopoly of power in the traditional sense of hard power, through the emergence of a new type of power, which is electronic or virtual power. Furthermore, this power became accessible to everyone who possesses technological knowledge and has the ability to use it to achieve his goals. However, it is not only used peacefully, but also by terrorist groups to conduct their attacks. Moreover, it is used by individuals and non-state actors to penetrate information networks or espionage and other offensive purposes.

As it is well known, cybercrime evolves as society develops, becoming more dangerous than ordinary crime. Especially with the spread of modern technology, and the increasing dependence of the world on computers and the Internet, the terrorist only needs, for example, a computer and secure his connection to the Internet company to carry out terrorist acts. In addition to, the crime of terrorism by electronic means has become a threat to the whole world, as the danger lies in its ease of use, in which it is employed by the terrorist while he is at home, office or hotel room away from the attention of the authority and society.

In a little more than two decades, the rapid growth of the Internet and information and communication technologies has enabled economic growth and expanded access to vital services. However, it also created new opportunities for criminal activities. As criminals have become the unintended beneficiaries of new technology and globalization because those developments have enabled them to commit and profit from crimes by exploiting transnational activities, as well as to expand their illegal activities and actions through digital platforms in a way that reduces risks, especially exposure. On the other hand, current technologies offer new opportunities for law enforcement, criminal investigation and prosecution, and fight cyber-crimes, including cyber terrorism, so as to improve public safety and enable law enforcement and criminal justice agencies to prevent and combat crime through technological progress and technology as well as artificial intelligence which has a positive impact in preventing or confronting cyber terrorism.

The significance of this study stems from our existence within the realm of the technological revolution, a period marked not only by its positive impacts but also by negative consequences. The convergence of terrorism and cyberspace has given rise to the explicit notion of cyber terrorism. This phenomenon is anticipated to be the most alarming criminal development in the coming years, with the potential for terrorists to exploit the Internet for destructive purposes, resulting in more severe consequences compared to traditional methods.

The research aims at identifying the concept of cyber terrorism, its characteristics and causes, and then highlighting the other aspect that resulted from technological development, which is artificial intelligence as a means of preventing and combating this type of crime.

From the above, the main question of the study revolves around how to use artificial intelligence techniques and expert systems in preventing and combating cyber terrorism?

The descriptive analytical approach was adopted, through the analysis and extrapolation of jurisprudential opinions, and data collection, benefiting from the results of previous research, writings and studies that were published in the field of this study.

Therefore, we will attempt to answer the problematic of the study by dividing the research paper into two main sections:

- First - the concept of cyber terrorism and its causes.
- Second - the use of artificial intelligence technology to combat cyber terrorism.

II. The concept of cyber terrorism and its causes

Everyone recognizes the difficulty of giving a specific concept of terrorism, due to the lack of a unified agreement among specialists on this complex term of a changing nature, according to some, it is due to the overlap of the concept of terrorism with other concepts, such as political violence, political crime or organized crime. Furthermore, it is also a dynamic and evolving concept whose forms and motives vary in different places and time periods. Thus, the concepts of terrorism have varied and differed, according to the varying premises of researchers on the subject. However the common factor among them is that the terrorist act is a form of violence that targets the entity of society (Ben Amrouche, 2018, p. 218).

In an attempt to give a definition of cyber terrorism, we will discuss its definition linguistically, then jurisprudentially, and explain its characteristics and perpetrators, and try to determine their motives (VERRE, 2011, p. 24 et S).

2.1. The definition of cyber terrorism and its characteristics

There are many different definitions and opinions about cyber terrorism, as the international community has not determined yet an agreed comprehensive definition of terrorism, due to the diversity of its forms and manifestations, the multiplicity of its methods and patterns, the different international views and political trends around it, in addition to the various beliefs and ideologies espoused by states towards it, while some see it as terrorism, while others as a legitimate act.

2.1.1. Linguistic and terminological definition of cyber terrorism

The term "Cyber terrorism" consists of two words, a familiar and common word "Cyber" which means the Internet, and the other word "Terrorism" which means violent, criminal acts, however until now it has not been defined in a specific way. Ibn Faris said in Mu'jam al-Lughah: "Ra', Ha', and Ba'a are two principles: one of them indicates fear, and the other refers to accuracy and lightness (Ibn Faris, 1999, p. 401)." in Taj Al Arous: (El Irhab – by Al Kasr - disturbing and frightening) (Al-Zubaidi, 1987, p. 50). The Academy of the Arabic Language in Cairo indicated that terrorists are a description given to those who use the way of violence to achieve their political goals (The Arabic Language Academy, s.d, p. 282). From the foregoing, it is clear that the meaning of terrorism in the language indicates intimidation, frightening and horrifying (Sharqi & Gharib, 2020, p. 561).

As for the definition of terrorism terminologically, there are many definitions of terrorism where opinions regarding it are varied and differed. However, the international community has not found yet a comprehensive and unified definition of terrorism. This is due to the diversity of its forms and manifestations, the multiplicity of its methods and patterns, the different international opinions and political trends around it, as well as the different beliefs and ideologies espoused by states towards it.

We can mention the most significant definitions of this term as follows:

> The International Islamic Fiqh Academy of the Organization of the Islamic Conference defines terrorism as: aggression, intimidation, or threat, whether material or moral, issued by states, groups or individuals against a person, in his religion, self, honour, mind or money without right, in various forms of violence and forms of corruption on land. (Al-Mukarramah, 5-10/1/2002)

Despite the numerous efforts at the international level to define terrorism, there is no single, comprehensive definition of the concept of terrorism. The most prominent of them is the one of the political encyclopaedia; which defined terrorism as: "the use of illegal violence, or the threat in its various forms, such as assassination, mutilation, torture, sabotage and bombing, in order to achieve a specific political goal, such as breaking the spirit of resistance and commitment among individuals, and destroying morale among organizations and institutions, or as a means of obtaining information or money. In general, it is the use of coercion to subjugate an opposing party to the will of the terrorist entity (Al Kayali, 1994, p. 562).

Barry Collins also defines it as "an electronic attack whose purpose is to threaten or attack governments, in pursuit of religious, political, or ideological goals, and that the attack must have a devastating and disruptive effect equivalent to the physical acts of terrorism. (Sharqi & Gharib, 2020, p. 562)"

Cyber terrorism can be defined as the illegal activity of a party by digital electronic technology through its networks to achieve a specific purpose (Mustafa, 2009, p. 5).

Furthermore, it is defined by Dergham Jaber Attoush as "aggression, intimidation, or physical or moral threat using electronic means issued by states, groups, or individuals against a person in his religion, self, honour, or intellect, without right in all kinds and forms of corruption on land" (Al-Mawash, 2017, p. 9).

2.1.2 Characteristics of cyber terrorism

Cyber terrorism is characterized by many features that distinguish it from terrorism in its traditional form, which ultimately endeavours to achieve illegal goals, as follows:

Cyber terrorism is a transcontinental and cross-border terrorism, therefore is not subject to any specific geographical scope. It is one of the most serious types of terrorism, as it negatively affects the national security of the target country and the lack of a high degree of certainty in the results of those attacks. Besides, in traditional attacks, the target location is specific where the damages can be expected, however they can be repaired quickly because it is easier to discover the sources of defects, unlike electronic attacks (Sharqi & Gharib, 2020, p. 562).

What distinguishes cyber terrorism is the ability to conceal and obscure the sources of information: one of them is the difficulty of tracing the perpetrator of the cyber terrorism incident, as there are many difficulties that stand in the way of obtaining physical evidence linking the perpetrator to the incident. Besides, cyber terrorism crimes are characterized as being difficult to prove because there is no clear physical evidence, as well as the case of traditional attacks. However, the difficulty of proving them is due to many reasons: they are committed by a person with a high degree of competence, deception and misinformation has, in addition to the difference in time, place and the applicable law in the country in which it was committed.

The vulnerability to dangers, as the computer has a very significant role in contemporary life, and a base on which the work of many important facilities "hospitals - airports - banks…", this statement highlights the susceptibility to threats due to the pivotal role that computers play in modern life. The term "base" refers to the foundational reliance on computers, serving as a critical infrastructure for the functioning of essential facilities such as hospitals, airports, banks, and more. In other words, these important institutions and services heavily depend on computer systems for their operations. The interconnectedness of these sectors with computer technology makes them vulnerable to various risks and dangers, emphasizing the critical need for robust cyber security measures to safeguard against potential disruptions or attacks on these vital systems. therefore in the event of a malfunction in computers, this may lead to disasters, and then computers became widely targeted and an attractive target for terrorist groups. However, we no longer need to launch missiles and explosions to destroy a city, but it is enough to disable the transportation network or disable the computers of the stock exchange in that city.

The computer is the tool used in cyber-terror attacks: as it falls under the umbrella of cybercrime, which naturally occurs in a digital environment, and therefore the perpetrator needs to use a computer.

Cyber-terror attacks are also characterized by low cost, as they require only a person with competence and technical expertise (Ben Amrouche, 2018, p. 221). Moreover, cyber-attack is a cross-border activity, thus it is a global activity which depends on deception and misinformation. Furthermore, there is difficulty in technical retention of its effects, and it is hard for the traditional investigator to deal with it. In addition, the motives of electronic terrorism are mainly political.

Calm environment: Cyber terrorism takes place in a calm environment that does not require force, violence (Abdel-Sadiq, 2009, p. 112) and the use of weapons. Therefore, it is called soft crimes. All it needs is a computer and the Internet, thus transferring data from a computer or cyber burglary does not need violence or shooting (Waquaf, 2006, p. 12).

Furthermore, one of the features of cyber terrorism is the multiplicity of actors in the use of cyber terrorist attacks, where terrorists resort to using cyberspace so as to collect information, recruit, plan, coordinate and finance, this will be dealt with in detail in the third section. Besides, the terrorists have a tremendous ability to use and employ the Internet to achieve their goals. Among the most prominent groups that have used this weapon are Al-Qaeda and, more recently, the most dangerous terrorist organization at all, "the Islamic State of Iraq and the Levant" "ISIS".

In addition to terrorist groups, countries use cyber terrorist attacks against hostile countries to achieve certain goals, as there are different ways to use cyber terrorism by the state, it may be used in the field of intelligence, or cooperation with individuals or terrorist groups to damage another country. Moreover, the state's use of this type is more dangerous than the one of terrorist groups, given the enormous capabilities of the state, which far exceeds the capabilities of the former.

Moreover, considering the widespread accessibility of the Internet to millions of users, its profound influence on public opinion becomes increasingly significant. As a result, there are individuals who sympathize with both the perspectives advocated by the state and those aligned with terrorist groups, encompassing their ideologies and associated issues.

2.2 The causes of cyber terrorism

The causes and motives of terrorism vary in the degree of their significance according to political trends, economic conditions, social conditions, as well as religious and ideological differences. We can summarize the causes of the phenomenon of terrorism as follows:

2.2.1 Personal and ideological motives

The personal and psychological factor is closely related to political, ideological and economic factors. As the marginalized youth who lose the meaning of life in the developing world for reasons related to injustice, inequity, unemployment, poverty and lack of a decent life are vulnerable to deviation and entry into the world of crime and terrorism. This is due to:

- A person's lack of the significance of his role in the family and society and his failure in family life, which leads to the acquisition of some bad qualities, including a lack of sense of belonging and loyalty to the homeland.
- The desire to appear and the love of fame, as a person is not qualified, therefore he searches for what qualifies him in vain, thus he feels aggression, sabotage and destruction.
- The person's resentment against the society in which he lives as a result of injustice and the violation of rights.
- The role of the media in stimulating the psychological factors of the individual and fuelling the spirit of a person's revenge.
- On the cultural level, the peoples of the developing world suffer from the negative repercussions created by globalization represented in cultural dependency and the identity crisis, as this led to the creation of cultural conflicts within the same society (Al-Huwaidi, 2011, p. 13).

With regard to ideological and intellectual motives, the misunderstanding of the principles and provisions of religion and its misinterpretation, and the dependence of young people on each other without referring to scholars, as well as the intellectual void and ignorance of the true religion rules, ignorance of the purposes of Sharia, extremism and radicalization in thought are all intellectual motives that led to an increase in the phenomenon of terrorism. Thus, the ideological motives leading to the phenomenon of terrorism vary, the most important of them can be stated as follows:

1. Ignorance of the objectives of Islamic law represented by conjecture not by certainty and confirmation, misunderstanding and misinterpretation of religion, and the ignorance of the rules, etiquette and behaviour of the true religion.
2. The various intellectual divisions between the diverse and different trends.
3. Extremism, which is very dangerous in any field, especially intellectual domains.

Among the most prominent causes and political motives for the phenomenon of terrorism, we find the following:

- The political motive is one of the stimulating motives for terrorism, as the unjust policies pursued by some people.
- States against their citizens, the political repression that they exercise, the marginalization of the citizen's role, the violation of his rights, and the failure to meet the requirements of social balance, all them represent a strong motive for the practice of terrorism in order to get rid of these conditions.
- In addition to the absence of social justice, inequality in the distribution of national wealth, disparity in the distribution of services and public utilities, and the negligence of citizens' needs.

2.2.2 Political and technical motives

One of the political motives for the phenomenon of terrorism is the suffering of some international societies and peoples from injustice, persecution, colonial control, theft of funds, and violation of international laws and charters, which push peoples to extremism and radicalization.

Facts have also proven that the existing conflicts between two countries often lead to the exchange of electronic terrorist operations, as the case of the existing conflict between America and Cuba, in which the American political class attempted to link the Cuban island to cyber terrorism, and that was a few days after the receipt of (George W. Bush) the authority arguing that Cuba represents an indirect threat to the national security of the United States, and has the ability to launch cyber-attacks on the infrastructure of the superpower (Alejandro, 2012, pp. 154-155).

Among the technical reasons that facilitate cyber terrorism, we find:

1. The low cost of electronic mechanisms combined with the traditional tools with which terrorist operations are carried out, such as bombs, explosives, and developed weapons (Shafiq, 2016, pp. 36--37).
2. The lack of geographical borders and spatial barriers in cyberspace is an appropriate opportunity for terrorists.
3. The weakness of the information network structure and its penetrability provides terrorists with a way to attack them to achieve their goals. As terrorist groups may attack the computer networks of governments, private companies, or individuals.
4. The lack of control and oversight over information networks is one of the main reasons for the spread of cyber terrorism. In many cases, it is difficult for the police to pursue those who carry out cyber terrorism operations and to determine their identity.
5. The difficulty of proving these aspects is considered as one of the strongest motives helping to commit terrorist crimes, because it gives the criminal a hope of escaping punishment. Besides, the regulatory and legislative vacuum in crimes that are used in electronic crimes helped to increase this crime. Furthermore, the absence of a unified central authority that controls what is offered on the network and its inputs and outputs is an important reason for the spread of this crime (Ben Amrouche, 2018, p. 221); (Carole, 2019, p. 2).

The use of artificial intelligence technology to combat cyber terrorism.

The roots of artificial intelligence go back to the forties with the spread of computers, where Dan. W. Patterson defined it as "a type of computer science that is concerned with the study and formation of computer systems which show some forms of intelligence, as these systems have the ability to draw very useful conclusions about the problem set. Furthermore, these systems can also understand natural languages or living perception, and other capabilities that need intelligence when implemented by humans (Sheikh, 2018, p. 82).

The term artificial intelligence has increased in use recently in light of the technical renaissance that the world is witnessing in the field of machine development. Although it was just a dream put forward by directors in fantasy films until the middle of the twentieth century, today it has become a tangible reality that we resort to many times, even if we sometimes do not realize it.

2.3 The definition of artificial intelligence and its characteristics

Artificial intelligence is one of the modern and innovative sciences that rely mainly on computers and its programs. It is the cornerstone in making programmed and computerized machines perform tasks similar to the human intelligence processes, which are learning, deduction and decision-making, it is characterized by a set of features

2.3.1 The definition of Artificial Intelligence

There is no specific definition of intelligence, therefore we find **Marvin Minsky**, who is one of the most famous scientists specialized in administrative and cognitive sciences in the field of artificial intelligence, in his book "Steps Towards Artificial Intelligence", defines it as "A branch of science that is concerned with machines that can solve the kind of problems that a person resorts to when solving them to his intelligence" (Suleiman, s.d, p. 3).

Mohammed Ali Al-Sharqawi defines artificial intelligence in his book as "Artificial Intelligence and Neural Networks" as "that branch of computer science through which it is possible to create and design computer programs that simulate the method of human intelligence so that the computer can perform some tasks instead of the human being that requires thinking, comprehension, hearing, speaking, and movement" (Al-Sharqawi, 1996, p. 24).

It is also defined as a technology dedicated to programming the machine to perform tasks that require human intelligence to solve, i.e. simulating the intelligent behaviour of humans. It is also described as an attempt to build machines that think and act like humans, so that they are able to learn and use their knowledge to solve problems alone (Al-Hamdani, 2008, p. 260).

2.3.2 The characteristics of artificial intelligence

Artificial intelligence has many characteristics that made it an effective investment in many areas, such as its application to devices and machines that enable it to plan and analyse problems using logic (Khaza'leh, 2015,), where machine is programmed by human and works well, however in many cases its work is more elaborate than the human.

It also recognizes sounds, speech and the ability to move things:

> The use of artificial intelligence contains many areas, including the field of robots that speak, move and distinguish sounds, which makes humans benefit from them

in the future, especially in the field of crime control, by recording sounds, movement and images and using them as evidence in proving or denying crimes, which helps to achieve justice.

In addition to the possibility of machines which carry out their work continuously without feeling tired or bored, as well as the stability of their ability to produce at all times without regard to the time or circumstances surrounding the work (Bana, 2020).

Furthermore, the devices that adopt artificial intelligence can understand the input and analyse it well to provide outputs that meet the user's needs with high efficiency (Khaza'leh, 2015,), such as entering information about a person by the police, thus the results are quickly given from the computer programmed for this process. Therefore, this makes it easier for the police to work easily and not to waste time, especially since the speed in proving crimes is among the things that help to achieve justice and not allowing criminals to evade them.

Moreover, artificial intelligence is also characterized by the ability to process the huge amount of information that is presented (sans référence), where, for example, the police can search for a person's name on a computer with just the touch of a button the result will be available, knowing that the device may contain hundreds of thousands of people's (Victor, Kenneth, & Big, 2013)names, which is considered a tremendous development and service to humans that exceeds their intelligence, as they cannot reach the level of machine intelligence no matter what they do, because the human mind is very limited.

Besides, the machine can find similarities and differences between the cases recorded in its brain or programmed, as well as it cannot forget unless a technical failure occurs, thus it helps to achieve justice.

2.4. Combating cyber terrorism through artificial intelligence

Artificial intelligence techniques play a pivotal role in predicting terrorist operations through the analysis of big data of citizens (Kathleen, August 2019), however at the same time, they face challenges related to human rights, and the implications of their practical applications, which raise questions about the limits of their predictive uses in combating terrorism, and the implications of opportunities and risks (Kathleen, August 2019).

By relying on the use of security surveillance cameras networks to monitor hundreds of thousands of faces on a daily basis in search of any suspected terrorist, where terrorist crimes can be reduced. In addition to using the characteristics of previous attacks, training in identifying terrorists in crowded areas, introducing artificial intelligence systems to analyse surveillance videos in criminal investigations, identifying suspected persons targeting major events, determining vehicle models and analysing suspicious financial transactions, and automatically detecting people who appear unusual behaviour such as frequently visiting a particular site or staying in one place, or suspicious items that have been abandoned.

2.4.1 Methods of neutralizing cyber terrorist attacks

There are two ways to prevent terrorist attacks (Kathleen, August 2019); The first is deterrence, by protecting infrastructure, and implementing security controls, forecasting contributes to the physical protection of infrastructure, and it can also be a way to improve resource allocation to locations that are likely targets for terrorists.

The second aspect involves preventing the initiation of attacks, by arresting terrorists before they carry out their plans, combating future terrorist recruitment and extremism, imposing restrictions on the movement and freedom of individuals. Furthermore, effective prediction helps in the use of force or coercive restrictions against violent terrorists, whereas restorative measures are used with individuals prone to extremism.

Counter-terrorism predictability requires a type of artificial intelligence that enables knowledge and predictions to be extracted from diverse, large digital data. As algorithms that support predictive models are self-programmed based on data handling. In many cases, it would be impossible to analyse data without such an approach, and it would be impossible to build models without data (Kathleen, August 2019). However, the problem is that predicting terrorist operations imposes the need to expand the surveillance space for people in contravention of human rights, and exposes governments and intelligence services to human rights problems. Thus, in the near future, good predictions based on artificial intelligence techniques about whom or what to monitor can contribute to reducing the wholesale misuse of technical aspects of monitoring.

2.4.2 Applications of cyber counter-terrorism

Artificial intelligence can be used to make predictions about terrorism by analysing communications metadata, information about financial transactions, travel patterns, and web browsing activities. Furthermore, it can also be employed to analyse social network data to counter negative phenomena (Olivier, 2017), whether represented in combating extremist content on the Internet (Dr. Haider & Dr. Mahmoud, 2014, p. 19). Moreover, there is a growing interest by security authorities in using **Social Analytics** to analyse social network data to discover the possibility of riots and demonstrations in a given region (Dr. Al-Salmi, 1999, p. 43).

The Artificial Intelligence and Computer Science Laboratory at the Massachusetts Institute of Technology designed an algorithm that analysed more than 600 hours of YouTube videos with the aim of studying human behaviour. The algorithm was then able to correctly predict human actions in 43% of the test samples, which is less than the ability of humans by only 28% (Tolba & Fahmy, 2005, p. 38).

Artificial intelligence analyses the "big data" of individuals, which is the huge amounts of personal and professional information that can be analysed to identify developments in human behaviour patterns and interactions, as this data is very complex, which helps in a deep understanding of societies, in which it allows more ability to monitor collective and individual human behaviour, and predict their future trends (Shadi, Al-Ghitan, & Yahya, p. 12).

Artificial intelligence endeavours to determine terrorists by distinguishing between what characterizes the activity of a particular subgroup on these media. Furthermore, machine learning methods allow interpreting and analysing patterns that are inaccessible with large amounts of data. These methods include analysing relationships between entities or more complex tools for image or sound recognition. In this regard, some examples of the ability of artificial intelligence to predict (Kathleen M., 2019), are represented as follows:

A. Predicting the timing and location of attacks: Models have been developed to predict the location and timing of terrorist attacks. In 2015, for example, a tech start-up (PredictifyMe) claimed that its model, which contains more than 170 data points, was able to predict suicide attacks with 72% accuracy. Furthermore, some other models have relied on open source data for individuals using social media and apps on their mobile phones include the Early Event Recognition System (EMBERS), which integrates the results of various separate predictive models in order to predict events such as disease outbreaks and civil disturbance events.

B. Fragility and vulnerability to extremism: Some technology companies have developed tools to assess vulnerability to violent extremist ideologies; Like Alphabet Inc's Jigsaw (formerly Google Ideas) which announced its project called "Redirect", that targets users of video-sharing sites who may be vulnerable to propaganda from terrorist groups such as "ISIS", as the project redirects them to videos that adopt an authoritative and anti-regulatory narrative.

C. Identification of terrorists: Some leaked details of a US National Security Agency (SKYNET) program indicate that an artificial intelligence-based algorithm was used to analyse metadata from 55 million local Pakistani mobile phone users in 2007, the result was that a percentage of only 0.008% of cases are mistaken as potential terrorists, which is about 15,000 people out of Pakistan's total population of 200 million at the time. Although the model used was not effective, it illustrates the predictive value of the data when identifying close links with terrorism.

Even though the prediction is not accurate at this time, with the development and improvement of machine recognition technology, we may reach a high rate of accuracy that makes us use this technology one day to correctly predict human actions, which we believe will contribute significantly to improving the level of security in cities.

III. Scope for future work

Cyber security needs much more attention. Given human limitations and the fact that agents such as computer viruses and worms are intelligent, network-centric environments require intelligent cyber sensor agents (or computer-generated forces) which will detect, evaluate and respond to cyber-attacks in a timely manner. The application of AI techniques in cyber defense will need planning and future research. One of the challenges is knowledge management in network-centric warfare, hence a promising area for research is introduction of modular and hierarchical knowledge architecture in the decision making software. Rapid situation assessment and decision superiority can only be guaranteed with automated knowledge management. It is also foreseeable that the grand goal of AI research – development of artificial general intelligence - can be reached in not so distant future which would lead to Singularity described as "the technological creation of smarter-than-human intelligence". Nevertheless, it is of crucial importance that we have the ability to use better AI technology in cyber defense than the one offender possess. Furthermore, a lot more research needs to be done before we are able to construct trustworthy, deployable intelligent agent systems that can manage distributed infrastructures. Future work must search for a theory of group utility function to allow groups of agents to make decisions. (Dilek, S, Çakır, H., Aydın, M. 2015. P33-34).

The role of artificial intelligence (AI) in combating cyber terrorism constitutes a critical and evolving field with considerable scope for future research. One promising avenue for exploration involves advancing the capabilities of AI-driven predictive models for early detection and prevention of cyber threats associated with terrorism. Future research could delve into the development of more sophisticated algorithms and machine learning techniques, enhancing the accuracy and efficiency of AI systems in identifying emerging cyber threats and potential terrorist activities. Furthermore, there is a pressing need to investigate the integration of AI in cyber security strategies employed by governments, organizations, and security agencies. This research could focus on understanding how AI technologies can be effectively incorporated into existing frameworks to bolster cyber defenses against evolving and sophisticated cyber threats associated with terrorist activities. Examining the practical implementation of AI-powered cyber security measures and their effectiveness in real-world scenarios would provide valuable insights for policymakers and practitioners.

The ethical and legal dimensions of AI in the context of combating cyber terrorism present a complex and multifaceted area for future inquiry. Research in this domain could explore the development of ethical frameworks and regulatory guidelines governing the responsible use of AI in counterterrorism efforts. Understanding the ethical considerations and legal implications associated with AI technologies would contribute to the establishment of robust governance mechanisms that balance security imperatives with individual rights and privacy concerns. Additionally, as AI technologies continue to advance, there is potential for research on the vulnerabilities and countermeasures specific to AI systems themselves. Investigating the susceptibility of AI algorithms to adversarial attacks and developing techniques to enhance the resilience of AI-powered cyber security solutions would be crucial for ensuring the reliability and trustworthiness of these systems in the fight against cyber terrorism.

An interdisciplinary approach to studying the socio-technical aspects of AI in combating cyber terrorism is another promising direction for future research. Examining the human factors involved, such as user interactions with AI-based security systems and the socio-political implications of widespread AI adoption in counterterrorism could provide a comprehensive understanding of the broader impact of AI technologies on security practices.

In conclusion, the future scope for research in the role of AI in combating cyber terrorism is vast and multifaceted. From technical enhancements and practical implementations to ethical considerations and societal implications, researchers have the opportunity to contribute significantly to the advancement of knowledge in this critical domain. As AI technologies and cyber threats continue to evolve, ongoing research endeavors will be essential for developing effective and responsible strategies to safeguard against cyber terrorism.

IV. Conclusion

We addressed in this study a significant subject that has become a current event, which is cyber terrorism, and the role of artificial intelligence technology systems in preventing and combating it, as it is a very thorny and complex subject.

Cyber terrorism is one of the most serious types of terrorism in the world, especially since the phenomenon of cyberspace has played a strategic role in the international community at the economic, political, cultural, security and social levels.

The danger of cyber terrorist acts lies in their reliance on advanced technologies such as devices that eavesdrop on communication networks, encryption software, to penetrate network and computer security systems. Furthermore, a single automated network may include tens, hundreds of thousands, or millions of computers or devices connected to the Internet that can be used to launch various attacks for criminal purposes such as sabotage, terrorism, threats and extortion.

We concluded a set of results, the most important are:

- Cyber terrorism is a deliberate activity or attack with political motives aiming to influence government decisions or public opinion by exploiting cyberspace in the implementation process with the intent of intimidating individuals by threatening them or causing actual damage to them.
- The fundamental reasons for the spread of this kind of terrorist acts are: the political reasons represented in the dictatorship of the regime and the lack of political participation of citizens. Moreover, the economic reasons which are due to social inequality, and the spread of unemployment. As for the technological reasons, it is mainly due to the weakness of the information network system. Therefore, it is easy to penetrate by terrorist groups, in addition to its ease of use, low risks and cost.
- The methods and means used by terrorist groups to exploit cyberspace in carrying out their terrorist acts are represented in coordination and communication, in addition to media promotion, as well as spying on and destroying websites, and finally, propaganda war which aimed at attracting and recruiting many individuals, especially minors, as well as obtaining support and financial resources.

- Advancement in the field of artificial intelligence has made robots more intelligent and able to perform many functions and tasks instead of humans, it also has encouraged an increasing number of law enforcement agencies to take advantage of these technological advances in a variety of their operations.
- Artificial intelligence is very much a double-edged sword, as it can lead to important changes in the way justice agencies deal with the task of policing, however it also enhances the working methods of terrorist groups, and can even facilitate the emergence of new forms of crime and the priority must be to enhance policing using AI techniques to combat AI-based crime.

At the end of the research, we recommend the following:

- Giving special significance to identifying ways and means to enable criminal justice and law enforcement personnel to employ advanced technologies, such as artificial intelligence, information and communication technologies, including big data, as well as to make full use of them in combating the crime of cyber terrorism.
- Countries of the world should identify and address existing gaps in their legal systems to ensure effective investigation and prosecution of technology-facilitated crimes, including adopting new laws and/or updating existing laws with technology-neutral language, and promoting international cooperation.
- States should promote and expand partnerships and synergies with international and regional organizations, civil society, the private sector and academia, in order to enhance research, innovation, development and use of technology in the areas of law enforcement and criminal justice in the context of preventing and combating terrorist cybercrime.
- Working to constantly improve new technologies to ensure preparedness to address their problems; and to promote the application of ethical standards in the use of these technologies.

Bibliography list

ABDEL-SADIQ, A. (2009). *Cyber Terrorism: The Power in International Relations, a New Pattern and a Contrasting App*. Cairo: Center for Political and Strategic Studies.

AL KAYALI, A. W. (1994). *Political Encyclopedia, part 7*. Beirut: the Arab Foundation for Studies and Publishing.

AL-SHARQAWI, M. A. (1996). *Artificial Intelligence and Neural Networks* (éd. 1). Egypt: The Modern Egyptian Office Press

AL-ZUBAIDI. (1987). *Taj al-'arūs min jawāhir al-Qāmūs* (éd. 2). (A. Hilali, Éd.) Kuwait.

AL-HAMDANI, B. H. (2008). Al-Bakry, Riyad Hamza, *The reality of development in light of scientific progress and the concept of artificial intelligence*. Journal of Comprehensive Management Accounting, College of Management and Economics.

AL-HUWAIDI, O. (2011). *Combating Terrorism Crimes*. Amman: Dar Wael Li Al Nasher.

AL-MAWASH, D. J. (2017). *The Crime of Information Espionage (a comparative study)* (éd. 1). Egypt: Longitudinal Center for Scientific Studies and Research.

AL-MUKARRAMAH, T. d. (5-10/1/2002). *(Makkah Al-Mukarramah: the Islamic Fiqh Council of the Muslim World League in its sixteenth session.*

AL-SALMI, A. A.-R. (1999). *Information Systems and Artificial Intelligence*. Amman: Dar Al-Manhaj for Publishing and Distribution.

ALEJANDRO, C. A. (2012). *The Empire of Terror* (éd. 1). (W. Ibrahim, Trad.) Beirut: Publications Company for Distribution and Publishing.

BANA, D. (2020, January 14). Consulté le November 16, 2021, sur https://mawdoo3.com

BEN AMROUCHE, F. (2018). *Electronic Terrorism: A Study in Conceptual and Dimensional Problems*. Algerian Journal of Social and Human Sciences, 8(2).

CAROLE, M. (2019). Laurent Guille, *Intelligence Artificielle Et Cybersécurité*. Wavestone.

DILEK, S., ÇAKIR, H., & AYDIN, M. (2015). Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. International Journal of Artificial Intelligence & Applications (IJAIA), 6(1).

HAIDER, S. A.-B., & Dr. MAHMOUD, H. A.-H. (2014). *Technology and Information Systems in Contemporary Organizations* "A Technological Administrative Perspective." Cairo: Published by Mahmoud Hassan Jomaa Foundation.

IBN FARIS. (1999). *A Dictionary of Language Standards* (éd. 1). Beirut: Dar al-Kotob al-Ilmiya.

KATHLEEN, M. (2019, October 9). *Predicting Attacks: Opportunities and Risks of Using Artificial Intelligence* in. Récupéré sur https://futureuae.com/ar/Mainpage/Item/5022/%D8%A7%D9%84%D8%AA%D9%86 %D8%A8%D8%A4-%D8%A8%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA.

KATHLEEN, M. (August 2019). *Artificial Intelligence Prediction And Counterterrorism*. Britain: Chattam House.

KHAZA'LEH, S. (2015, August 15). *The Characteristics of Artificial Intelligence*. Consulté le November 16, 2021, sur https://mawdoo3.com.

MUSTAFA, M. M. (2009). *Electronic Terrorism (legal, security, psychological, and social study)* (éd. 1). Cairo: Egyptian National Books and Documents House.

OLIVIER, T. (2017, June 6). *Artificial Intelligence Will Save Us From Cyberterrorism*. Consulté le August 12, 2020, sur https://Www.Telerama.Fr/Medias/L-Intelligence-Artificielle-Va-Nous-Sauver-Du-Terrorisme'159806.Php.

sans référence. (s.d.).

SHADI, A.-W., Al-GHITAN, I., & YAHYA, S. (s.d.). *Opportunities and Threats of Artificial Intelligence in the Next Ten Years.*

SHAFIQ, N. (2016). *The Impact of Cyber Threats on International Relations: A Study in the Dimensions of Cyber Security* (éd. 1). Cairo: al-Maktab al-'Arabī lil-Ma'ārif.

SHARQI, S., & Gharib, H. (2020). *Electronic Terrorism and the Transformation of the Concept of Power*. Al-Bahith Journal for Academic Studies,, 7(2).

SHEIKH, H. (2018). *The role of artificial intelligence in managing the electronic customer relationship of the Algerian People's Credit* CPA. Academic Journal of Human and Social Studies,(20).

SULEIMAN, Y. A.-F. (s.d). *Artificial intelligence*. Syria: Al-Badr Magazine.

The Arabic Language Academy. (s.d). *The Intermediate Lexicon*. (I. Mustafa, & others, Éds.) Turkey: the Islamic Library.

TOLBA, D., & FAHMY, M. (2005). *Computer Knowledge Department*. Alexandria: Modern Egyptian Office Press.

VERRE, D. (2011). *Cyberspace And Actors Of Cyberconflict* (Edition Bermes Science ed.). Paris: La Voisier.

VICTOR, M.-S., KENNETH, C., & BIG, D. (2013). *A Revolution That Will Transform How We Live. Work And Think* (London, John Murray).

WAQUAF, A.A. (2006). *Combating Terrorism Between Politics and Law*. Algeria: Dar Al-Kheldonia Publishing and Distribution.