التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION

USE OF ARTIFICIAL INTELLIGENCE TOOLS IN COUNTERING TERRORISM

DR. OBAID SALEH ALMUKHATTIN
RESEARCHER IN ARTIFICIAL INTELLIGENCE AND CYBERCRIME
UNITED ARAB EMIRATES

Dec. 2023
5
TERRORISM ISSUES

TERRORISM ISSUES

A monthly publication issued by the Islamic Military Counter-Terrorism Coalition

General Supervisor

Maj. Gen. Mohammed bin Saeed Al-Moghedi

Secretary-General of the Islamic Military Counter Terrorism Coalition

Editor-in-Chief

Ashour Ibrahim Aljuhani

Head of Studies and Research Department

Disclaimer: The views expressed in this study are those of the author and do not necessarily reflect the opinions or views of IMCTC.

5

TERRORISM ISSUES

USE OF ARTIFICIAL INTELLIGENCE TOOLS IN COUNTERING TERRORISM

DR. OBAID SALEH ALMUKHATTIN
RESEARCHER IN ARTIFICIAL INTELLIGENCE AND CYBERCRIME
UNITED ARAB EMIRATES

Using artificial intelligence (AI) in combating terrorism can have a significant and positive impact on the efforts exerted to counter terrorist threats. AI allows systems to analyze massive amounts of information and data more quickly and accurately, which helps to identify patterns and potential threats and to take appropriate measures to prevent and predict terrorist attacks (Al-Huqail 2023). There is a global trend to benefit from AI in countering terrorism and organized crime. Data will be an essential part of counter-terrorism strategies in the future. Strategies for using artificial intelligence in combating crime and terrorism include focusing on a group of aspects, such as analyzing data and detecting potential patterns and threats, developing image and video recognition systems, detecting suspicious behavior, conducting predictive analysis, estimating future threats, analyzing terrorist behavior, and deleting extremist content from social media platforms.

1. Research Objectives

- A major goal of utilizing AI in analyzing big data for intelligence operations is quick access to the required information, swift arrest of perpetrators, and prediction of terrorist acts and escalations before their occurrence;

- Using AI technologies to counter terrorism and monitor terrorist content on social media platforms, by understanding the stages and components of these technologies, such as machine learning, algorithms, natural language processing, intelligent neural networks, identification of violent extremist content, combating the spread of hate speech, and countering the spread of extremist and terrorist ideologies on social media platforms.

- Formulating a strategy for digital security cooperation between Arab counter-terrorism security agencies in the fight against cyber terrorism;

- Identifying the Dark (hidden) Web, describing Deep Web and its operation techniques, and shedding light on terrorist tactics via the Deep Web and terrorist financing.

2. Research Questions

- What are the mechanisms for utilizing artificial intelligence to protect societies and individuals from extremism and terrorism?

- What is the concept of artificial intelligence in terms of countering extremism and terrorism on social media platforms? What capabilities are used by AI companies to combat terrorist content?

- What are the security risks of social media sites and their impact on societal security in the Arab region?

- How is terrorism financed through the Deep Web and the international challenges that security agencies around the world encounter in monitoring and tracking illegal activities?

3. Key Terms

Violent extremism, terrorism, cyberspace, artificial intelligence (AI), neural networks, machine and deep learning, algorithms, social media platforms.

4. Research Plan

The study is divided into two parts. Part I is entitled "Smart Tactics of Terrorism in Financing, Recruitment, and Dissemination of Extremism;" it discusses three topics: (1) Utilization of technology and cyberspace by terrorist groups; (2) Dissemination of violent extremism via online platforms; and (3) The tactics of disseminating extremism and terrorism on the Dark Web. Part II of this study is entitled "Artificial Intelligence and Opportunities for Countering Extremism and Terrorism;" it also addresses three topics: (1) Opportunities for using artificial intelligence applications in predicting terrorist operations; (2) Utilization of algorithm-based software to enhance counter-terrorism activities; and (3) Digital security cooperation mechanisms for counter-cyberterrorism. The study ends with a Conclusion, together with the major results and recommendations.

Part I: Smart Tactics of Terrorism in Financing, Recruitment, and Dissemination of Extremism

Introduction

Smart tactics of terrorism depend on the use of advanced strategies in financing, recruitment, and spreading extremism. These tactics include the use of financing, secret communication, social media, encryption, intelligent exploitation of multimedia, and a diverse digital presence (*United Nations Global Counter-Terrorism Strategy*, 2020). In fact, artificial intelligence can be extremely dangerous if used by terrorist organizations with malicious intent and with a proven track record in the world of cybercrime. It is a powerful tool that could conceivably be used to increase or facilitate terrorism and violent extremism, which also leads to terrorism, for example, by providing new methods of physical attacks, using drones or self-driving cars, by increasing cyber-attacks on critical infrastructure, or by enabling the spread of hate speech and incitement to violence in a faster and more efficient manner. we address these risks by focusing on three topics as follows:

1. Utilization of technology and cyberspace by terrorist groups;
2. Dissemination of violent extremism via online platforms;
3. Tactics of disseminating extremism and terrorism on the Dark Web.

1st Topic

Utilization of Technology and Cyberspace by Terrorist Groups

Extremist groups are rapidly exploiting technology and evolving in their use. Therefore, it is crucial to understand the threats related to extremism and to develop effective strategies to prevent and combat these threats. Understanding the growing threat of extremism and the sophisticated technology tools used by extremist groups is a vital issue in developing effective strategies to prevent and combat this phenomenon, especially with the increasing use of the Internet and social media as tools to spread extremist ideology. It also reinforces the need to analyze and monitor digital content and to develop pattern recognition techniques and to predict the upcoming behavior of extremists.

Recent examples have been reported of terrorists using technology through a range of advanced devices. For example, Global Positioning System (GPS) devices, mobile phones and the Internet were used by the perpetrators of the 2008 Mumbai attacks to plan, coordinate and execute their attacks, representing an innovative use of the latest technological developments at the time. More recently, terrorists have used Blockchain-based virtual assets, such as Bitcoin, as well as mobile banking, crowdfunding for fundraising purposes or for fund transfer. On the other hand, the Dark Web serves as a market for materials, weapons, and counterfeit documents.

There is ample evidence that these terrorist groups utilize technologies related to artificial intelligence. This can be particularly seen in the use of unmanned aerial systems, also known as drones, which are considered as a related technology to artificial intelligence. These drones have been used by terrorist groups for various purposes, including actual and attempted attacks, disruption, surveillance, propaganda, mobilization, crowding, and recruitment of new terrorists. New recruits join these terrorist organizations to ensure their survival and continuity. These recruits make use of the sympathy of other Internet users for their causes and attract their attention with bright and enthusiastic statements through online chat rooms, as follows (Abdul Moati, 2012):

- Giving instructions and online indoctrination: The Internet is filled with a vast number of websites containing manuals and guidelines explaining methods for making bombs and deadly chemical weapons.
- Psychological warfare: Disseminating misleading information and spreading terror and fear in the hearts of individuals by filming and documenting their terrorist crimes and operations, and glorifying their perpetrators (Abdel Salam, 2020).
- Funding: The Internet is used to obtain donations using online financial transfers. International organizations of a humanitarian or charitable nature may be used as an umbrella to provide funding or work under its cover.

2nd Topic

Dissemination of Violent Extremism via Online Platforms

The policy of terrorist organizations, including ISIS, depends on using mass polarization, violation of digital privacy, and abuse of human rights by spreading scenes of violence, pirating graphics (hashtags) and applications, chat programs, and the so-called “internet bots,” which are locally prepared. The scene of extremism and terrorism produces more effect if coupled with speed. For example, ISIS's media production and its subsequent dissemination is characterized by speed and secrecy. The media behavior of this terrorist organization that accompanied the suicide bombings on November 14, 2015, which targeted the French capital, Paris, and resulted in the killing of 127 civilians and 8 militants, indicates media work coordinated and prepared in advance. This demonstrates the synchronization between the operations conducted and media communication in the terrorist scene (*Terrorism and Human Rights Report*).

The prominence of social media can make people vulnerable to manipulation through misinformation and disinformation. The integration of artificial intelligence into this equation, for instance through the proliferation of deepfakes, will greatly enhance the nature of security threats (*Algorithms and Terrorism*, 2023). The following section will address the spread of violent extremism through online platforms and abuses of human rights.

1. Social media platforms as a cover for terrorist acts

Terrorist organizations use social media networks as a tool to identify their targets and monitor their movements, especially in the context of assassination operations in targeted countries. They monitor either the targeted people who have accounts on those networks or their circle of friends and acquaintances to be able to reach them and collect the necessary data about their movements. Terrorist groups employ social media websites for several main objectives, including operational communications purposes, intelligence collection and information exchange, recruitment and training, and other functional uses. In 2014, a report issued by the Los Angeles-based Simon Wiesenthal Center indicated that there are more than thirty thousand forums, websites, and social media accounts, promoting terrorism in the United States of America and abroad. The report also highlighted the rising numbers of extremists using social media networks. It is noted that many right-wing groups on social media redirect the public towards their forums and constantly reveal the pages and accounts of members of these groups and groups on social media platforms, such as Facebook and Twitter (*Wiesenthal*, 2021).

2. Utilization of artificial intelligence by terrorist groups

Terrorist groups utilize artificial intelligence, which is considered an abuse of human rights. It serves as a type of misuse of technology that causes damage to societies and humanity in general, especially with the increased access of individuals to self-learning technologies. In February 2020, the proper operation of systems based on artificial intelligence was interrupted, when a German artist tricked Google Maps into believing that traffic on the streets of Berlin was higher than it actually was by feeding incorrect data to the Google Maps machine learning algorithms. He carried 99 mobile phones with him while walking through the streets, which Google Maps incorrectly understood as referring to different people in their cars, causing the system to malfunction. Thus, malicious capabilities are used to create chaos and confusion when maliciously leveraged.

3. Dissemination of hate speech and deepfakes through online platforms

Social media platforms are used as tools to spread hatred and rumors online, leading to increased instances of violence in society. Social media facilitate and accelerate dissemination of or engagement in violent or inflammatory behavior under the guise of hiding behind a computer screen.

Social media platforms are also used as a backdoor to terrorism, most notably by spreading hate speech, misinformation, and extremist content. They have provided violent racists with an available public platform for permanent use. In addition, the anonymity of social media users has given countries the ability to harbor and incite hatred transnationally. Terrorist groups also rely on social media platforms to legitimize violence, recruit assassins, and glorify victories. In the course of its rise, ISIS in Iraq and the Levant had a prominent presence on social media, through which it broadcast video clips of executions, attacks, and other content (Nisreen Al-Sharqawi, 2022).

There are forms of security threats posed by deepfake technology that affect national and societal security, as explained by (Khalifa, 2018), namely the following:

- Fabricating offensive statements by politicians may lead to the outbreak of violence, demonstrations, or even tension in relations with other countries.
- The Cybersecurity company "Forcepoint" expects cybercriminals to use deep phishing to generate images and videos that can be used to demand ransoms. In parallel, data theft is likely to increase by tricking employees into giving up information, including access credentials, financial records, etc. Phishing attacks are also expected to increase through posting videos containing malware, or recording messages designed to lure users into clicking on links as part of phishing attacks (Hammes, 2020).

4. Social media as a threat to societal security

Social media platforms play an active role in creating and shaping public opinion. They contribute to promoting the ideologies embraced by the elite in society. One of the most influential innovative programs in the digital world is the world's most famous application TikTok. This application raises several global security challenges. For example, it is accused of excessively collecting and extracting user data and of subjecting such data to extensive analysis processes, including unnecessary copying of data from phones, collecting information that can be used to determine and track the user's location, and using the application as a means to spread rumors, especially those that would threaten national and Arab security. Some videos shown on TikTok also promote forms of hate speech and spread extremist and terrorist ideologies, which creates disputes and struggles within society, and threatens its security and stability. The application also collects all metadata about users and followers.

Following is an account of a number of security risks posed by the TikTok application and the negative influences of artificial intelligence.

- The application shows several video clips of children being raped and killed.
- Security threats are increasing, and attention is growing due to the fact that some extremists and terrorists use the "Tik Tok" application in some criminal and extremist practices. For example, some American extremists used the application during the riots and storming of the Capitol building in January 2021 to recruit and incite people to violence, promote weapons, and share tactical instructions related to the criminal activities that have been conducted (Khaled Kazem Abu Doh, 2022).

3rd Topic

Tactics of Disseminating Extremism and Terrorism on the Dark Web

The operations of terrorist organizations have developed in terms of financing, money exchange, and collection of donations. They no longer need to receive funding from their supporters through bank accounts that are subject to supervision and accountability. Nor do they need companies and institutions to launder or multiply their funds. The Internet has become an important, sufficient, and dangerous alternative. The ISIS organization, for example, has become able to collect, multiply, and spend millions of dollars via the Internet, using the "Bitcoin" currency. The leaders of terrorist organizations have been able to communicate and collect donations in complete secrecy via the Dark Web, or the so-called "Deep Web."

For this reason, many security agencies in countries around the world were prompted to create artificial intelligence platforms and tools to monitor prohibited content. Terrorist organizations leak content to less well-known and sometimes unknown sites that do not have sufficient resources to devote to censorship.

To establish and manage online financial networks, it is sufficient for any terrorist or criminal organization worldwide to provide an Internet connection, possess virtual accounts and financial wallets in a number of online banks, have members trained to work within the virtual currency market, and to fill its financial wallets with virtual currencies, either through donations provided by its supporters and followers, or by receiving funding via the Internet from its supporting agencies, countries, and entities (*belfercenter.ksg.harvard,* 2023).

Terrorist tactics used across the Dark Web include the following:

1. Youth recruitment and brainwashing as one of the dynamics of the terrorist threat via online platforms

The recruitment of youth and the influence of terrorist groups on them through social media platforms and the Dark Web is an important part of the dynamics of the terrorist threat to countries. Terrorists use these platforms to promote extremist ideologies, collect information, and direct youth towards terrorist action. Following are some of the main aspects of these operations: (*Counter-Terrorism Reference Curriculum*, 2023):

The effect of trust and the promotion of extremism: Terrorists seek to establish a relationship of trust with young people and to convince them of their extremist ideologies. They use psychological manipulation and emotional maneuvers to attract and recruit young people into their ranks. Extremist ideologies are promoted through motivating publications and videos targeting these young people.

2. Use of Bitcoin to finance terrorism through the cyber environment

ISIS exploits Bitcoin in two separate ways: first, to purchase its needs from illegal stores on the Dark Web (Ahmed Shawqi Al-Attar, 2021); and second, to convert these virtual funds into liquid money to disburse on its living requirements and organized operations. Illicit markets on the Dark Web for buying and selling illicit goods represent one of the most important places where ISIS spends its Bitcoin to meet its operational needs. These needs comprise, for example, purchasing fake passports that enable extremists to easily cross borders, renting vehicles and safe houses, and purchasing weapons, bomb-making supplies, and small drones. They also include stealing sensitive data regarding targets detected by the organization anywhere in the world, such as secret maps, codes, and numbers, which can facilitate the implementation of terrorist operations.

ISIS websites on the Deep Web included advertisements for fundraising "terrorist" activities. An advertisement appears on the home page of ISIS news site employs a title that uses Islam as a cover for terrorist operations, namely "Funding the Islamic battle starts from here" (Hisham Saghur, 2019). Islam has nothing to do with these terrorist battles. Such titles are translated into both Arabic and English together. By clicking on the advertisement, an internet user will be directed to a page called "Fund the Islamic struggle" for fundraising terrorist operations in cryptocurrency through an online address for financial transactions. It is noteworthy that the European Police Agency (Europol) issued warnings of the risk of ISIS launching attacks in Europe and explained that this risk is still remarkably high. The head of Europol's Counter-Terrorism Centre, Manuel Navarrete, said: "As ISIS strength declines, the organization is urging its members to launch lone attacks in their countries instead of directing them to travel."

Part II

Artificial Intelligence and Opportunities for Countering Extremism and Terrorism

Introduction

Several opportunities are available to adapt systems to combat terrorist operations and to invest the outputs of artificial intelligence to analyze the expected terrorist behavior and detect indications of terrorism, in addition to detecting terrorist content on social media sites, using algorithms to confront smuggling of firearms, and developing terrorist fortifications using artificial neural network systems (*course.elementsofai*, 2020). These issues are addressed in the following three topics:

Topic 1: Opportunities for using artificial intelligence applications in predicting terrorist operations.

Topic 2: Utilization of algorithm-based software to enhance counter-terrorism activities.

Topic 3: Digital security cooperation mechanisms for counter-cyberterrorism.

1st Topic

Opportunities for Using Artificial Intelligence Applications in Predicting Terrorist Operations

Artificial intelligence (AI) is considered a powerful tool in developing the field of combating organized crime and enhancing intelligence. AI can be used in many different fields in criminal research, such as criminal analysis, investigations, genetic analysis, facial recognition, and location identification (Ammar Al-Babli, 2023). Using artificial intelligence technologies, criminal investigators can analyze substantial amounts of available data and information, which increases their chances of success and allows them to make appropriate decisions regarding similar crimes in the future. In addition, artificial intelligence can help to analyze genetic data and to identify suspects and prove incriminating evidence.

Counter-terrorism operations can be improved by analyzing enormous amounts of available data and information, such as criminal records, police reports, and judicial documents, to reveal patterns, trends, and significant information that can be used in criminal investigations. Machine learning, classification and forecasting techniques can also be used to analyze data and generate accurate predictions about potential future events, as well as to analyze images, videos, and audios to uncover important evidence and information that can be used in criminal investigations.

Using artificial intelligence correctly and effectively can contribute to improving counter-terrorism efforts and enhancing public security.

The security applications of artificial intelligence are used in photography, surveillance, and facial recognition technology, which is an essential tool in identifying the perpetrators of terrorist incidents. AI has been used and has already succeeded in reducing the possibilities of error in the stages of search and investigation, as well as in the stages of prosecution and pursuit of law enforcement. It also serves to narrow the circles of suspicion and facilitate the processes of surveying and classifying relevant information, people, and data. All these potentials help to raise the level of accuracy and efficiency in the direct security aspect of confronting terrorism. AI has also provided a climate of trust in security agencies and created reassurance in public opinion towards the institutions and mechanisms involved. (Wijdan Fahd, 2022). Based on the foregoing discussions, the following section highlights the concept of artificial intelligence:

1. Definition of Artificial Intelligence

It is a branch of computer science that is concerned with creating machines or computers capable of acting like humans in an intelligent or rational manner when making decisions, using the knowledge stored in these devices or which they learn by feeding.

2. Concept of artificial intelligence in the context of confronting extremism and terrorism on social media platforms

It refers to the activation of smart software and algorithms towards achieving specific behavioral and technological goals with the aim of serving individuals around the world to disseminate specific information for multiple goals. As far as the security and intelligence aspects are concerned, smart software quickly identifies information, words, meanings, images, and videos that suggest terrorist content across platforms (including violence or dissemination of terrorist culture), which this software is responsible for detecting, monitoring, and tracking with giant technological companies in preparation for analyzing and deleting such content.

Through analyzing social media platforms with smart algorithms, artificial intelligence confronts violent extremism via the Internet, especially social media platforms, by identifying the types of people susceptible to extremist ideas. These comprise people who are potential targets for either ideologically extremist groups or mobile terrorist organizations.

The use of artificial intelligence in combating terrorism has produced some clear advantages and strengths that have been able to limit some terrorist crimes by creating the following opportunities, or more precisely, successes achieved by these strategies in combating violent terrorism:

- Analysis of big data and prediction of the future: Major AI-based tools comprise search engines, analysis systems, and natural language processing, which enable technology companies and security agencies to understand and recognize the language of terrorism and extremists. They also translate suspicious writing, which provides the ability to manage content over the Internet, especially with regard to languages used for communication between groups of people (D. Valentini, A. Lorusso, & A. Stephan, 2020).
- Other platforms support extremism under the pretext of providing freedom of expression, claiming that they do not want to restrict users. In this case, the improvement in natural language processing (NLP) has made it possible to translate content into languages of which the moderators have good command, and which can detect unusual semantic patterns on websites as well, with the aim of identifying extremist activity and terrorism, as well as its promoters and the type of extremist activity on social media platforms.
- Vulnerability to radicalization: Technology companies have developed tools to assess vulnerability to violent extremist ideologies. These include, for example, the *Jigsaw* subsidiary of *Alphabet Inc. (*formerly *Google Ideas)*, which announced its "Redirect Method," which targets users of video-sharing sites who may be susceptible to propaganda from terrorist groups such as ISIS (McKendrick, 2019).
- Monitoring: AI applications contribute to identifying the group, party, or person involved in the terrorist act, whether in implementation or planning, by analyzing data related to the operations under investigation. Such data include the type of operation, location, type of weapon, target, matching information with the previous history of the suspected group or individuals.

2nd Topic

Utilization of Algorithm-Based Software to Enhance Counter-Terrorism Activities

Facial recognition and location identification technologies integrated into artificial intelligence can help criminal investigators identify and locate suspects. This increases the effectiveness of investigations and helps maintain security. The following section will address the role of artificial intelligence in enhancing counter-terrorism operations:

1. Tools that can be used to analyze forensic evidence using artificial intelligence

- Advanced Artificial Intelligence: AI is an advanced artificial intelligence system that uses machine learning, voice and image recognition technologies, and natural language processing to analyze forensic evidence. This system relies on data related to crimes, suspects, victims, witnesses, and other available information to analyze evidence accurately and effectively (Ahmed Saleh, 2022):

2. Role of algorithms in inferring and detecting indications of terrorism

- The use of AI to predict terrorism is part of the transition from a reactive to a proactive approach to combating terrorism (Haidi Issa, 2021).

- Algorithms are used for inference to detect signs of terrorism in any environment and to identify patterns or trends in data or intelligence information that may indicate the possibility of a terrorist attack. These algorithms also analyze the data to look for specific patterns or correlations between different elements that may indicate a terrorist conspiracy (Wijdan Fahd, 2022).
- Analyzing data from surveillance cameras and other sources to detect suspicious behavior or activities. A heuristic method can then be used to draw conclusions from such data (Ammar Al-Babli, 2023).
- Big Data Analysis: Analyzing terrorism-related data, identifying models, patterns, and information that can be used to detect potential terrorist threats.
- Machine learning technologies: These include, for example, classification, clustering, and prediction to analyze terrorism-related data and identify potential models of terrorist activities (Marie Schröter, 2022).
- Textual analysis: It refers to analyzing texts related to terrorism, and identifying words, phrases and patterns used in terrorist communications.
- Temporal analysis: This type of analysis can be used to determine the times when terrorists are active and potential terrorist operations.
- Behavior analysis: It comprises analyzing suspect behavior and potential terrorist activities; it also identifies information that helps to detect suspects and prevent terrorist attacks.
- These tools and technologies are commonly used in security and intelligence services to counter terrorism and reduce potential terrorist attacks. Many real-life examples show how artificial intelligence and algorithms can be used to counter terrorism and predict terrorist operations.

3. Use of artificial intelligence in combating firearms smuggling

Illicit arms flows play a significant role in fueling conflicts in many countries, ranging from petty crimes to insurgency and terrorist activities. There are numerous negative effects, especially of illicit small arms and light weapons, on national security, as they endanger the security and peace of countries. Civilians, including militias and terrorist groups own approximately 80% of such light weapons.

Artificial intelligence can play a crucial role in combating smuggling of firearms to terrorists. Following are some examples of how artificial intelligence can be used in this context:

- Border and port monitoring: Analysis of geographic data, traffic flows, and port information to identify unusual or suspicious patterns in firearms smuggling operations. AI-enabled systems can alert security agencies to suspicious activities.
- Intelligence analysis: Analysis of information and intelligence related to terrorist networks and illegal firearms trade. Advanced machine learning technologies can analyze big data, extract patterns and trends, and find links between suspected terrorists and smugglers.
- Behavioral analysis and pattern recognition: Analysis of behavioral data and recognition of common patterns in the behavior of smugglers and potential terrorists, by monitoring and analyzing behavior. Unusual or suspicious behavior that indicates firearms smuggling can be detected.

Using intelligent applications to detect the smuggling of firearms to terrorists, many AI-based tools, methods, and algorithms can be used as follows:

- Machine Learning: Machine learning technologies can be used to develop models capable of recognizing patterns of firearms smuggling. These patterns are trained using a wide range of data that includes known examples of smuggling cases.
- Image and video recognition: (Computer Vision) Image and video recognition technologies can be used to detect firearms in images. Shape and pattern recognition algorithms analyze images and videos and identify the weapons in them. These technologies can be used at checkpoints or border control to detect smuggled weapons.
- Deep Neural Networks: They extract information from unrelated and complex data, and can be used to analyze texts, images and videos related to smuggling operations to uncover unusual models and patterns. Artificial neural networks link people and terrorist and criminal institutions that operate in secret. These networks cluster link and monitor these groups and extract information for security agencies in the same field.

4. Developing neural networks and algorithms in terrorist criminal investigations

The development of neural networks and algorithms plays a vital role in terrorist criminal investigations. Artificial neural networks are computational models inspired by the human brain system. They are considered part of a set of artificial intelligence tools used to analyze data and extract valuable information, as explained in the following section.

- Neural networks and algorithms allow extracting essential information and analyzing big data related to terrorist crimes. There are several methods that can be used in this context:

- Deep Neural Networks: These can be used to analyze data related to terrorist crimes. Such networks allow training models that extract information and distinctive patterns to determine terrorist behavior and predict potential activities.
- Classification Algorithms: Classification algorithms, such as the Support Vector Machine and the Decision Tree method, can be used to classify data related to terrorist criminal investigations. These algorithms serve to determine terrorist behavior and distinguish between normal and abnormal activities.
- Cluster Analysis: These technologies can be used to analyze data related to terrorist crimes and group them into similar clusters. This can help to identify common patterns and interconnections between crimes and to reveal potential groups of suspects.

5. Role of artificial intelligence, public intelligence, improved decision-making process, and big data analysis at the security level

The analysis of big data and information has become the basis for making strategic decisions to combat crimes, terrorism, and national security threats, as well as to build human and logistical capabilities and future plans. The processing and analysis of big data and the use of artificial intelligence reveal the necessary clues to discover criminal and terrorist plans in their initial stages, narrow the workspace, and consequently cut down on efforts and funds, thus leading to increased efficiency and professionalism. These tasks are performed by establishing links and patterns and building algorithms that allow for the extraction of expectations, scientific implications, and implementation steps from the flow of data and information. These types of analysis (Ziad Al-Hajaya, 2021) include the following:

- Through the use of diverse information analysis, AI systems help to understand the surrounding environment in a deeper and more comprehensive way, analyze patterns and trends, predict future events, and provide effective solutions and procedures in the fields of security and intelligence. By analyzing this large amount of big data, real-time and instant analyses and scenarios can be provided, taking into account rapid changes, and helping to improve the decision-making process and to support military forces in the field. Big data is used in the field of national security to analyze the actions of individuals and collect information about their behavior through social media networks. This data includes discussions on sensitive and accurate issues and is considered extremely valuable. Social media analysis can also be used to uncover people who have several accounts on these networks, by analyzing and linking data. This type of analysis is considered an effective tool in fighting terrorism, as it makes it possible to identify supporting networks, locate supporters and analyze data (Iman Rajab, 2019).

3rd Topic

Digital Security Cooperation Mechanisms for Counter-Cyberterrorism

International cooperation in the security field across various arenas serves to achieve several goals that represent new aspects of this cooperation and stress its necessity. It can be said that these goals are realized in reality as ends which all security institutions in the Arab countries seek to achieve in order to build bridges of cooperation between Arab security institutions and achieve Arab national security (Moataz Abdul Rahman, 2020).

1. Axes for developing digital cooperation policies between Arab security agencies

This access includes collecting, analyzing, and evaluating information related to terrorism, determining threat levels, issuing threat warnings, analyzing the information collected, and combining the expertise of police and government departments and agencies in the counter-terrorism field. In this way, the information can be analyzed and processed on a common basis, with an eye to sharing new applications and genetic fingerprinting applications with INTERPOL and Europol.

2. Methods of digital security cooperation to limit the spread of cybercrimes

Terrorist crimes and financing terrorist groups

- Exchanging information about the activities and crimes of terrorist groups and organizations, their mutual relationship, their leadership, their members, their secret organizational structures, their public façade, their locations, their means of financing, their training methods, and the weapons they use

(Montaser Hamouda, 2021);

- Developing and strengthening methods of monitoring and exchanging information to uncover plans or activities aimed at transporting, importing, exporting, storing, or using of weapons, ammunition, and explosives, as well as other materials and means that help to commit terrorist acts transnationally.
- Accessing the flow of data from one country to another and Internet Protocol (IP) tracking data.
- Viewing cybercrime as a commercial service where criminals use innovative technologies to commit cyberattacks against governments, companies, and individuals. These crimes do not stop at national borders, whether physical or virtual, but cause considerable damage, and pose tangible threats to victims all over the world. For such reasons, the exchange of technology has become a crucial issue, especially for police agencies entrusted with combating cybercrimes; it makes these agencies able to understand the capabilities that technology provides to criminals and how to use these technologies as tools to combat cybercrime, especially with regard to the change and use of online behaviors and trends in light of the Covid-19 pandemic.
- Exchanging the experiences of security agencies in filling security gaps related to collecting and analyzing available information about criminal activities committed in the digital space with the aim of providing countries with intelligence information, such as:

- Protecting critical electronic infrastructure from online hacking and protecting important and vital facilities from cyber-attacks, especially Denial of Service (DoS) attacks.

References:

List of References

I. Arabic References

- Abu Douh, Khaled Kazem (2022). "Policies to Deal with "Tik Tok" Application: Security Challenges." Security Research Center, Naif Arab University for Security Sciences, https://spp.nauss.edu.sa/index.php/spp/ article/view/82/60.

- The United Nations Global Counter-Terrorism Strategy. (n.d.). Retrieved from https://news.un.org/ar/focus/counter-terrorism.

- Terrorism and Human Rights. (n.d.). https://www.ohchr.org/ar/documents/reports/terrorism-and-human-rights-report-united-nations-high-commissioner-human-rights. (Report of the United Nations High Commissioner for Human Rights A/HRC/45/27).

- "Bitcoin and the Charity of Jihad" (2021). European Center for Counter-Terrorism and Intelligence Studies.

- Al-Bably, Ammar (2023). "Artificial Intelligence in Confronting Rumors and Terrorist Financing Crimes in the Cyber Environment: Repercussions and Ways of Confrontation." Arab Organization for Administrative Development, League of Arab States.

- Al-Bably, Ammar (2023). "Artificial Intelligence Mechanisms in Confronting Violent Extremism." *Journal of Police and Legal Sciences*, Volume 14.

- Al-Babli, Ammar (2022). "Digital Security Cooperation between Arab Security Agencies." Security Policy Papers. Naif Arab Academy for Security Sciences Riyadh.

- Al-Bar, Adnan Mustafa (2020). "Big Data and its Application Areas." College of Computers and Information Technology, King Abdulaziz University, KSA.

- Al-Bahyy, Raghda (2021). "Deepfake: Real Security Challenges and Problems." https://ecss.com.eg/14200/. Egyptian Center for Thought and Strategic Studies (ESCC), Cybersecurity Unit.

- Al-Hajaya, Ziad (2021). "Big Data Processing and Artificial Intelligence in Combating Organized Crime and Terrorism." Jordan: Shorufat Center for Globalization & Terrorism Studies. https://www.shorufatcenter.com/4326/.

- Al-Huqail, N. A. (2023). "The Effectiveness of Artificial Intelligence in Countering Crime and Terrorism."

- Al-Samalouti, Nabil (2021). "Extremism and Terrorist Groups in Egypt: Emergence, Goals, Islam's Attitude, Methods of Confrontation." *Journal of Social Sciences Research and Development*, Issue no. 3.

- Al-Sharqawi, Nisreen (2022). "The Dual Roles of Social Media Platforms." Egyptian Center for Thought and Strategic Studies (ESCC). https://marsad.ecss.com.eg/73432/.

- Al- Attar, Ahmed Shawqi (2021). "ISIS Online Banks Trade in Bitcoin." https://www.albawabhnews.com/ Retrieved on 3/3/2022.

- Al-Alawi, Ibrahim (2023). "Applications of Artificial Intelligence in Forensic Science." *Scientific Journal of Forensic Sciences*.

- Al-Omari, Ahmad Adel (2013). *Security Planning to Confront the Repercussions of International Crises*. PhD thesis. Police Academy, Cairo, Egypt.

- Counter-Terrorism Reference Curriculum. (n.d.). https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/2012-DEEP-CTRC-arabic.PDF(2020).

- Al-Wazzan, Al-Sayed (2014). *Information Authority: A Contemporary Security Vision*. Dar Al-Nahda Al-Arabiya.

- Orofino, Elisa. (2022). *Exploring Online Radicalization and How to Spot Extremist Content and What to Do About It: A British Case Study*. https://eeradicalization.com/exploring-online-radicalization-how-to-spot-extremist-content-and-what-to-do-about-it/.

- Report of the "European Eye on Radicalization" website.

- "INTERPOL Policing Capabilities Programme" (2019). Interpol Report. Retrieved from https://www.interpol.int/ar/1/2/2019/88th-INTERPOL-General-Assembly.

- Hamouda, Muntaser (2021). *International Criminal Police Organization (INTERPOL)*. 2nd Edition. Dar Al-Fikr Al-Jami'a.

- Khalifa, E. (2018). "Opportunities and Threats of Artificial Intelligence in the Next Ten Years." Future Report.

- Omand, David (2015). "Social Media Intelligence." Emirates Center for Strategic Studies and Research, Issue no. 152

- Rashid, Sameh. (2021). "Artificial Intelligence in the Face of Terrorism: Opportunities and Challenges." *Strategic Horizons Magazine* (4).

- Al-Qadhi, Rami Metwally (2021). "International Security Confrontation of Criminal Activities Committed via the Dark Web." *Public Security Magazine* (253).

- Rajab, Iman (2019). "Counter-terrorism Policies in Egypt." Center for Political and Strategic Studies, (296).

- Schröter, Marie (2022). *Artificial Intelligence and Countering Violent Extremism: A Primer*. King's College London; GNET is a special project supervised by the International Centre for the Study of Radicalization and Political Violence.

- Saghur, Hisham (2019). "Social Networking Sites: A Fertile Platform for Spreading Extremism and Recruiting Jihadists." https://www.europarabct.com/?p=53141. European Center for Counter-Terrorism and Intelligence Studies.

- Saleh, Ahmad (2022). *Applications of Artificial Intelligence and its Role in Crowd Security Management*. PhD Thesis. Police Academy, Cairo, Egypt.

- Saleh, J. A. (2014). *Ideological Terrorism: Forms and Practices*. Library of Law and Economics.

- Abdel Salam, Sh. (2020). “5G Warfare: Methods of Implosion on the International Arena.” Future Center for Advanced Research and Studies.

- Abdel Sadiq, Adel (2018). “Cryptocurrencies Threaten the National Economy and Security.” Arab Center for Cyberspace Research.

- Abdel Moati, N. (2012). “Social Media Platforms and the Industry of Extremism and Terrorism: Reality and Mechanisms of Confrontation.” *International Politics Journal* (213).

- Fahd, Wijdan (2022). “Study of Artificial Intelligence: Between Terrorist Tactics and National Strategies.” https://trendsresearch.org/ar/insight/ai-between-terrorist-actics-and-national-strategies/. Emirates, Abu Dhabi: Trends Center for Research and Studies.

Fouda, Hala (2020). “Social Media and National Security of Countries.” https://marsad.ecss.com.eg/21163. Cairo: Egyptian Center for Thought and Strategic Studies (ESCC).

Qunswa, Ali. (2021). “Electronic Warfare.” *Lebanese National Defense Journal*, (A peer-reviewed scientific journal), Vol. 118.

Interpol Innovation Centre (2019). “Artificial Intelligence and Law Enforcement: Challenges and Opportunities.” https://www.interpol.int/ar/4/4/2.

Abdel Rahman, Moataz (2020). *Role of International Exchange of Information in Criminal Evidence*. PhD Thesis. Police Academy, Cairo, Egypt.

Miqdadi, Saleh (2021). Incentives for International Cooperation in Combating Terrorism (International Report). IMCTC. Retrieved from https://imctc.org/ar/Pages/default.aspx.

Miqdadi, Saleh Al-Saad. (5 3, 2021). International report, incentives for international cooperation in combating terrorism, Islamic Military Coalition to Combat Terrorism. Retrieved from https://imctc.org/ar/Pages/default.aspx.

United Nations Office on Drugs and Crime (2021). “International Cooperation in Criminal Matters: Counter-Terrorism.” https://www.unov.org/unov/ar/unodc.html.

Independent website in Arabic (17/12/2021). “Cyberattacks: Most Dangerous Global Economic Weapon in 2022.” Retrieved from https://www.independentarabia.com.

Issa, Heidi (2021). “Human Rights in the Age of Artificial Intelligence: Data, Visions, and Solutions.” *Sharia and Law Journal,* Vol. 35.

II. References in English

Counter-Terrorism Reference Curriculum (2023). https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/2012-DEEP-CTRC-arabic.PDF(2020).

“Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes” (2023). United Nations Office of Counterterrorism (UNOCT), 2021 New York. https://www.cambridge.org/core/journals/international-journal-of-law-in-context/article/regulating-terrorist-content-on-social-media-automation-and-the-rule-of- law/B54E339425753A66FECD1F592B9783A1.

belfercenter.ksg.harvard (2023). Joseph S. Nye: The Future of Power. Press Release. Harvard Kennedy School, Belfer Center for Science and International Affairs, December 2019. http://belfercenter.ksg.harvard.edu/publication/20690/joseph_s_nyes_the_future_of_power.html. Retrieved from belfercenter.ksg.harvard.

blog.khamsat (2022). https://blog.khamsat.com/tiktok-profit-guide/. Retrieved from https://blog.khamsat.com/tiktok-profit-guide/.

Canada Police (2021). “Police Use of Facial Recognition Technology in Canada and the Way Forward.” *Police Science*, Canada.

Rigano, Christopher (January 2019). “Using Artificial Intelligence to Address Criminal Justice Needs.” (*US NIJ Journal* 280, January 2019). Retrieved from www.nij.gov/journals/280/Pages/using-artificial-intelligence-to-address-criminal-justice-needs.aspx accessed 2 December 2021.

course. elementsofai (2020). https://course.elementsofai.com/1/1: Reaktor & University of Helsinki (2018), “How should we define AI?” Retrieved from https://course.elementsofai.com/1 /1.

demandsage (2, 2023). https://www.demandsage.com/tiktok-user-statistics/#:~:text=One%20billion%20active%20users%20spread,media%20platforms%20as%20of%. Retrieved from https://www.demandsage.com/tiktok-user-statistics/#:~:text=One%20billion%20active%20users%20spread,media%20platforms%20as%20of%.

Hammes (Sep 4, 2020). “Terror and Technology from Dynamite to Drones.” *War on the Rocks*. Retrieved from https://warontherocks.com/2020/09/terror-and-technology-from-dynamite-to-drones/

McKendrick, Kathleen (2019). “Artificial Intelligence Prediction and Counterterrorism.” CHATHAM HOUSE, August 2019, P.9.

Molla, R. and Stewart, E. (2019). “How 2020 Democrats think about breaking up Big Tech.” Retrieved from https://www.vox.com/policy-and-politics/2019/12/3/20965447/tech-2020-candidate-policies-break-up-big-tech.

Office of the Privacy Commissioner of Canada. (n.d.). “Police Use of Facial Recognition Technology in Canada and the Way Forward.”

Quemener, M. (2017). “Enquetes dans le Darkweb.” Dalloz IP/IT (version Dalloz IP/IT).

Valentini, D., Lorusso, A. & Stephan, A. (2020). Onlife Extremism: Dynamic Integration of Digital and Physical Spaces in Radicalization.*” Frontiers in Psychology*.

Wiesenthal (2021). Retrieved from https://www.wiesenthal.com/about/regional-offices/los-angeles.html