



ISSN: 1112-4040 & EISSN: 2588-204X

رت م د: 1112-4040، رت م د: 2588-X204

تاريخ النشر: 2026-06-09

الصفحة: 301-281

السنة: 2026

العدد: 01

المجلد: 40

Date of Publication: 09-06-2026

pages: 281-301

Year: 2026

N°: 01

Volume: 40

دور الذكاء الاصطناعي في مكافحة جريمة تمويل الإرهاب الإلكتروني

The Role of Artificial Intelligence in Combating the Crime of Electronic Terrorism Financing

Nabila Ben Cheikh¹

boukannabilaabechikh@gmail.com

University of Constantine1 Frères Mentouri,

تاريخ القبول: 2026/05/24

تاريخ الإرسال: 2026/01/14

ABSTRACT:

Electronic financing of terrorism has become one of the most pressing problems troubling most countries, including Algeria. This issue results in difficulties in tracing and controlling such funds, producing negative effects on financial and banking systems as well as on criminal justice institutions—all through the use of artificial intelligence technologies.

The growing threat of cyber terrorism stems from the widespread use of technology by states, which terrorist groups have exploited to threaten various political and economic sectors by hacking security websites, in addition to targeting economic institutions such as banks and adopting electronic financing strategies.

Given the emergence of new methods for launching and funding cyber terrorist attacks through digital networks beyond the scope of criminalization, there is an urgent need to strengthen international, regional, and national efforts, as well as to promote cooperation and information exchange concerning financial movements and bank accounts among countries via the Internet.

Keywords: Cyber terrorism; electronic financing; artificial intelligence; bank accounts; Internet.

الملخص:

لقد أصبح التمويل الإلكتروني للإرهاب من أهم المشاكل التي تترق معظم الدول بما فيها الجزائر، مما ينتج عنه صعوبة إجراءات تعقب وضبط تلك الأموال وبما له من آثار سلبية على النظم المالية والمصرفية وعلى أجهزة العدالة الجنائية، وكل ذلك باستخدام تقنيات الذكاء الاصطناعي.

¹ - المؤلف المرسِل: Dr Nabila Ben Cheikh . boukannabilaabechikh@gmail.com



ISSN: 1112-4040 & EISSN: 2588-204X

رت م د: 1112-4040، رت م د: 2588-X204

تاريخ النشر: 2026-06-04

الصفحة: 301-281

السنة: 2026

العدد: 01

المجلد: 40

Date of Publication: 04-06-2026

pages: 281-301

Year: 2026

N°: 01

Volume: 40

The Role of Artificial Intelligence in Combating the Crime ----- . Nabila Ben Cheikh

والتهديد المتزايد للإرهاب الإلكتروني يرجع إلى استخدام الدول للتكنولوجيا، فقد استغلت الجماعات الإرهابية هذا الوضع لتهديد مختلف القطاعات السياسية والاقتصاد من خلال اختراق المواقع الأمنية، بالإضافة إلى المؤسسات الاقتصادية كالبنوك، وانتهاج سياسة التمويل الإلكتروني. ونظراً لظهور أساليب جديدة شن هجمات إرهابية إلكترونية وتمويلها عبر الشبكات الرقمية خارج نطاق التجريم، ولذلك دعت الضرورة لتعزيز الجهود الدولية والإقليمية والوطنية وكذلك التعاون وتبادل المعلومات حول حركات الأموال والحسابات المصرفية بين الدول على شبكة الإنترنت..

الكلمات المفتاحية: الإرهاب الإلكتروني، التمويل الإلكتروني، الذكاء الاصطناعي، الحسابات المصرفية، شبكة الإنترنت.

Introduction

Over the last two decades the world has witnessed a radical transformation in the nature of security threats as a result of the digital revolution, which has turned cyberspace into a field of activity for terrorist groups.

These groups have begun to employ artificial intelligence techniques to develop new methods of financing and concealment using modern technologies, digital currencies, and smart platforms to collect and transfer funds illicitly.

The importance of this topic lies in the spread of terrorism throughout society in general and especially in the Arab world. Although there are numerous laws addressing terrorism (and — to a lesser extent — cyber terrorism), these statutory texts are retroactive or lagging; this gap stems from the evolution of these crimes and the emergence of new methods for carrying out cyber terrorist attacks that fall outside existing criminalization frameworks.

This study aims to clarify the relationship between artificial intelligence and electronic terrorism financing, and to assess the extent to which national and international laws contribute to combating cyber terrorism.

Traditional criminal laws no longer keep pace with this type of crime, which helps perpetrators evade punishment because Algerian law has not expressly criminalized cyber terrorism and its financing.

Therefore, it is important to answer the following problem statement: How does artificial intelligence contribute to financing cyber terrorism? What legislative



ISSN: 1112-4040 & EISSN: 2588-204X

رت م د: 1112-4040، رت م د: 2588-X204

تاريخ النشر: 2026-06-04

الصفحة: 301-281

السنة: 2026

العدد: 01

المجلد: 40

Date of Publication: 04-06-2026

pages: 281-301

Year: 2026

N°: 01

Volume: 40

The Role of Artificial Intelligence in Combating the Crime -----, Nabila Ben Cheikh

measures can limit its spread and combat it? What international efforts exist to prevent the exploitation of this technology for financing terrorist activities?

To answer the research question, the study relies primarily on the descriptive and analytical methods, which are the most suitable for the subject. The research proceeds by defining artificial intelligence, cyber terrorism, and its financing, and by an objective reading and analysis of the causes and motives behind cyber terrorism crimes.

The study is divided into two main sections:

Section One: The Conceptual Framework of Artificial Intelligence and Cyber Terrorism

Modern science has moved toward inventing new methods for storing information and transferring knowledge and experience from the human element to something that mimics the human mind and becomes its partner in thinking and able to follow the lifecycle of that information. It was thus necessary to resort to modern systems capable of absorbing and developing this knowledge — hence the emergence of the idea of artificial intelligence (AI), which we will define (**First requirement**).

Moreover, the outputs of the technological revolution led to the emergence of new concepts, most notably cyber terrorism, whereby terrorists resort to using scientific means to achieve their criminal aims (**Second requirement**).

Since cyber terrorism is treated as a crime, it must have its constituent elements — material and moral (**Third requirement**).

First Requirement: The Concept of Artificial Intelligence

AI is an umbrella term for a series of advanced techniques that the world has witnessed over recent decades, and there is no single simple definition of AI (**Branch One**). AI is characterized by a set of features and properties and has significant importance across many fields (**Branch Two**). Given its pervasive impact, the question of granting legal personality to AI has arisen (**Branch Three**).

Branch One: Definitions of Artificial Intelligence

First: Linguistic (lexical) definition:

The Arabic root for intelligence (ذكاء) denotes keenness of mind, quickness of insight and understanding. It is the ability to analyse, synthesize, distinguish, choose, and adapt to different situations. “To be intelligent” traditionally meant to be quick-



ISSN: 1112-4040 & EISSN: 2588-204X

رت م د: 1112-4040، رت م د: 2588-X204

تاريخ النشر: 2026-06-04

الصفحة: 301-281

السنة: 2026

العدد: 01

المجلد: 40

Date of Publication: 04-06-2026

pages: 281-301

Year: 2026

N°: 01

Volume: 40

The Role of Artificial Intelligence in Combating the Crime -----, Nabila Ben Cheikh

witted and fully understanding. Artificial intelligence is described as the capacity of a machine or device to perform some activities that require intelligence — such as actual inference and self-repair. (Omar, 2008, pp. 817-818)

Second: Terminological (technical) definitions:

AI consists of two parts: “intelligence,” meaning the capacity for learning, adaptation, flexibility, and responding to situations and problems — the ability to understand and think; and “artificial,” which relates to actions performed by humans or the non-natural/man-made. Thus, AI can be characterized as man-made intelligence. (Moussa & Bilal, 2019, p. 18)

In general, AI is a science that aims to provide intelligent software and to create smart machines to perform tasks similar to those performed by humans, in order to facilitate life and work at lower cost and effort. (Abu al-Nasr, 2020, pp. 131-133)

Researchers’ definitions converge on the idea that AI seeks to emulate human intelligence and mental capabilities — including creativity, inference, self-learning, and equipping systems with skills like conversation, transcribing speech to text, etc. (Dahshan, 2020, p. 12)

Some jurists define AI as “part of computer science aiming to design intelligent systems that make computers represent and simulate human thinking and certain human behavioral abilities, giving them properties we recognize as intelligence in human behavior.” (al-Faqi, 2012, p. 8)

Technically, AI can be defined as a computer-programmed machine that uses algorithms and specific procedures to perform a task; the programmed device receives inputs automatically and applies the programmed logic. (Hudhaib, 2024, p. 11)

Consequently, AI revolves around the use of computers and various programs to perform operations that resemble human intelligence, using computational algorithms and complex mathematical rates.

Oxford Dictionary defines AI as a “faculty of understanding,” i.e., the manufacture of machines that perform tasks requiring intelligence. (Belbay, 2024, p. 27) Other definitions emphasize autonomous machines that operate within complex, interconnected environments. (Al-Deeb, 2023, p. 23)



ISSN: 1112-4040 & EISSN: 2588-204X

رت م د: 1112-4040، رت م د: 2588-X204

تاريخ النشر: 2026-06-04

الصفحة: 301-281

السنة: 2026

العدد: 01

المجلد: 40

Date of Publication: 04-06-2026

pages: 281-301

Year: 2026

N°: 01

Volume: 40

The Role of Artificial Intelligence in Combating the Crime ----- . Nabila Ben Cheikh

Therefore, AI represents a modern stage of technological use designed to execute tasks typically attributed to humans but done automatically by programs or devices. (‘Ali, 2024, p. 49)

Branch Two: Characteristics and Importance of AI

AI technology is precise and fast, with high learning and perception capacities. Key characteristics include:

First: Knowledge representation:

AI programs structure information using facts, relationships among facts, and rules that bind these relationships into a knowledge base that stores as much information as possible. (Al-‘Ubaidi, 2022, p. 43)

Second: Prediction and adaptation:

AI systems can predict and adapt (e.g., spell correction, predictive text in search engines, route suggestions in mapping software). (al-Faqi, 2012, p. 67)

Third: Autonomy for decision-making:

AI encompasses perception, understanding, interpretation, interaction, decision-making, behavioural adaptation, and goal achievement (Hudhaib, 2024, pp. 13-14).

It can take independent decisions via unsupervised machine learning. Complete autonomy has not yet been reached, but autonomy increases with rapid development. (Belbay, 2024, p. 40)

Fourth: Its Abilities of Motion, Learning, and Perception

With the emergence of **Big Data** and the increasing size of the “data and information” community along with the integration of these datasets, the current field of artificial intelligence (AI) has undergone profound changes since the term was first coined in 1956 by the scientist **John McCarthy**. AI has now entered a new stage, distinguished by advanced intelligent perceptual abilities — including **visual perception, speech recognition, auditory perception, information processing, and learning** — as seen in **unmanned aerial vehicles (drones), automated lighting systems, and smart thermostats**.

However, some reject the idea that AI devices possess genuine perceptual ability, arguing that they are incapable of perception on their own and only “perceive” after being **fed with pre-existing data**.



ISSN: 1112-4040 & EISSN: 2588-204X

رت م د: 1112-4040، رت م د إ: 2588-X204

تاريخ النشر: 2026-06-04

الصفحة: 301-281

السنة: 2026

العدد: 01

المجلد: 40

Date of Publication: 04-06-2026

pages: 281-301

Year: 2026

N°: 01

Volume: 40

The Role of Artificial Intelligence in Combating the Crime ----- . Nabila Ben Cheikh

The growing attention devoted to AI reflects increasing recognition of its importance, which is manifested in the following indicators:

- **AI plays an essential role in many sensitive fields**, whether in **medicine**—such as assisting in disease diagnosis and drug prescription—or in **security and military fields**, including **the manufacture of weapons**.

- Regarding the **general use of legal technology**, law enforcement has taken a leading role not only in the **United States** but also in many **European countries**. Police authorities have adopted **Big Data** technology to help predict potential crimes before they occur, in an initiative known as **“Predictive Policing.”** In **England**, predictive policing was recently endorsed by the **Supreme Court**, while the **German police** have also introduced this new technology through programs known as **“PreCobs” (Pre-Crime Observation System)** or **“SKALA” (System zur Kriminalitätsanalyse und Lageantizipation)**. These systems analyze characteristics of certain crimes (crime scene, victims, etc.) to estimate the likelihood of an individual reoffending. The “crime prediction” system displays risk levels for different areas and applies preventive measures to the most vulnerable zones, enabling police officers to be present at crime scenes **before the crime actually occurs** (Ibrahim, 2024, pp. 47-48)

- **Artificial intelligence also assists in providing legal consultations** and offers broader access to information across various **security and military domains**. It enables the **use of smart machines** to perform strenuous tasks such as **exploring unknown areas** and **participating in rescue operations during natural disasters**.

- **AI contributes to solving mathematical problems and theories**, is employed in the **design of intelligence-related games**, and is used in **IQ testing** and many other fields (Hudhaib, 2024, p. 16)

- **AI allows for a better understanding of human intelligence** by uncovering the inner workings and depths of the **human brain**, thus making it possible to **simulate its functions**. As is well known, the **nervous system** and the **human brain** are among the most complex organs, functioning in constant and integrated coordination to recognize and identify objects (Al-‘Ubaidi, 2022, pp. 45-46).

Branch Three: The Importance of Applying Artificial Intelligence Techniques in Crime Detection



ISSN: 1112-4040 & EISSN: 2588-204X

رت م د: 1112-4040، رت م د: 2588-X204

تاريخ النشر: 2026-06-04

الصفحة: 301-281

السنة: 2026

العدد: 01

المجلد: 40

Date of Publication: 04-06-2026

pages: 281-301

Year: 2026

N°: 01

Volume: 40

The Role of Artificial Intelligence in Combating the Crime ----- . Nabila Ben Cheikh

As previously mentioned, companies producing artificial intelligence systems have launched a **new intelligent system** capable of **predicting crimes before they occur**, while also providing a **vast amount of visual information** to help identify the perpetrator ('Ali, 2024, p. 60).

This system or program has contributed to uncovering those responsible for **human trafficking cases in Thailand**, and **University College London** is currently developing an **image-analysis system** capable of identifying the number of **microscopic particles** found on a suspect's **shoe sole**—such as **gunshot residue**—in order to determine the **time frame during which the suspect was present at the scene** (Hudhaib, 2024, p. 123).

Reliance on **artificial intelligence systems** therefore aims to **establish the link between the crime and the perpetrator** and to **combat crime in its modern forms** through the **examination of blood and its chemical composition**, as well as **hair, skin, cells, and weapon traces**.

Second requirement: Cyber Terrorism

Terrorism is a **global phenomenon** experienced by societies in multiple forms and manifestations. Due to **technological and digital transformations**, a new set of crimes has emerged—most notably **cyber terrorism**, which has arisen as a result of terrorist groups' exploitation of modern technologies and the virtual world.

Several attempts have been made to define **cyber terrorism**, although there is **no unanimous legal or scholarly consensus** on its precise meaning (**Branch One**).

As the forms of terrorism evolve with **scientific and technological progress**, its manifestations also diversify (**Branch Two**).

And since **cyber terrorism** is classified as a **crime**, it naturally possesses its **own constituent elements** that determine and distinguish it from other crimes (**Branch Three**).

Branch One: The Concept of Cyber Terrorism

Terrorism, in all its forms and varieties, arises from **multiple motives** and pursues **specific goals**. Consequently, **electronic systems** and **information infrastructure** have become **prime targets** for terrorists. Given the growing danger of the criminal activities of terrorist groups and organizations, these actors have taken advantage of **modern technology** to achieve their **criminal objectives** (Matar, 2005, p. 175).



ISSN: 1112-4040 & EISSN: 2588-204X

رت م د: 1112-4040، رت م د: 2588-X204

تاريخ النشر: 2026-06-04

الصفحة: 301-281

السنة: 2026

العدد: 01

المجلد: 40

Date of Publication: 04-06-2026

pages: 281-301

Year: 2026

N°: 01

Volume: 40

The Role of Artificial Intelligence in Combating the Crime ----- . Nabila Ben Cheikh

First: Definition of Cyber Terrorism

There are numerous definitions of **cyber terrorism**, primarily because there is **no universally agreed-upon definition of terrorism itself**; the definitions vary even further in scope and emphasis.

According to the **Arab Convention on Combating Terrorism**, terrorism is defined as:

“The dissemination of terror among people, causing harm to the environment or to public or private facilities, regardless of motives and purposes, or intimidating individuals or endangering national resources by offering or exposing them to harm.”

(Al-‘Amoush, 2006, p. 138).

The scholar **Barry Collin** was among the first to use the term “**cyber terrorism**” in the **1980s**, defining it as: “An electronic attack aimed at threatening or assaulting governments in pursuit of political, religious, or ideological objectives, where the attack must have a destructive or disruptive impact equivalent to the physical acts of traditional terrorism.”

In general terms, **cyber terrorism** (or **electronic terrorism**) can be defined as: “A physical or moral attack or threat conducted by a state, group, or individual through the use of information resources and electronic means in various forms of assault.” (Mahmoud, 2023, p. 22).

Cyber terrorism relies on the **use of scientific and technological capabilities**, and the **exploitation of communication tools and information networks** to **intimidate, terrorize, harm, or frighten** others (Mahmoud, 2023, p. 22).

Second: Motives of Cyber Terrorism

The **causes and motives** of cyber terrorism vary according to **political orientations, economic and social conditions, and differences in religion and ideology**.

1. Personal Motives: There are numerous personal factors that lead to terrorism, the most prominent of which include:

→ **Lack of a sense of belonging or loyalty** to the family and society, meaning a weak connection to one’s homeland and failure in family life.



ISSN: 1112-4040 & EISSN: 2588-204X

رت م د: 1112-4040، رت م د: 2588-X204

تاريخ النشر: 2026-06-04

الصفحة: 301-281

السنة: 2026

العدد: 01

المجلد: 40

Date of Publication: 04-06-2026

pages: 281-301

Year: 2026

N°: 01

Volume: 40

The Role of Artificial Intelligence in Combating the Crime ----- Nabila Ben Cheikh

→ **Desire for fame:** an unqualified individual seeks, in vain, to gain recognition or validation, often feeling attacked, obstructed, and destroyed (Al-Shukri, 2008, p. 193).

2. Ideological Motives (Mahmoud, 2023, p. 24):

→ **Ignorance of the true objectives of Islamic law (Shari'a)** and of the correct principles, ethics, and conduct of religion, resulting from a **misinterpretation of religious teachings**.

→ **Emergence of divergent intellectual currents**, which in turn generate divisions and sectarian fragmentation.

→ **Extremism of all kinds**—political, religious, or sectarian—which represents a serious and dangerous phenomenon.

3. Political Motives:

→ **Absence of social justice, inequality in the distribution of national wealth, and disparities in the provision of public services**, along with government neglect of citizens' needs and aspirations.

→ **Suffering of certain societies and peoples from injustice, oppression, dispossession, and violations of laws and international conventions**, which drives some communities toward **radicalization and extremism**.

Third: Characteristics and Objectives of Cyber Terrorism (Khalifa, 2005, p. 12)

Cyber terrorism is a **transnational terrorist crime** that crosses **borders, countries, and continents**. It is not confined to any limited geographical area, which makes it **difficult to control or prosecute**, largely due to the **limited experience** of security and judicial institutions in handling such crimes, as well as the **multiplicity of individuals** who cooperate in committing them.

Proving **cyber terrorism offenses** is also difficult because **digital evidence disappears quickly** and can be **easily destroyed**.

Cyberterrorist attacks are further characterized by their **low cost**, requiring only individuals with **technical skills and experience** in handling information networks and **minimal resources**. These crimes are often committed in a **quiet environment**, without the need for **force, violence, or weapons**, which is why they are often referred to as **"soft crimes."** All that is required is a **computer and an Internet connection** (Khalifa, 2005, p. 12).



ISSN: 1112-4040 & EISSN: 2588-204X

رت م د: 1112-4040، رت م د: 2588-X204

تاريخ النشر: 2026-06-04

الصفحة: 301-281

السنة: 2026

العدد: 01

المجلد: 40

Date of Publication: 04-06-2026

pages: 281-301

Year: 2026

N°: 01

Volume: 40

The Role of Artificial Intelligence in Combating the Crime ----- . Nabila Ben Cheikh

In addition, **cyberspace** is often used for **indirect terrorist purposes**, such as **facilitating the execution of terrorist acts** by providing information, **collecting funds**, and **spreading fear, panic, terror, and hatred** through digital means. Cyber terrorism aims to **instill fear among peoples and nations**, **disturb public peace**, and **damage communication systems, information technology infrastructure, financial resources**, and both **public and private facilities** (Hamad, 2017, p. 445).

Accordingly, it can be said that **cyber terrorism is a specific form of terrorism**, but its **digital nature** makes **young people** the group **most vulnerable to its dangers**.

Branch Two: Forms of Cyber Terrorism

As noted above, cyber terrorism has no single fixed definition; its concept evolves with technological development.

First: Exchange and Dissemination of Terrorist Information via Information Networks

Various terrorist groups and organizations use global information networks to communicate and coordinate with one another due to the low cost of communication and ease of using the networks. These groups exploit global information networks to spread and promote a culture of terrorism, create communities of like-minded individuals, and facilitate recruitment for carrying out terrorist activities (Rashed, 2005, p. 17).

These networks have also become important means for **training, planning, and execution**, in addition to hosting websites and pages that include instructions on how to make bombs and weapons, where terrorist materials or electronic messages are published and reach members of the public.

Second: Creation of Terrorist Websites

A website consists of information stored as pages, where the page designer uses a set of codes; such pages are published on the World Wide Web to achieve false goals and propagate extremist beliefs (Yusuf, 2011, p. 2).

Third: Destruction of Websites and Electronic Data

Electronic hacking is currently one of the methods used to sabotage websites. This type of attack often targets military-related information networks by penetrating air defense and nuclear-missile systems. It can also involve breaching control systems for air, land, and maritime navigation, infiltrating telephone service distribution stations, and launching a series of attacks against cellular networks.



ISSN: 1112-4040 & EISSN: 2588-204X

رت م د: 1112-4040، رت م د إ: 2588-X204

تاريخ النشر: 2026-06-04

الصفحة: 301-281

السنة: 2026

العدد: 01

المجلد: 40

Date of Publication: 04-06-2026

pages: 281-301

Year: 2026

N°: 01

Volume: 40

The Role of Artificial Intelligence in Combating the Crime -----, Nabila Ben Cheikh



ISSN: 1112-4040 & EISSN: 2588-204X

رت م د: 1112-4040، رت م د: 2588-X204

تاريخ النشر: 2026-06-04

الصفحة: 301-281

السنة: 2026

العدد: 01

المجلد: 40

Date of Publication: 04-06-2026

pages: 281-301

Year: 2026

N°: 01

Volume: 40

The Role of Artificial Intelligence in Combating the Crime -----, Nabila Ben Cheikh

Fourth: Electronic Threats

The methods of threatening employed by terrorist organizations and groups are numerous and include websites, chat rooms, and electronic messaging—threats to kill politicians, threats to bomb government buildings, etc.

Fifth: Cyber Espionage

The cyber-espionage operations carried out by terrorist groups and organizations involve obtaining secrets and information and disclosing them to hostile states or exploiting them to undermine national unity (Haymar, 2013-2014, p. 127)

Third requirement: Elements of the Cyberterrorism Crime

The crime of cyberterrorism does not differ in its elements from traditional terrorism, except in terms of the means used to commit it. It is therefore based on two elements: the material element and the mental element.

Branch One: The Material Element

Physical activity or behavior in cybercrimes requires a digital environment, a computer, and internet connectivity. It is also necessary to create a page and upload it to the host device. The elements of the material component are three: the act or behavior, the criminal outcome, and the causal link.

1. **Criminal Behavior:** The difficulty of proving criminal behavior in cyberterrorism lies in the fact that it is committed through information transmitted via computers, which cannot be physically seized (Bayyumi, 2018, p. 121)

2. **Criminal Outcome:** The criminal outcome in cyberterrorism is related to the element of danger and fear that terrorist groups and organizations instill in societies.

3. **Causal Link:** For the material element to encompass all its components, there must be a causal link between the criminal act committed by the perpetrator and its consequences, so that the outcomes result from the act. This is an essential condition for establishing criminal liability.

Branch Two: The Mental Element

Cyberterrorism is not a crime based solely on acts and their consequences; it also involves the psychological element. The crime requires criminal intent, meaning the perpetrator must be aware that their activity constitutes an assault on a legally protected right, and that their will is directed toward committing the criminal



ISSN: 1112-4040 & EISSN: 2588-204X

رت م د: 1112-4040، رت م د إ: 2588-X204

تاريخ النشر: 2026-06-04

الصفحة: 301-281

السنة: 2026

العدد: 01

المجلد: 40

Date of Publication: 04-06-2026

pages: 281-301

Year: 2026

N°: 01

Volume: 40

The Role of Artificial Intelligence in Combating the Crime -----, Nabila Ben Cheikh

behavior using electronic means, which leads to creating fear and threatening the safety of society. This constitutes specific intent.

Section Two: Electronic Financing of Terrorist Organizations

The phenomenon of terrorist financing is considered one of the most dangerous phenomena facing the national and global economy, as terrorist-financing operations encompass a range of activities to transfer funds for planning and carrying out terrorist operations.

Electronic financing of terrorist activity represents one of the forms that embody illicit financial operations which perpetrators resort to because of their ease, speed, and difficulty of detection, and because investigative and law-enforcement authorities often require technical expertise that may not be available across all security agencies. Consequently, terrorist organizations resort to electronic means to complete financial support and funding operations.

Accordingly, this study will address the objective aspect of electronic financing for terrorist groups (**First requirement**), the procedural aspects of confronting electronic financing of terrorist groups (Second requirement), and the role of international organizations in combating the financing of terrorist groups (**Third requirement**).

First requirement: The Objective Aspect of Electronic Financing for Terrorist Groups

Terrorist activities have imposed a special mode on financing operations characterized by secrecy, speed, simplicity, and transnational reach, which has driven terrorist elements to resort to electronic financing because of these advantages (Suwaylim, 2018, p. 121). Below we will first examine the concept of electronic financing (**Branch One**) and then the sources of electronic financing that support terrorism (**Branch Two**).

Branch One: The Concept of Electronic Financing

First: Definition of Electronic Financing:

Unlike comparative legislation, the Algerian legislator did not define electronic financing of terrorism. The federal legislator remedied this omission through Federal Law No. 7 of 2014 on combating terrorist crimes, which, pursuant to Article 1, defined it as "assets of whatever kind, tangible or intangible, movable or immovable, including national and foreign currency and documents or instruments



ISSN: 1112-4040 & EISSN: 2588-204X

رت م د: 1112-4040، رت م د: 2588-X204

تاريخ النشر: 2026-06-04

الصفحة: 301-281

السنة: 2026

العدد: 01

المجلد: 40

Date of Publication: 04-06-2026

pages: 281-301

Year: 2026

N°: 01

Volume: 40

The Role of Artificial Intelligence in Combating the Crime ----- . Nabila Ben Cheikh

proving ownership of those assets or any right related thereto, in whatever form, including electronic or digital form” (Faraj, 2016, p. 112).

This definition encompasses all types of funds that may be contributed to terrorist activity, and it enumerates acts that constitute financing as acts of providing, collecting, receiving, or facilitating access to funds for the benefit of an unlawful organization or a terrorist act.

Electronic financing operations frequently occur across borders: the financier transfers the funds in question from the territory of one state to another. This is done through any computer device, and funds can be transferred easily over the network from one bank account to another, with the money reaching its destination at the same time it is transferred.

Second: Types of Electronic Financing

1. **Electronic Money, Credit Cards, and Electronic Transfers:** Electronic money, transfers, and credit cards represent a conversion from the paper form to the electronic form. Terrorist organizations resort to using illicit electronic money through identity forgery in opening bank accounts, credit card forgery, electronic theft and use for illicit financing, unlawful banking transfers, or hacking personal accounts and exploiting them for transfers (Khaz'al., 2022, p. 149).

2. **Digital Electronic Financing:** Technological development has affected all economic sectors, leading financial institutions, investment companies, and banks to adopt digital financing. Financial technology has materialized in cryptocurrencies, banking financial services, and non-banking financial services. Cryptocurrencies have been used by terrorist organizations to finance their activities (Khaz'al., 2022, p. 150), as they are unregulated by governments, less subject to fluctuations, and provide a secure method for transferring funds.

Branch Two: Sources of Electronic Financing for Terrorism

First: Legitimate Sources of Financing:

Illegal activities can be financed from legitimate sources. Accordingly, terrorist groups or organizations may be funded with lawful money, for example, through legitimate business deals whose profits support terrorist activities, or through the transfer of funds via officially designated channels such as bank transfers and electronic payment methods like credit cards.

Second: Illegitimate Sources of Financing:



ISSN: 1112-4040 & EISSN: 2588-204X

رت م د: 1112-4040، رت م د إ: 2588-X204

تاريخ النشر: 2026-06-04

الصفحة: 301-281

السنة: 2026

العدد: 01

المجلد: 40

Date of Publication: 04-06-2026

pages: 281-301

Year: 2026

N°: 01

Volume: 40

The Role of Artificial Intelligence in Combating the Crime ----- . Nabila Ben Cheikh

In this case, financing comes from criminal activities such as drug trafficking, arms trafficking, etc. It also includes spending on websites that promote extremist ideology, hacking banking sites, and conducting illegal transfers to terrorist organization accounts.

Second requirement: Procedural Aspects in Preventing the Crime of Electronic Terrorist Financing

Given that this type of crime is relatively new in criminal procedure law, special procedural rules have been established, whether related to searches and evidence (**Branch One**) or to investigative and inquiry procedures (**Branch Two**).

Branch One: Search and Evidence in the Crime of Electronic Terrorist Financing

First: Search of Digital Evidence:

A digital search is defined as “a procedure that allows the use of electronic means to collect evidence stored or recorded electronically” (Al-Feel, 2012, p. 39) The search typically targets computers, automated service systems, and technical accessories. Precautionary measures are applied to stored data due to its susceptibility to disappearance, and electronic communications transmitted via email and private voice channels of service providers may be intercepted.

Suspected systems may extend to other connected systems, a common situation due to internal networks. Extending the search to systems not initially suspected presents significant challenges, primarily regarding the legality of such a procedure and its impact on informational privacy rights of the owners of the systems involved (Bayyumi, 2018, p. 14).

Second: Proof of Financing Crimes:

As the electronic financing of terrorist organizations is conducted via smart devices and digital networks, proving it is difficult because it leaves no physical traces. Service providers are obligated to disclose data and information that reach them, provided there is a judicial order to do so. They maintain electronic records of financial transactions conducted through digital networks, including information about both the sender and recipient and their geographical locations, which constitute essential elements of evidence for this crime.

Branch Two: Investigative and Inquiry Procedures:



ISSN: 1112-4040 & EISSN: 2588-204X

رت م د: 1112-4040، رت م د: 2588-X204

تاريخ النشر: 2026-06-04

الصفحة: 301-281

السنة: 2026

العدد: 01

المجلد: 40

Date of Publication: 04-06-2026

pages: 281-301

Year: 2026

N°: 01

Volume: 40

The Role of Artificial Intelligence in Combating the Crime -----, Nabila Ben Cheikh

The evidence-gathering phase is crucial as it seeks the perpetrator and the evidence that assists the public prosecution, investigating judge, and trial judge. This phase aims to collect as much information as possible about terrorist financing activities and then provide this information to the investigating authorities.

The investigating judge and public prosecution learn of terrorist financing activities only through reports prepared by the judicial police officer, and the prosecution will only press charges if sufficient evidence exists of the terrorist activity.

Given that investigating cyberterrorism requires special skills, investigators need to be proficient in digital systems and networks.

It is worth noting that the Algerian legislator enacted the Anti-Money Laundering and Terrorist Financing Law in 2005 under Law No. 05/01 dated 6 February 2005, defining terrorist financing in Article 3, which was later amended by Law No. 15/06 dated 25 February 2015.

Electronic financing emerged in Algerian legislation when the legislator issued Law No. 16/02 dated 19 June 2016 amending and supplementing the Penal Code, specifically Article 87 bis 11, which penalized the use of information and communication technologies to train for committing terrorist acts, and Article 87 bis 12, which penalized recruiting individuals for terrorist organizations using information and communication technologies.

Third requirement: The Role of International Organizations in Combating the Financing of Terrorist Groups

Terrorist financing is considered one of the risks threatening the international community, as it constitutes a fundamental pillar enabling terrorist groups and organizations to carry out and sustain their criminal activities. The United Nations has issued a series of resolutions aimed at halting any activity that may support terrorism (Al-'Adli, 2004, p. 287) (**Branch One**). In addition, a number of binding international conventions have been adopted to address the phenomenon of terrorist financing (**Branch Two**). International efforts have also demonstrated a commitment to combating terrorist financing by imposing oversight on cross-border bank transfers and preventing their use to fund terrorist organizations (**Branch Three**).

Branch One: International Efforts to Combat Electronic Terrorist Financing



ISSN: 1112-4040 & EISSN: 2588-204X

رت م د: 1112-4040، رت م د: 2588-X204

تاريخ النشر: 2026-06-04

الصفحة: 301-281

السنة: 2026

العدد: 01

المجلد: 40

Date of Publication: 04-06-2026

pages: 281-301

Year: 2026

N°: 01

Volume: 40

The Role of Artificial Intelligence in Combating the Crime -----, Nabila Ben Cheikh

First: International efforts to combat the financing of cyber-terrorism

Given the increasing crimes committed by cyber terrorism, the United Nations convened a convention in 2000 to combat the misuse of technology for terrorist purposes.

The UN also held the Twelfth United Nations Congress on Crime Prevention and Criminal Justice in 2010, which discussed the use of technology by terrorists and convened a meeting of a team of experts.

Since 2014, the Financial Action Task Force (FATF) has issued recommendations regarding the risks of crypto currencies and virtual assets, obliging states to establish legal frameworks to regulate and supervise Virtual Asset Service Providers (VASPs). FATF also conducts periodic assessments to determine states' compliance in combating electronic terrorist financing (Financial Action Task Force, 2015)

The role of international financial institutions, including the International Monetary Fund and the World Bank, is also notable, as they provide technical support to develop digital financial monitoring systems and assess cyber risk exposure.

Moreover, INTERPOL coordinates efforts to track terrorist networks online and supports the exchange of information among countries regarding suspicious electronic transactions.

Second: Regional Efforts to Confront Electronic Terrorist Financing

Combating electronic terrorist financing requires effective regional cooperation based on information sharing, updating legislation, and developing technical capabilities. Technology used by terrorists today can, if used intelligently and with tight regional coordination, become a powerful tool against them.

In 2017, the International Centre for Targeting Terrorist Financing (CITF) was established in Riyadh with the participation of Gulf Cooperation Council countries and the United States, aiming to track terrorist financial networks. Saudi Arabia has also developed anti-money laundering and counter-terrorist financing systems and launched financial awareness programs about the risks of electronic financing (International Center for Targeting Terrorist Finan, 2021)

Additionally, the United Arab Emirates established a Financial Intelligence Unit, imposed regulatory frameworks on crypto currency trading to limit its use in terrorist financing, while Bahrain, Qatar, and Kuwait strengthened cooperation with



ISSN: 1112-4040 & EISSN: 2588-204X

رت م د: 1112-4040، رت م د: 2588-X204

تاريخ النشر: 2026-06-04

الصفحة: 301-281

السنة: 2026

العدد: 01

المجلد: 40

Date of Publication: 04-06-2026

pages: 281-301

Year: 2026

N°: 01

Volume: 40

The Role of Artificial Intelligence in Combating the Crime ----- . Nabila Ben Cheikh

international banking institutions to develop systems for detecting suspicious transactions.

The GCC also established the Criminal Information Center to exchange data on suspicious accounts and financial activities and developed an Arab cyber security platform in collaboration with the International Telecommunication Union (ITU) to monitor digital terrorist attacks.

Regarding the European Union, the EU Cyber security Strategy was adopted in 2020, which includes combating electronic terrorist financing. An agreement was concluded between the EU and the United States to track financial transfers directed toward terrorist groups. The EU also launched the IRU initiative, which monitors digital content promoting terrorist financing online (Bures, 2010)

Moreover, the Horizon Europe program was established to fund scientific research projects aimed at developing artificial intelligence tools to detect patterns of illicit financing in cyberspace.

Conclusion:

Electronic financing of terrorism in the digital environment represents one of the most prominent modern forms of crime, due to rapid developments in information and communication technologies.

While artificial intelligence (AI) technologies have been applied in various aspects of daily life, their use by judicial authorities is justified in the field of crime prevention, especially since the criminal phenomenon itself has exploited these technologies and terrorists have used them to commit electronic financing crimes, particularly in countries that have achieved a significant level of technological advancement.

AI systems have also provided solutions to combat electronic terrorist financing and to detect early any transactions that may be considered fraudulent. Although security and banking oversight authorities have traditionally relied on human personnel and physical workforce, it has become clear that, with current technological advancements, many tasks and services can now be fully entrusted to digital systems.

Based on the foregoing, the following conclusions can be drawn:

— Terrorist organizations resort to using modern technical means for electronic financing of terrorism via the Internet.



ISSN: 1112-4040 & EISSN: 2588-204X

رت م د: 1112-4040، رت م د: 2588-X204

تاريخ النشر: 2026-06-04

الصفحة: 301-281

السنة: 2026

العدد: 01

المجلد: 40

Date of Publication: 04-06-2026

pages: 281-301

Year: 2026

N°: 01

Volume: 40

The Role of Artificial Intelligence in Combating the Crime -----, Nabila Ben Cheikh

— The Algerian Penal Code does not address electronic terrorist financing in the same manner as specific laws.

— After reviewing the procedural aspects of the crime of electronic financing of terrorist organizations from the perspective of investigation and enforcement, it is clear that this type of crime differs significantly in terms of follow-up and investigation procedures and requires training by experts in electronic means. Most countries have realized that without modern and technical tools, it is impossible to investigate and detect electronic financing of terrorist organizations, as this crime occurs in the digital environment where criminal traces can be quickly and easily concealed.

— Challenges in combating electronic terrorist financing through digital currencies remain and are still under continuous study in national legislative frameworks, especially concerning issues of proof.

Recommendations:

— It is essential to criminalize electronic financing of terrorist organizations through specific legislation that explicitly aligns with developments in this type of crime.

— All financial institutions should be subjected to new obligations to tighten control over terrorist organizations and prevent them from exploiting financial institutions for illicit money laundering operations.

— Banking secrecy should be reduced to prevent it from being used as a pretext to hinder the prosecution of terrorist organizations.

— Computer network security should be de

References List

▪ Al-'Adli, M. (2004). International Crime: A Comparative Study. Alexandria: Dar al-Fikr al-Jami'i.

▪ Al-'Amoush, A. (2006). The Future of Terrorism in the 21st Century. Riyadh: Research and Studies Center, Naif Arab Academy for Security Sciences.

▪ al-Faqi, A. (2012). Artificial Intelligence and Expert Systems. Dar al-Thaqafa for Publishing and Distribution.

▪ Al-Feel, A. (2012). Investigation Procedures, Evidence Collection, and Preliminary Investigation in Computer Crime. Dar al-Kutub wa al-Watha'iq al-'Ilmiyya.



ISSN: 1112-4040 & EISSN: 2588-204X

رت م د: 1112-4040، رت م د: 2588-X204

تاريخ النشر: 2026-06-04

الصفحة: 301-281

السنة: 2026

العدد: 01

المجلد: 40

Date of Publication: 04-06-2026

pages: 281-301

Year: 2026

N°: 01

Volume: 40

The Role of Artificial Intelligence in Combating the Crime -----, Nabila Ben Cheikh

- Bayyumi, A.-F. (2018). Combating Computer and Internet Crimes. Cairo: Dar al-Fikr al-Jami'i.
- Dahshan, Y. (2020). Criminal Responsibility for Artificial Intelligence Crimes. Journal of Sharia and Law, 34(82), 100-144.
- Faraj, A. (2016). Combating Cyberterrorism (Digital Terrorism) in the Gulf States under the GCC Anti-Terrorism Agreement. Cairo: Dar al-Kutub wa al-Dirasat al-'Arabiyya.
- Hamad, F. (2017). Combating Terrorism Before and After the September 11, 2001 Attacks (éd. 1st ed). Beirut: Halabi Legal Publications.
- Haymar, A.-K. (2013-2014). Interpol Organization. Master's Thesis, Faculty of Law and Political Science, Mohamed Khider University, Biskra.
- Khaz'al., S. (2022). International and National Confrontation of Terrorist Financing Crime: A Comparative Study. . Amman: Durub al-Ma'rifa Publishing and Distribution.
- Matar, I.-F. (2005). Terrorist Crime. Alexandria: Dar al-Jami'a al-Jadida.
- Moussa, A., & Bilal, A. (2019). Artificial Intelligence: A Revolution in Modern Technologies1 (éd. 1st ed). Egypt: Arab Group for Training and Publishing, Cairo.
- Rashed, A.-D. (2005). The United Nations and Terrorism Before and After 11 September. Cairo: Dar al-Nahda al-'Arabiyya.
- Suwaylim, M. (2018). Cybercrimes and Electronic Terrorism. Cairo: National Center for Legal Publications.
- 'Ali, A. (2024). Artificial Intelligence: Historical and Philosophical Roots and Legislative and Judicial Applications in the USA and EU Countries. UAE: Dar al-Kutub wa al-Dirasat al-'Arabiyya, Sharjah.
- Abu al-Nasr, M. (2020). Artificial Intelligence in Smart Organizations (éd. 1st ed.). Egypt: Arab Group for Training and Publishing, Cairo.
- Al-'Ubaidi, O. (2022). Contemporary Applications of Crimes Arising from Artificial Intelligence: A Legal Study from an International Law Perspective. (éd. 1st ed). Cairo.: Arab Center for Publishing and Distribution.
- Al-Deeb, A. (2023). Killer Autonomous Robots: Legal and Ethical Dimensions. Egypt: Dar al-Ahram for Publishing, Distribution, and Legal Editions.
- Al-Shukri, A. (2008). International Terrorism (éd. 1st ed). Jordan: Dar Usama Publishing and Distribution, Amman.



ISSN: 1112-4040 & EISSN: 2588-204X

رت م د: 1112-4040، رت م د: 2588-X204

تاريخ النشر: 2026-06-04

الصفحة: 301-281

السنة: 2026

العدد: 01

المجلد: 40

Date of Publication: 04-06-2026

pages: 281-301

Year: 2026

N°: 01

Volume: 40

The Role of Artificial Intelligence in Combating the Crime -----, Nabila Ben Cheikh

- Belbay, I. (2024). Artificial Intelligence in International Law¹ (éd. 1st ed.). Legal Book Foundation.
- Financial Action Task Force, (. (2015). Rapport on virtual currencies key definition and potential AML/CFT, Risks. Paris.
- Hudhaib, I. (2024). Objective Aspects of Using Artificial Intelligence in Crime Prevention. Cairo: Dar al-Nahda al-'Arabiyya.
- Ibrahim, M. (2024). Legislative Regulation of Artificial Intelligence Applications (éd. 1st ed). Cairo.: Mahmoud Center for Legal Book Distribution.
- International Center for Targeting Terrorist Finan, (. (2021). Annual Report on Electronic Terrorism Financing. Riyadh.
- Khalifa, M. (2005). Criminal Protection of Computer Data in Algerian and Comparative Law. Alexandria.: Dar al-Jami'a al-Jadida.
- Mahmoud, A. (2023). The Role of International Law in Combating Cyberterrorism: A Comparative Study¹ (éd. 1st ed). Hatrick Publishing and Distribution.
- EU's Fight Against Terrorist Finances: Internal ' .(2010) .Oldrich Bures
'Terrorism and Political Violence .Shortcomings and Unsuitable: External Models
438-419 '(03)22
- Omar, A. (2008). Contemporary Arabic Language Dictionary (éd. 1st ed, Vol. 01). Cairo: 'Alam al-Kutub.
- Yusuf, Y. (2011). International Internet Crimes (éd. 1st ed). Cairo: National Center for Legal Publications.