REVISTA SOCIO DEBATE

Núm. 6 (2026) | ISSN electrónico 2451-7763 | pp. [20-34]

Cyberterrorism Threats And International Mechanisms For Combating Them

Amenazas del ciberterrorismo y mecanismos internacionales para combatirlas

Bounif Abdelkader (Ph.D)

University of Sfax, Tunisia

aekamrawi@gmail.com

Received: 06.08.2026 Accepted: 08.09.2026 Publishing: 24.10.2026

Abstract:

Cyberspace, as a virtual digital domain, relies on computer systems, Internet networks, and stored electronic data connected to computers extending across the territories of all states. This has made cyberspace a fundamental basis for transactions in international relations. At the same time, digital criminal activities have emerged in several forms, including cyberwarfare and digital terrorism. Cyberterrorism is considered one of the principal factors threatening the continued existence of states and undermining efforts to preserve domestic national security. It increasingly affects states' internal systems economically, politically, and security-wise. International organisations have therefore devoted attention to cybersecurity and to means of protecting states' internal security from cyber threats that undermine their unity and survival. Relevant United Nations instruments include General Assembly document A/CONF.222/122 of 22 February 2015, concerning strengthened crime-prevention and criminal-justice responses to emerging forms of crime, including cybercrime and trafficking in cultural property; document CCPCJ/2013/2, issued during the session held from 25 to 28 February 2013; Security Council resolution 2354 (2017), adopting the international comprehensive framework to counter terrorist narratives; and resolution 2462 (2019), concerning the suppression of terrorist financing and the risks associated with modern financial technologies, crowdfunding, and virtual assets. This paper seeks to identify the international and domestic mechanisms capable of enabling Algeria to protect its security system and internal national unity against cybercrimes, cyber-organisations, and external electronic threats to which it may be exposed.

Keywords: Cyberterrorism; Cybersecurity; Cybercrime; International Security; Counterterrorism; Algerian Legislation.

Resumen

El ciberespacio es un entorno digital virtual sustentado en sistemas informáticos, redes de Internet y datos electrónicos almacenados en equipos interconectados en distintos Estados. Esta infraestructura se ha convertido en un medio fundamental para realizar transacciones en el ámbito de las relaciones internacionales. Paralelamente, han surgido diversas formas de actividad delictiva en el entorno digital, entre ellas la ciberguerra y el ciberterrorismo. El ciberterrorismo se considera una de las principales amenazas para la continuidad de los Estados y para sus esfuerzos por preservar la seguridad nacional. Su impacto en el funcionamiento interno de los Estados es cada vez mayor y se manifiesta en los ámbitos económico, político y de la seguridad. Ante esta situación, las organizaciones

internacionales han prestado especial atención a la ciberseguridad y a los mecanismos para proteger a los Estados frente a amenazas cibernéticas que pueden comprometer su seguridad interna, su unidad y su continuidad. Entre los instrumentos pertinentes de las Naciones Unidas figuran el documento A/CONF.222/122 de la Asamblea General, de 22 de febrero de 2015, relativo al fortalecimiento de las respuestas en materia de prevención del delito y justicia penal frente a nuevas formas de delincuencia, como la ciberdelincuencia y el tráfico de bienes culturales, y el documento CCPCJ/2013/2, emitido durante el período de sesiones celebrado del 25 al 28 de febrero de 2013. También se examinan la resolución 2354 (2017) del Consejo de Seguridad, por la que se adopta el marco internacional amplio para contrarrestar las narrativas terroristas, y la resolución 2462 (2019), relativa a la represión de la financiación del terrorismo y a los riesgos asociados con las nuevas tecnologías financieras, la financiación colectiva y los activos virtuales. Este artículo tiene por objeto identificar los mecanismos internacionales y nacionales que pueden permitir a Argelia proteger su sistema de seguridad y preservar su unidad nacional frente a la ciberdelincuencia, las organizaciones que operan en el ciberespacio y las amenazas cibernéticas procedentes del exterior.

Palabras clave — ciberterrorismo, ciberseguridad, ciberdelincuencia, seguridad internacional, lucha contra el terrorismo, legislación argelina.

Introduction :

Cyberattacks have become prominent only relatively recently, and they constitute one of the major contemporary challenges facing specialists in public international law, particularly with regard to determining their nature and constituent elements.

The challenge is compounded by the ambiguity surrounding cyberattacks and the absence of agreement on a specific definition. Legal scholars have nevertheless attempted to define the term. Some describe a cyberattack as conduct occurring in a virtual world based on the use of digital data and electronically operated communication technologies. The concept subsequently developed to include the achievement of direct military and security objectives through the penetration of sensitive websites.

Among the sources of cyberattacks against states are attacks originating from cyberterrorism, which has emerged in several countries in recent years as an evolutionary form of traditional terrorism. The concept of the unlawful use of force in international relations is no longer confined to the use of weapons of different kinds: even a single computer can threaten a state's survival, security, and territorial integrity.

Cyberterrorism has consequently become a major subject of concern for scholars and researchers in legal and political sciences. This paper seeks to identify the international and domestic mechanisms developed by Algeria to safeguard its continued existence, protect its security system and internal national unity, and defend against cybercrimes, cyber-organisations, and external electronic threats. It therefore raises the following question: How has cyberterrorism contributed to threatening the stability and security of states? The discussion is organised into three sections:

Section One: The concept of cyberterrorism.

Section Two: The impact of terrorist groups on the security and survival of states.

Section Three: The efforts of comparative legislation and the United Nations to combat cyberterrorism.

Section One: The Concept of Cyberterrorism:

Determining the nature of international terrorism has generated considerable debate in international relations. There is no definition of terrorism agreed upon by all states; however, a distinction is generally recognised between terrorism and legitimate resistance undertaken by liberation movements.

Cyberterrorism is a practical development of traditional terrorism, arising primarily from scientific progress and the emergence of technological means. Terrorism is no longer associated solely with physical harm; it also encompasses moral and psychological harm. Defining cyberterrorism therefore requires examining its meaning, distinguishing it from overlapping concepts, considering the position of international law, and applying these considerations to state cyberterrorism.

A discussion of cyberterrorism must begin by defining both terrorism and cyberterrorism and then identifying the objectives of cyberterrorism.

First: Definition of Terrorism

Legal scholars differ over the definition of terrorism because the term is broad and open to multiple interpretations. International efforts have also been made to define the phenomenon.

The Jurisprudential Definition of Terrorism

Dr Ismail Sabri Muqallid defines international terrorism as "terrorism that crosses the political borders of states, or terrorism that produces international reactions and repercussions whose impact may expand or contract depending on the circumstances." Dr Ahmad Bilal Ezz al-Din defines it as "a strategy of organised and continuous violence involving acts of killing, assassination, aircraft hijacking, hostage-taking, planting explosives, and similar acts, for the purpose of achieving political objectives." (Muqallid, n.d.; Ezz al-Din, n.d.)

The first definition does not encompass all forms of terrorism; rather, it focuses on terrorism that crosses state borders. International terrorist acts cannot, however, be linked exclusively to a state's territorial scope. The criterion for classifying an act as international terrorism should instead be the results or consequences of the act. Nor should the classification depend solely on international reactions, since actual international practice often relies on political interests in determining whether conduct constitutes international terrorism. The acts committed by Israel in the Palestinian territories, particularly in Gaza, are cited by some international-law scholars as terrorist acts under international law.

The second definition does not fully reflect developments in international society, particularly in the field of crime. Terrorist organisations now employ methods more dangerous than killing, assassination, and aircraft hijacking to threaten states' survival. These include cyberterrorist acts, also known in international legal scholarship as international electronic terrorism. Some states and terrorist organisations exploit state electronic systems to threaten their existence and security. As technological realities increasingly shape international relations, states are compelled to modernise their domestic and international administrative systems and rely on the Internet in their dealings. Consequently, penetrating a state's information systems may be sufficient to destroy its economy, institutional structure, and stability.

The Operational Definition of Terrorism:

Scholars have sought to formulate a practical definition of terrorism and generally agree that terrorist phenomena pose an imminent threat to international peace and security. Three approaches have emerged.

The first regards terrorism as a multidimensional social phenomenon in which psychological, social, cultural, historical, security, and political elements intersect. Because these elements are ambiguous, proponents of this approach consider it impossible to formulate a practical definition of terrorism.

The second approach considers terrorism definable solely as a material act committed by terrorists against the safety or security of citizens, facilities, or services associated with the state or individuals, irrespective of the motive. This

approach may, however, confuse terrorism with similar phenomena such as international war, international crime, civil war, extremism, and guerrilla warfare.

The third approach defines terrorism as an ideological doctrine. Under this view, an ideological belief or orientation must underlie the terrorist offence; terrorism is therefore linked to a political or doctrinal character.

Efforts by International and Regional Organisations to Define Terrorism:

International organisations have made substantial efforts to define terrorism, but these attempts have encountered difficulties that have prevented agreement on a uniform definition. Some attribute these difficulties to the complexity of terrorism and the diversity and contradiction of its forms and objectives. Others point to the practices of powerful states, which may invoke terrorism to conceal acts they themselves commit. Another difficulty concerns attempts by certain states to classify peoples' struggles for self-determination, including the use of force, as terrorist acts.

One of the earliest international legal attempts to define terrorism was made in 1937 in Article 1 of the Geneva Convention for the Prevention and Punishment of Terrorism. It defined terrorist acts as "criminal acts directed against a State and intended or calculated to create a state of terror in the minds of particular persons, or a group of persons, or the general public." (Geneva Convention for the Prevention and Punishment of Terrorism, 1937).

The Security Council has also described terrorism as criminal acts committed against civilians with the intention of causing death or serious bodily injury, or taking hostages, in order to spread terror among the public or compel a government or an international organisation to perform or refrain from performing an act. The definition also encompasses other acts constituting offences under international conventions relating to terrorism, which cannot be justified by political, philosophical, ideological, racial, or religious considerations. Although criticised for failing to cover new forms of terrorism such as cyberterrorism, this Security Council definition is regarded as binding on all states, including non-members of the United Nations, and represents an important development in defining international terrorism. (UNSC, 2004)

At the regional level, the 1998 Arab Convention for the Suppression of Terrorism, adopted by the League of Arab States, was the first Arab convention to include a definition of terrorism. Article 1(2) defines terrorism as any act of violence or threat thereof, whatever its motives or purposes, committed in furtherance of an individual or collective criminal plan and intended to terrorise people, harm them, or endanger their lives, security, or freedoms; damage the environment, public or private facilities or property; occupy or seize such facilities or property; or endanger national resources. (League of Arab States, 1998)

The 1999 Convention of the Organisation of African Unity on the Prevention and Combating of Terrorism defines a terrorist act in Article 1 as an act that violates the criminal laws of a State Party and endangers the life, physical integrity, or liberty of any person or group of persons, or causes serious injury or death; or causes damage to public or private property, the environment, cultural heritage, or national resources, where the intention is: (Organization of African Unity, 1999)

1. To intimidate, threaten, coerce, or compel a government, body, institution, or public service to undertake or refrain from undertaking an act, adopt or abandon a particular position, or act according to certain principles.

2. To disrupt an essential service or create a state of emergency.

3. To generate a general insurrection in a state.

Second: Definition of Cyberterrorism (Al-Fil, 2010; Denning, 2000):

Cyberterrorism differs from other forms of terrorism through its modern method of employing information resources and electronic means to overthrow systems and threaten states' information infrastructure. It thus combines elements

of cyberspace and terrorism, as well as a virtual world based on the symbolic and simulated representation of information. (Al-Fil, 2010; Denning, 2000)

Virtual terrorism has been described as the convergence of terrorism and virtual space. It refers to unlawful threats against computers, networks, and stored information, intended to intimidate or coerce governments or people in pursuit of political or social objectives. Such conduct may be sufficiently harmful to generate fear. Death, injury, explosions, and economic loss are among the possible consequences. The target audience may be classified into three categories: individuals, property, and governments. Collins also defines it as the deliberate misuse of a digital information system, network, or component in support of, or to facilitate, a terrorist campaign or act. (Al-Fil, 2010; Denning, 2000)

Cyberterrorism has also been defined as aggression, intimidation, or physical or moral threats directed by states, groups, or individuals against persons, their religion, honour, minds, or property, without lawful justification, through information resources and electronic means. It relies primarily on technical and scientific capabilities and exploits communication tools and information networks to harm individuals, groups, and states. By way of example, the Council of Europe estimated in the Convention on Cybercrime context that the cost of repairing damage caused by computer viruses amounted to approximately USD 12 billion annually. (Al-Fil, 2010; Denning, 2000)

Dorothy Denning defines cyberterrorism as a computer-based attack, or threat of attack, intended to intimidate or coerce governments or societies in pursuit of political, religious, or ideological objectives. The attack should be destructive or disruptive enough to generate fear and should be comparable to the physical acts of terrorism. (Al-Fil, 2010; Denning, 2000)

The United States Department of Defense defines it as a criminal act prepared through the use of computers and communication systems, resulting in violence, destruction, or the dissemination of fear among service recipients, thereby causing confusion and uncertainty. (Al-Fil, 2010; Denning, 2000)

The Federal Bureau of Investigation defines cyberterrorism as a deliberate, politically motivated attack against information systems, computer programmes, and stored data, carried out by various actors. (Al-Fil, 2010; Denning, 2000).

Cyberterrorism is also described as the intersection of cyberspace and terrorism. It refers to unlawful attacks, or threats to attack, computers, networks, and the information stored in them when undertaken to intimidate or coerce a government or its population in order to achieve political or social objectives. (Al-Fil, 2010; Denning, 2000).

In Algerian legislation, the concept of cyberterrorism reflects the evolution of criminal methods and the use of technology as a tool for carrying out terrorist acts. Under Article 87 bis 11, paragraph 4, of the Algerian Penal Code, the relevant conduct includes “the use of information and communication technologies for the purpose of committing terrorist acts.” (Al-Fil, 2010; Denning, 2000).

This provision indicates that cyberterrorist offences involve exploiting modern technologies, such as the Internet and social-media networks, to facilitate or carry out terrorist operations. Such acts may include: (Al-Fil, 2010; Denning, 2000).

• Incitement to terrorism through the dissemination of extremist ideas or the promotion of terrorist acts online. (Al-Fil, 2010; Denning, 2000).

• Electronic recruitment by attracting individuals or groups to join terrorist organisations. (Denning, 2000).

• Electronic terrorist financing through online channels to transfer or collect funds supporting terrorist activities. (Ahmad & Yunos, 2012).

• Cyberattacks, such as disrupting critical infrastructure or penetrating security systems. (Al-Fil, 2010).

The Algerian legislation thus reflects an awareness of the dangers of technology-related offences and establishes a legal framework for combating them. (Al-Fil, 2010).

Third: Objectives of Cyberterrorism (Algerian Penal Code, 2016):
Cyberterrorism seeks to achieve a range of unlawful objectives, the most important of which are:

• Spreading fear and terror among individuals, states, and peoples.

• Disrupting public order and information security and undermining public tranquillity.

• Endangering the safety and security of society.

• Damaging or destroying critical information infrastructure and harming communications and information-technology systems, as well as public and private funds and facilities.

Cyberterrorism also seeks to threaten and blackmail the public authorities of states and international organisations, take revenge on adversaries, collect funds, and seize property. (Attiya, 2014)

To this end, terrorists may use demographic statistical data selected from personal information that users provide online through website enquiries and surveys. This information can be used to identify individuals and solicit financial donations for legal persons acting as fronts for terrorist groups. The requests may be sent deceptively by email so that donors do not realise they are assisting a terrorist organisation. This method enables such groups to expand their membership and recruit additional operatives.

Section Two: The Impact of Terrorist Groups on the Security and Survival of States:
The danger posed by cyberterrorist groups lies in their ability to use information systems and networks to destroy the electronic infrastructure on which governments, public institutions, and major economic companies depend. There is a possibility that the infrastructure of information systems and networks could collapse worldwide, rather than only in targeted institutions, major companies, or individual states.

Cyberterrorism has become a threat to the entire world because digital weapons are easy to use. For example, the severing of the submarine cable connecting Europe and the Middle East at the end of January 2008, followed by the cutting of another cable near the coast of Dubai and the Gulf of Oman, caused losses to the telecommunications and electronic-transactions sectors estimated at hundreds of millions of dollars.

First: Forms of the Threat Posed by Cyberterrorism to States:
In carrying out coordinated criminal operations, cyberterrorism relies on computers, software, and information networks through which electronic data are transmitted. Because global societies are interconnected through technological information systems, satellites, and international communication networks, terrorist groups' criminal capabilities have increased through their use of these technologies.

The infrastructure required to develop electronic weapons may consist of a computer or an Internet-connected mobile phone, together with malicious software, spyware, and similar tools. Such weapons require specialised skills to produce but only simple, inconspicuous platforms for deployment: a desktop or laptop computer, a website or email account, a search engine, a social network, a virtual or physical server, or data clouds. These elements may be brought together in a computer serving as the launch device. Electronic weapons can be designed from anywhere and by anyone, including hackers, terrorist groups, or rival states.

Email, as a communication tool, helps different terrorist groups communicate and exchange information. Practical studies have shown that email played a significant role in exchanging plans and ideas among those responsible for many terrorist operations in recent years. Websites have likewise enabled terrorist groups to expand their activities substantially by using them to plan and coordinate operations intended to penetrate states' internal electronic systems.

The electronic penetration of state data takes place through the leakage of key data and codes associated with Internet programmes. It can be carried out from anywhere in the world; the intruder need not be physically present in the state whose websites have been penetrated. Geographical distance is therefore irrelevant to preventing cyber intrusions. A significant proportion of intrusions remain undetected because of the complexity of computer operating systems. Website destruction, meanwhile, involves unauthorised access to a primary or secondary Internet-connected access point through an automated system (PC–server) or a group of interconnected systems (intranet), with the aim of damaging the access point or the system. (Al-Hashimi, n.d.; Al-Fil, 2010)

These operations and attacks are supported in advance by specialised training in secret training camps established for this purpose. Such camps have a technical and electronic character and rely on covert training, planning, and execution. This has contributed to the increased danger cyberterrorism poses to the security and survival of states.

Second: Effects of Cyberterrorism on States:

Cyberterrorism generally directs various electronic weapons against systems connected to the cyberspace of the state concerned. These weapons are invisible and capable of causing widespread destruction to state systems without posing a direct physical threat to human life or infrastructure. Cyberattacks have accordingly been described as "acts carried out by certain groups with the aim of penetrating the computers and networks belonging to another state in order to cause serious damage or disrupt them." (Abd al-Sadiq, n.d.)

The principal effects of cyberterrorism on states include the following:

1. Threats to States' Economic Systems (Buhada, 2017):

The penetration of domestic banks and manipulation of states' electronic balances undermine economic stability. Terrorist groups may transfer funds by using credit-card data and stealing them, or by penetrating electronic systems used to transfer capital between international banks. (Abd al-Sadiq, n.d.)

A number of major companies and banks have suffered substantial economic losses as a result of cyberattacks. According to a study conducted by B2B International and Kaspersky Lab and announced on 15 April 2015, 25 per cent of companies in the Gulf region considered distributed denial-of-service (DDoS) attacks to be among the three greatest threats facing businesses in the region. As one of the common techniques used by cybercriminals to make money, the number and impact of these attacks have increased year after year, making user protection a priority for companies. The source text also refers to a date before 6 February 2015. (Al-Hashimi, n.d.)

Kaspersky, a leading information-security company, also reported that a group of hackers had taken control of accounts at international banks and stolen approximately one billion dollars. They used sophisticated techniques to access the accounts and exploited a vulnerability in banks' computer systems to copy account data in no more than 20 seconds, enabling them to transfer money at great speed. (Abd al-Sadiq, n.d.)

2. Threats to States' Political Systems (Abd al-Sadiq, n.d.):

Terrorist organisations seek to paralyse command, control, and communication systems; sever communication networks between units and central leadership; disable air-defence systems; or divert missiles from their paths. These actions threaten state security. Terrorist groups may also threaten prominent political figures with murder, threaten to blow up national facilities, or spread viruses to damage information networks and electronic systems. They may

penetrate the email accounts of heads of state and senior political figures, expose their secrets, access and spy on their information and data, monitor their correspondence, and exploit it in terrorist operations. They may also blackmail officials in order to compel them to perform acts the groups intend to bring about.

For example, in 2010 what became known as the "WikiLeaks storm" involved the use of the global Internet to leak documents containing highly confidential information exchanged between the US administration and its consulates around the world. In March 2014, the Ukrainian group CyberBerkut attacked NATO websites, disrupting them for several hours. The Kremlin also announced that hackers had launched a "violent" attack on the Russian presidential website and disrupted the website of the Central Bank of Russia. In August 2014, an inspector from the US cybercrime unit acknowledged that foreign hackers had penetrated computers belonging to the US nuclear regulatory authority at least twice during the preceding three years. More recently, The New York Times reported on 26 April 2015 that Russian hackers had accessed emails belonging to US President Barack Obama after penetrating the unclassified electronic network of the White House. They accessed the email archive of White House staff who communicated with Obama daily and were thereby able to read messages received by the President, posing a threat to US national security. The text also refers to Russian interference in the 2016 US elections, possibly the first instance in which a major power such as the United States experienced this type of interference targeting one of its most important sovereign institutions: its democratic electoral system, regarded as one of the most advanced in the world and a symbol of the strength and sophistication of the American nation. (Muhammadi, n.d.)

Third: Reasons Why Cyberterrorism Can Threaten States' Electronic Systems:

The destruction of states' principal electronic websites and systems through terrorist operations is attributable to several causes and vulnerabilities that have contributed to the increasing number of attacks and the development of their risks. Among the most important causes is the use of weak passwords to access state systems. States sometimes use numbers or letters that are easy to remember. Another cause is the failure to install adequate website-protection software or to update such software regularly, even though it is designed to issue alerts when an intrusion occurs. (Al-Fil, 2010)

Failure to update states' operating systems regularly may also lead to the discovery of further security vulnerabilities, which must then be remedied through software patches. Likewise, failure to back up files and folders stored on state computers increases the risk of losing important data on which the state relies in carrying out its domestic functions and its external relations with subjects of international law. The source text identifies 2002 as a year in which intrusions and destruction increased substantially, attributing this to the discovery of additional vulnerabilities in Internet servers and the spread of numerous viruses. (B2B International & Kaspersky Lab, 2015).

Section Three: Efforts by Comparative Legislation and the United Nations to Combat Cyberterrorism (Kaspersky Lab, n.d.):

As discussed above, cyberterrorism is one of the most prominent forms of modern crime and has imposed significant challenges on states. This has prompted numerous international and Arab legislatures to criminalise it and incorporate relevant provisions into their laws, whether in general penal codes or specialised cybercrime legislation.

First: Combating Cyberterrorism under Comparative Legislation (Ayman Hussein, n.d.; Buhada, 2017):

1. Western Legislation:

Australia: Section 1 of the Australian anti-terrorism legislation criminalises electronic terrorism and provides severe penalties intended to deter and confront threats posed by this type of crime.

United States: The Computer Fraud and Abuse Act (CFAA) criminalises electronic terrorism, particularly offences targeting the US government, such as disrupting government institutions, threatening public safety, and carrying out destructive activities. These offences are described as “Crimes Against the Government.” (Al-Fil, 2010)

France: The French Penal Code addresses electronic terrorist offences through Articles 323 and 421-1. It criminalises acts targeting the security of the state or individuals through digital means and imposes enhanced penalties.

2. Arab Legislation:

Jordan: Jordanian legislation criminalises electronic terrorism under the Anti-Terrorism Law. This is also reinforced by Article 10 of the Information Systems Crimes Law No. 30 of 2010, which contains clear provisions for punishing perpetrators of such offences.

Saudi Arabia: The Anti-Cyber Crime Law, issued by Royal Decree, criminalises various forms of electronic terrorism. Articles 3 and 5 provide deterrent penalties to protect national security against digital threats.

As for Algeria’s efforts to combat cyberterrorism, the country has faced major challenges because of terrorism, prompting it to take pioneering legal steps to criminalise this type of offence. With the significant development of information technology, new forms of terrorist threats have emerged, foremost among them cyberterrorism, which poses a global danger to international and domestic security.

In response, the Algerian legislature has worked to update legislation to keep pace with technological developments and cover offences associated with electronic terrorism. The most important legal provisions include:

• Article 87 bis of the Penal Code, which establishes the basis for defining and criminalising terrorist acts in comprehensive terms.

• Article 87 bis 11, paragraph 4, which focuses on the use of information and communication technologies to commit terrorist offences and highlights the danger of exploiting technology to strengthen terrorist activities.

• Article 394 bis 3, which addresses offences involving the use of technology in ways that affect public security, including electronic terrorism. (Jordan, 2010)

• Law No. 09-04, which is devoted to preventing and combating offences related to information and communication technologies, taking into account international obligations, including the Arab Convention on Combating Information Technology Offences. (Saudi Arabia, n.d.)

Through these legislative measures, Algeria has affirmed its determination to confront electronic terrorism as a contemporary threat and has sought to strengthen regional and international cooperation against a phenomenon that transcends traditional borders.

The Algerian state has also established several centres and bodies to combat cyberterrorism and reduce the country’s international and Arab ranking in terms of cyberattacks to which it is exposed. These bodies include:

1. The National Authority for the Prevention of Crimes Related to Information and Communication Technologies: established under Law No. 09-04 of 5 August 2009 on the prevention of and fight against offences related to information and communication technologies. The Authority works to activate international judicial and security cooperation, manage and coordinate preventive operations, and provide technical assistance to judicial and security authorities. It may also be tasked with conducting judicial expert examinations in cases involving attacks on information systems that threaten state institutions, national defence, or the strategic interests of the national economy.

2. Specialised criminal judicial bodies: established pursuant to Law No. 04-14 of 10 November 2004, amending and supplementing the Code of Criminal Procedure. They have jurisdiction over offences affecting automated data-processing systems under Articles 37, 329, and 40 of the Algerian Code of Criminal Procedure. They enjoy extended territorial jurisdiction pursuant to Executive Decree No. 06-348 of 5 January 2006. They may hear cases related to information and communication technologies committed abroad, even where the perpetrator is a foreign national, if the acts target state institutions or national defence, pursuant to Article 15 of Law No. 09-04.

3. The National Institute of Forensic Evidence and Criminology: it consists of 11 specialised divisions in different fields, all of which provide expertise, training, education, and technical assistance. Its computer and electronic division is responsible for processing, analysing, and presenting digital evidence that may assist the administration of justice, as well as providing technical assistance to investigators during inspections.

4. The General Directorate of National Security: it works to combat cybercrime from several perspectives, including public awareness. It undertakes prevention and awareness-raising activities by organising educational lessons at different school levels and participating in national meetings, seminars, and events intended to inform citizens about the dangers of cybercrime.

Second: Efforts of the United Nations and Its Specialised Agencies to Combat Cyberterrorism:

The United Nations and its specialised agencies have devoted attention to cyberterrorism because it has become a threat to the security and existence of states. Their work is reflected in the various resolutions and circulars they issue. This section considers the United Nations' efforts to combat cyberterrorism and the role of the International Telecommunication Union (ITU) as an example of a specialised agency working to combat electronic terrorism.

1. United Nations Efforts to Combat Cyberterrorism (Algeria, 2009):

States have sought to combat cyberterrorism under the auspices of the United Nations because of the danger it poses to their security and survival. Several international instruments have therefore been adopted, including the 1988 Vienna Convention, which encouraged states to conclude bilateral agreements against cyberterrorism. The Eighth United Nations Congress, held in Korea in 1990, subsequently considered the consequences of technological development and progress in relation to cybercrime and proposed encouraging international action against it. In its resolution on computer-related crime, the Congress urged participating states to intensify their efforts in several areas, including updating procedural laws and exchanging assistance in matters relating to cybercrime. (Algeria, 2004; Algeria, 2006)

The United Nations General Assembly has also adopted numerous resolutions reflecting growing international concern about the non-peaceful use of information and communication technologies. These include the General Assembly resolution of 19 December 2001 concerning the establishment of a legal basis for combating the misuse of information and communication technologies for criminal purposes. (Algerian National Institute of Forensic Evidence and Criminology, n.d.)

The General Assembly also adopted resolution 49 of 2012 at its sixty-seventh session on the use of information and communication technologies for development. It stressed that governments and companies should pay greater attention to cybersecurity, including countering threats arising from cybercrime, damage to the social and economic order, and threats to Internet security from spam, malicious software, computer hacking, distributed denial-of-service attacks, and other forms of attack. (Algerian General Directorate of National Security, n.d.)

In another resolution, the General Assembly emphasised the need for states to combine their efforts to prevent the misuse of technology for criminal or terrorist purposes. This represents another attempt to eliminate cyberterrorism, which has become a threat to states' survival.

The Security Council has also addressed the fight against digital terrorism through several resolutions. The most important include resolution 1373 of 28 September 2001, described in the source text as the first international resolution to address digital information terrorism. It established a special counter-terrorism committee composed of 15 international experts in the field of combating terrorism, including cyberterrorism. In 2004, resolution 1535 established the Counter-Terrorism Committee Executive Directorate. Resolution 1822 emphasised the need for cooperation to prevent terrorists from exploiting technology for terrorist purposes. Resolution 2255, adopted in 2015, expressed the Council's concern about the increasing use of technology by terrorists in their criminal activities.

In 2017, resolution 2395 also stressed the need to cooperate with the Executive Directorates to combat terrorists' use of the Internet and social-media platforms to promote their terrorist objectives. In 2019, the scope expanded to include terrorist financing: resolution 2462 required states to criminalise terrorist financing, drew attention to the risks associated with modern financial technologies, crowdfunding, and virtual assets, and called for public–private partnerships and compliance with Financial Action Task Force standards (United Nations Security Council [UNSC], 2019; Financial Action Task Force [FATF], 2012). However, this stricter approach raised concerns about its impact on humanitarian work, an issue addressed more decisively through resolution 2664 (UNSC, 2022). These resolutions are now complemented by the 2024 United Nations Convention against Cybercrime, which translates some of these approaches into treaty obligations concerning electronic evidence (United Nations General Assembly [UNGA], 2024), although it has not yet entered into force. Shared challenges remain: the absence of a universally agreed definition of terrorism, an implementation gap, and the need to balance security with human rights. These developments demonstrate the Council's continuing attention to cyberterrorism. They also illustrate the United Nations' efforts to address digital terrorism, which has emerged from traditional terrorism, through plans and strategies reflected in several resolutions, with the ultimate aim of maintaining international peace and security.

2. The Role of the International Telecommunication Union in Combating Cyberterrorism:

As a United Nations specialised agency concerned with information and communication technologies, the International Telecommunication Union (ITU) regards cybersecurity as one of its principal objectives. Its tasks include strengthening international cooperation in public wired and wireless telephone services, expanding their use, developing telecommunications capabilities, and allocating radio frequencies. The Union also issues recommendations and specialised technical studies on wireless communications and collects and disseminates information to build the capacities of Member States, particularly developing countries. Its work supports the coordination of national strategies and the protection of network infrastructure against risks through awareness-raising, self-assessment, capacity-building, expanded monitoring and warning systems, and incident-response capabilities for states and relevant stakeholders.

Information security has consequently become one of the general fields addressed by the Union, including digital terrorism. This is reflected in its various reports on information-security and technological standards in the digital environment.

In 2007, the ITU issued the Cybersecurity Guide for Developing Countries, which included a range of resources needed to achieve cybersecurity and prevent cyberattacks, such as the destruction or theft of sensitive state data, software cracking, electronic eavesdropping, and espionage involving state secrets. Such attacks often aim to threaten states' security and safety. (UNGA, 2001)

The guide identified a number of activities undertaken by the Union to combat cyber threats and spam, particularly digital terrorism threatening the survival and security of states. These activities are included in several instruments, among them: (UNGA, 2012)

• WTDC 2006 – E-strategies and ICT applications: this action plan aims to establish a common understanding among states of cyber-spam issues and the countermeasures that may be adopted against the danger of digital-terrorism attacks, and to reduce such threats through the exchange of successful national experiences. (UNGA, 2015)

• World Telecommunication Development Conference 2006 (WTDC-06), Resolution 45 – Mechanisms to enhance cooperation in cybersecurity, including combating spam. This resolution instructs the Telecommunication Development Bureau to organise meetings of Member States to discuss ways of strengthening cybersecurity.

• WTDC 2006, Annex 2 to Resolution 2, Study Group 1 of the Telecommunication Development Sector, Question 22 – Securing information and communication networks: best practices for building a culture of cybersecurity. This work focuses primarily on identifying best practices for establishing and operating monitoring, warning, incident-response, and recovery mechanisms that Member States may use to develop their national capacities in this area. (UNSC, 2017; UNSC, 2019; FATF, 2012; UNSC, 2022; UNGA, 2024)

• Resolution 130 (revised at Antalya, 2006) – Strengthening the Union's role in building confidence and security in the use of information and communication technologies. This resolution also seeks to enhance technological security through joint projects between states and development-sector groups working in the digital field, enabling the exchange of experience and information needed to prevent cyberattacks that threaten states.

At the regional conference on cybersecurity held in Qatar in 2008, all states were also called upon to establish and implement a national cybersecurity framework and protect critical information infrastructure. This was considered an initial plan for addressing the challenges arising from states' connection to information and communication technologies.

Conclusion (International Telecommunication Union [ITU], 2011):

This study has shown that cyberterrorism has become a concern threatening the survival of states through the various Internet-based attacks carried out by extremist groups. These attacks employ modern technological means, relying on both hardware and software to destroy states' electronic systems.

Scholars have not agreed on a clear definition of electronic terrorism. This may primarily result from their disagreement over the definition of traditional terrorism. The element on which there is agreement, however, is technology: a group may be considered cyberterrorist when it relies on planning and coordination through technological hardware and software to threaten and penetrate the internal systems of states and organisations. International law has not established a clear definition of traditional terrorism, let alone cyberterrorism, despite the many international resolutions issued in this area by the United Nations and other international organisations. (ITU, 2007)

Cyberterrorism seeks to achieve several strategic objectives, foremost among them spying on states' systems and seizing large sums of money from bank balances or credit cards in order to ensure the continuity of terrorist groups. Technological tools have reduced the burdens and costs of terrorist operations: a desktop or laptop computer and a set of software applications may be sufficient to threaten the security and safety of states.

The effects of electronic terrorism on state security and territorial integrity take the form of various political and economic threats capable of destroying some or part of the important digital data held by states. This is primarily attributable to weaknesses in the software on which states rely in performing their daily domestic and international functions. (ITU, 2006)

Algeria is also affected by cyber-theft and hacking operations to which it is exposed. This places the country in a difficult position between, on the one hand, the challenge of keeping pace with technological development, which has

become an unavoidable necessity, and, on the other, the negative consequences of that technology, reflected in the substantial losses resulting from electronic theft. For these reasons, the state has been concerned with establishing a number of bodies whose principal task is to combat electronic hacking. (ITU, 2006)

Finally, this research paper puts forward the following recommendations: (ITU, 2006)

1. The technical bodies responsible for protecting state systems against penetration should be activated. Strong passwords should also be adopted for digital systems, combining symbols, shapes, numbers, and letters in order to reduce electronic hacking. (ITU, 2006)

2. States should maintain backup copies of important files to ensure that they are not lost if the original copies are penetrated or destroyed. (ITU, 2008)

3. Legal disparities among states in this field should be reduced, and a unified international legal framework should be established within the United Nations system to confront and combat electronic terrorism through a multilateral international treaty. International cooperation in this field should also be strengthened.

4. The international resolutions adopted by global organisations and bodies should be effectively implemented to confront cyberterrorism. This could include establishing an international cyber police force tasked with responding to electronic hacking operations targeting states.

Editorial and Referencing Note

The Arabic source document contains 36 endnotes. The citations above have been inserted at the corresponding discussion points using APA-style author–date form where the source supplies an identifiable author and date. Where the source gives only a legal instrument, institutional document, or an incomplete reference, the citation identifies the issuing body or title and preserves the available date. Several notes use expressions such as “previous reference” and omit publication years or full bibliographic details; those details cannot be reconstructed without inventing information. The reference list below therefore records the bibliographic information recoverable from the source endnotes, and flags incomplete entries.

References:

Ahmad, R., & Yunos, Z. (2012). A dynamic cyber terrorism framework. International Journal of Computer Science and Information Security, 10(2), 149–158.

Al-Fil, Ali Adnan. (2010). Electronic terrorism. Al-Khaleej University Journal, Department of Law, Issue 2, University of Mosul, Iraq, p. 19. [The source also cites pp. 15 and 18 in later notes.]

Algeria. (2004). Law No. 04-14 of 10 November 2004, amending and supplementing the Code of Criminal Procedure.

Algeria. (2006). Executive Decree No. 06-348 of 5 January 2006.

Algeria. (2009). Law No. 09-04 of 5 August 2009 on the prevention of and fight against offences Algeria. (2016). Law No. 16-02 of 19 June 2016, amending and supplementing Law No. 66-156 (Penal Code), Official Gazette No. 37, 22 June 2016.

Ahmad, Ismail Sabri Muqallid. (n.d.).

Attiya, Aysar Muhammad. (2014). The role of modern mechanisms in reducing emerging crimes: Cyberterrorism and methods of combating it. Paper presented at the Conference on Emerging Crimes in Light of Regional and International Changes, Faculty of Strategic Sciences, Amman, Jordan, 2–4 September 2014, p. 9.

Abd al-Sadiq, Adel. (n.d.). Cyber-space weapons in light of international humanitarian law. Future Studies Unit Library, Alexandria, Egypt, pp. 55–56.

Abd al-Sadiq, Adel. (2015). Electronic terrorism in international conflict. Dar al-Kitab al-Hadith, Egypt.

Denning, D. (2000, August). Cyber terrorism. Global Dialogue, p. 10.

FATF. (2012). [Reference cited in the source as Financial Action Task Force standards.

Geneva Convention for the Prevention and Punishment of Terrorism. (1937). Article 1.

International Telecommunication Union. (2006). World Telecommunication Development Conference documents: WTDC-06 Resolution 45; Resolution 2, Annex 2, Study Group 1, Question 22; and Resolution 130 (Antalya revision).

International Telecommunication Union. (2007). Cybersecurity guide for developing countries (pp. 130–133).

International Telecommunication Union. (2008). Regional Conference on Cybersecurity, Qatar.

International Telecommunication Union. (2011, March). Report of the General Secretariat of the International Telecommunication Union. https://www.itu.int

Jordan. (2010). Information Systems Crimes Law No. 30 of 2010, Article 10.

Kaspersky Lab. (n.d.).

League of Arab States. (1998). Arab Convention for the Suppression of Terrorism. Article 1.

Muqallid, Ismail Sabri. (n.d.). [

Muhammadi, Saliha. (n.d.). Electronic terrorism and the national security of states: A new pattern and different threats. Algerian Journal of Security and Development, p. 67.

Organization of African Unity. (1999). Convention on the Prevention and Combating of Terrorism. Article 1.

Saudi Arabia. (n.d.). Anti-Cyber Crime Law. [Royal Decree number and date not supplied in the source].

UNGA. (2001, December 19).

UNGA. (2012). Resolution No. 49, 67th session, on the use of information and communication technologies for development.

UNGA. (2015, December 16). Resolution 125/70, 70th session.

UNGA. (2024). United Nations Convention against Cybercrime. [As referenced in the source text].

UNSC. (2004, October 8). Resolution 1566, 5053rd meeting.

UNSC. (2017). Resolution 2395.

UNSC. (2019). Resolution 2462.

UNSC. (2022). Resolution 2664.

Ahmad Bilal Ezz al-Din. (n.d.).

Al-Azzawi, Hussein. (n.d.). The position of international law on terrorism and armed resistance. Dar al-Hamid for Publishing and Distribution, Amman, Jordan, p. 29.

Al-Hashimi, Rafid Ayadah. (n.d.). Electronic terrorism. E-book, https://www.mizandz.com/2017/11/pdf.html. [Publication details not supplied].

Ayman Hussein. (n.d.). Electronic terrorism: The most dangerous battle of space wars. Al-Watan. http://alwatan.com/details/166324.

B2B International, & Kaspersky Lab. (2015, April 15).

Buhada, Sarah. (2017). The impact of electronic terrorism on the security and stability of states. National School of Political Science, Algeria

Jumah al-Yaqout, Yusuf Mulla. (2010). Terrorism (pp. 18–22).