
The crime of digital promotion of terrorism through digital platforms and new media: a comparative study of Jordanian and Emirati laws

Ashraf Fathi Al-Rai

Digital Law Department,
College of Humanities,
Midocean University,
P.O. Box 51124, Fujairah, UAE
ORCID: 0009-0009-8480-9686
Email: ashrafalrai@midocean.km.edu
Email: ashrafraie@gmail.com

Nayel Musa AlOmran*

Department of Legal Studies,
Zayed University,
P.O. Box 19282, Abu Dhabi, UAE
Email: drnayel0@gmail.com
*Corresponding author

Mohamed Abdul Jail Al Ansari

2024, Abu Dhabi, UAE
Email: Al_ansari_m@yahoo.com

Abstract: This study addresses the crime of promoting terrorist acts through digital platforms, its dangers, and the legislative gaps in this context within the Jordanian Cybercrime Law No. 17 of 2023, comparing it with the corresponding legislative provisions in UAE. The problem at the core of this study lies in the insufficiency of the Jordanian Cybercrime Law to effectively address the crime of promoting terrorist acts through digital platforms, social media, new media, and smart applications, with a clear oversight despite its importance and necessity. The study concludes with several results and recommendations, which will be summarised here. Firstly, technical infrastructure issues: The technical infrastructure continues to face significant issues that allow terrorists to infiltrate, along with insufficient international cooperation between Jordan and other countries to address advanced electronic threats and ensure effective digital security. The study concludes with several recommendations, the most prominent being the need to add a specific provision to the Jordanian Cybercrime Law No. 17 of 2023 to penalise this crime.

Keywords: crime of digital; promotion; terrorism; digital platforms; new media.

Reference to this paper should be made as follows: Al-Rai, A.F., AlOmran, N.M. and Al Ansari, M.A.J. (2024) ‘The crime of digital promotion of terrorism through digital platforms and new media: a comparative study of Jordanian and Emirati laws’, *Int. J. Electronic Governance*, Vol. 16, No. 4, pp.453–467.

Biographical notes: Ashraf Fathi Al-Rai is an Accomplished Editor, legal researcher, and writer with over 21 years of experience. He holds a PhD of Public Law with a specialisation of Criminal Law, alongside dual Master’s degrees in Criminal Law and Cybercrime, and Media and Journalism. As the first legal expert in Jordan to combine expertise in both criminal law and media studies, he has established himself as a leading authority in media laws, legislation, and international conventions. He brings substantial expertise in legal research, text development, and consultation, with a deep understanding of legal frameworks and documents. His academic and professional journey includes authoring key references in law and human rights, along with numerous impactful research papers. He is currently an Assistant Professor at Midocean University, where his contributions enrich the academic community.

Nayel Musa AlOmran is currently an Associate Professor of Constitutional and Administrative Law in Department of Legal Studies at Zayed University, UAE. Previously, he worked at the College of Law, Al Ain University, as an Assistant Professor for four years. In addition, he worked at the Department of Management, University of Malaya, Malaysia, for three years as an Assistant Professor. His experience teaching undergraduate and graduate courses are in constitutional law, administrative law, business law and ethics, and many other legal courses. As a researcher, he has an excellent track record of publishing in highly qualified and Widely-read peer-reviewed international journals. He has many high-ranking, peer-reviewed journal publications (Scopus). He has more than 40 publications in high-ranking journals.

Mohamed Abdul Jail Al Ansari is a Colonel at the UAE Ministry of Interior and was the Director General of Civil Defense in Abu Dhabi, and Lecturer at Several Universities. He holds PhD of Law and has 30 years of experience in security, disaster management, and rescue operations. He has held various local and international positions, including Regional President of the International Search and Rescue Advisory Group. He is internationally accredited in arbitration, crisis management, and disaster response, and serves as a certified consultant for cases of an international nature.

1 Introduction

The 20th century witnessed a significant spread of terrorist crimes worldwide, which subsequently had a negative impact on international peace and security. However, the focus on combating terrorism became more pronounced following the September 11 attacks, which involved the destruction of the World Trade Center towers in New York, USA, resulting in over 3000 civilian casualties (Al-Dakhil, 2002, p.17). The dangers of promoting these criminal acts have intensified in recent years, particularly with the proliferation of digital platforms, social media, new media, artificial intelligence systems, cloud computing, and smart applications. These technologies provide a fertile environment for the easy exchange of information and data, effectively turning the world into a global village. Many countries have recognised these risks, prompting them to join

numerous international agreements aimed at combating international terrorism on one hand, and amending their domestic laws to prevent the promotion of terrorist acts on the other. This has included the introduction of specific provisions in cybercrime laws that specifically penalise the promotion of terrorism (Al-Daribi, 2012, p.40). The risks associated with the spread of terrorist groups and the promotion of terrorist acts have indeed driven the international community to adopt several agreements aimed at combating any promotional ideas related to terrorism. Among these are the United Nations Global Counter-Terrorism Strategy of 2006, as well as other treaties and agreements that predate the September 11 attacks, such as the 1988 Arab Convention on the Suppression of Terrorism, the GCC Convention on Combating Terrorism, and the 1999 International Convention for the Suppression of the Financing of Terrorism in New York, among many others that combat terrorism or related activities such as money laundering, drug trafficking, and the trade in psychotropic substances.

In 2010, the Council of Arab Interior Ministers adopted the Arab Convention on Combating Information Technology Crimes, which aims to unify Arab efforts in combating these crimes and to strengthen judicial and security cooperation among Arab countries. The convention covers a wide range of crimes, including the promotion of terrorist acts. It was ratified by both Jordan and the UAE and includes provisions for facilitating international cooperation, information exchange, and extradition of criminals, while also establishing a mechanism for coordination among member states. The convention emphasised the need for continued efforts to review national legislation and to enhance security and judicial capacities.

This convention represents an important step towards enhancing Arab cooperation in combating information technology crimes. However, achieving its objectives requires intensifying efforts and coordinating actions among member states. Therefore, the state parties should work on updating their national legislations, strengthening their security and judicial capacities, and raising awareness of the importance of combating information technology crimes within Arab societies. Additionally, they must exchange expertise and knowledge and enhance technical and technological cooperation to ensure the effective and efficient implementation of the convention, thereby contributing to strengthening digital security and protecting citizens' rights online (Khidel and Casey, 2021, pp.373–375).

Given Jordan's sensitive geographical location, connecting several countries experiencing armed conflicts, such as Syria, Iraq, and Lebanon. with the Gulf states – witnessing massive economic activities and significant commercial development – terrorist groups may attempt to infiltrate and spread their disruptive ideologies. This situation necessitates the enactment of clear legal provisions criminalising the promotion of terrorist acts through social media and smart electronic systems, which have become widely prevalent in Arab societies in general, and in Jordanian society in particular.

Numerous studies have shown a close correlation between the growing use of the internet, rising unemployment rates among youth, and the increased spread of terrorist ideas online. The incidence of terrorist acts committed via the internet has also risen in countries neighbouring Jordan, particularly Syria and Iraq. Official figures from the Syrian Observatory for Human Rights indicate that 257 people were killed in July 2024 alone, a very high number (Syrian Observatory for Human Rights, 2024, pp.1–3). Additionally, the terrorist organisation ISIS's operations in 2023 claimed the lives of 700

people in Syria (*Al-Hurrah Channel, ISIS in 2023: Operations Claiming 700 Lives in Syria*).

Jordan, too, has suffered from terrorism, notably in 2005 with the bombings of three hotels in the Jordanian capital, Amman, known as the ‘Amman Black Wednesday’ bombings, which resulted in more than 60 casualties and over 200 injured. Furthermore, the Jordanian pilot Muath Al-Kasasbeh was burned alive by ISIS after his plane crashed in 2015, and Jordanian officer Rashid Al-Ziyoud was martyred after raiding a terrorist hideout in one of Jordan’s provinces (*Jordan News Agency “Petra”, On the 14th Anniversary of the Amman Bombings: Jordan Adopts Comprehensive Strategies to Combat Terrorism*).

These incidents highlight the imminent and real danger posed to the world, emphasising the necessity of addressing this menace, whose negative impacts are increasingly exacerbated by the proliferation of smart applications, social media, new media, and international communication mechanisms through artificial intelligence technologies and smart media that have become prominent in recent years, as mentioned.

All these dangers underscore the need for stringent legal provisions addressing the promotion of terrorist activities, whether through Jordan’s Anti-Money Laundering and Counter-Terrorist Financing Law No. 20 of 2021 and its amendments, or through the Jordanian Cybercrime Law No 17 of 2023. Addressing this crime requires a clear understanding of the meaning of terrorist crimes, their spread, promotion, and connection to other crimes, especially since the world today is a global village where movement is easy, and the promotion of terrorist ideas is even easier.

Therefore, this study was conducted to thoroughly examine the legal definition of the crime of promoting terrorism, its regulation in the Jordanian Cybercrime Law, and the adequacy of its provisions in addressing this crime compared to the Emirati legislation, which is considered one of the most advanced in the Arab world, particularly in the field of combating cybercrimes.

2 The concept of terrorism promotion and its impacts

Promotion, in commercial terms, is defined as “an activity involving a persuasive communication process” (Moualla, 2008, p.1). Generally, promotion involves contacting someone to persuade them to adopt a specific idea product or method in their behaviour, which can be done either directly or indirectly.

However, there is no clear and specific legal definition of terrorism yet. International organisations have not agreed on a definitive definition of terrorism, despite its long-standing impact, except for the definition provided in the Arab Convention on the Suppression of Terrorism of 1988. This is due to the notable evolution in the methods used by terrorists especially with technological, and technical advancements.

The Petit Robert Dictionary defines terrorism as “the organised use of exceptional means of violence to achieve a political goal, such as seizing power, maintaining it, or exercising it, particularly through acts of violence that include individual or collective attacks or sabotage carried out by a political organisation to influence the public and create an unsafe environment” (Le Petit, 1993).

Terrorism can be defined as “a serious criminal act that causes psychological, physical, and financial harm, aiming to intimidate civilians and instil fear in them, or to

force government authorities or international institutions to act or refrain from acting under the threat of committing internationally prohibited criminal acts”.

Thus, terrorism involves the deliberate use of violence or threats by some states or by groups supported by certain states to achieve political objectives through unlawful actions, targeting to create a state of panic in society.

Karl Mannheim defines extremism as a condition that arises in stable societies when a particular class or group monopolises the right to guide, educate, and interpret social and natural phenomena. The existence and continuity of this class depend on two social factors: first, its ability to organise itself as a group, which grants it power and influence, leading to the formation of closed patterns of thought often derived from a particular doctrine to interpret existence and knowledge; and second, the isolation of this thought from the ongoing struggles of daily life (Mannheim, 1991, p.54).

Extremism can also be defined as “an excessive attachment to a particular doctrine or idea, where this belief or thought completely dominates the extremist’s life, with a significant focus on promoting this doctrine or idea and a firm belief in its correctness, while rejecting and ignoring other ideas”. Referring to the Jordanian Anti-Money Laundering and Terrorism Financing Law No, 20 of 2021. It does not provide a clear and specific definition of terrorism.

Instead, it only specifies in Article 4 the acts classified as terrorist acts, which states that. A person is considered to commit a terrorism financing crime if they.

- 1 Directly or indirectly, knowingly provide or collect funds from either legal or illegal sources with the knowledge that these funds will be used, wholly or partially, to commit a terrorist act or by a terrorist individual or organisation.
- 2 Deliberately participates in committing a terrorism financing crime with a group of people or supports them in committing it.
- 3 Funds the travel of individuals to countries other than their country of residence or nationality for the purpose of committing, planning, preparing, participating in, or facilitating terrorist acts, or receiving training for them.
- 4 Contributes to committing any of the terrorism financing crimes mentioned in this paragraph or organises or directs others to commit them. This will be discussed in detail in three sections.

2.1 Definition of electronic promotion of terrorism

The Jordanian legislator has not provided a clear definition of terrorism, which can be attributed to the evolving nature of this phenomenon, particularly considering the rapid technological advancements we are witnessing today. Similarly, the UAE legislator has enacted Federal Law No. 7 of 2014 on Combating Terrorism Crimes, which includes various definitions of acts and crimes committed for the purpose of carrying out terrorist activities. This is comparable to the Jordanian Anti-Money Laundering and Terrorism Financing Law No. 20 of 2021, as both laws address the connections between the financing of terrorism and the legal measures taken to combat it.

The Jordanian and UAE legislators have done well in this regard due to the evolving nature of terrorist acts, which cannot be fully encompassed. Neither the Jordanian nor the UAE legislator has defined the crime of electronic promotion of terrorism. However, there have been doctrinal attempts to define it. Some legal scholars argue that “promotion

of terrorism means that a certain party conveys information to another party using specific means to incite them to commit acts criminalised by law, aimed at terrorising and destroying people morally, psychologically, physically, and materially”.

Before defining the crime of electronic promotion of terrorism, it is essential to highlight the importance of digital platforms today. Their significance has increased with the proliferation of digital platforms, social media, and websites, which now represent a new form of media through which individuals can express their inner thoughts and beliefs with simplicity and ease. These platforms have thus become ‘open forums’ (Al-Rai, 2024, p.53).

Websites and digital platforms have spread tremendously in Jordan since 2004, with the emergence of numerous websites and digital platforms that were not subject to any form of regulation or to the provisions of the Press and Publications Law. This situation continued until the decision of the Jordanian Court of Cassation in 2010, which subjected all websites to the provisions of the Jordanian Press and Publications Law. The court ruled that “websites are to be considered publications according to the definition of publication set forth in the Jordanian Press and Publications Law and are subject to its provisions, and that websites fall within the definition of publication as defined in Article 2 of the Press and Publications Law, which states that it is ‘any means of publishing in which meanings, words, or ideas are recorded in any manner’”.

It contributes to analysing and interpreting the events and challenges facing the state, providing accurate and reliable reports on terrorist activities, criminal movements, warning of potential security threats, and disseminating news and information related to national security, public safety, civil defense, emergency preparedness, and guidance on dealing with emergency incidents (Al-Rai, 2024, p.51).

Digital promotion of terrorism can be defined as “all digital activities targeting the use of violence and intimidation, especially for political purposes, regardless of the specific objectives”, according to the Oxford Advanced Learner’s Dictionary (1974) (Hornby et al., 1974).

Electronic promotion of terrorism can be defined through digital platforms, social media, mobile applications, websites, or any electronic means as “actions by an individual, entity, organisation, or group to persuade another party, whether an individual or group, to commit criminal acts aimed at terrorising, destroying morally, psychologically, or physically, facilitating or funding terrorist acts, planning or preparing for them, receiving training, or engaging in any actions that could achieve their results and impacts”.

It is worth noting that Article 4 of the Jordanian Anti-Money Laundering and Terrorism Financing Law No. (20 of 2021) considers the attempt to commit terrorist acts as terrorism and equates it with the complete crime. This reflects the legislator’s recognition of the seriousness of this crime and its catastrophic effects on society and individuals, like what the UAE legislator has stipulated in several papers of Federal Law No. (7 of 2014) on Combating Terrorism Crimes. The UAE law penalises threats to commit a terrorist crime in Article 18, planning or attempting to commit a terrorist crime in Article 19, and incitement to commit a terrorist crime in Article 20.

Moreover, Article 34 explicitly addresses the crime of promoting terrorist acts, stating.

Anyone who promotes or endorses by word, writing, or any other means any terrorist organisation, individual, or crime, with knowledge of this, shall be punished with temporary imprisonment for a term not exceeding 10 years.

Anyone who:

- 1 Possesses personally or through intermediaries any documents, publications, or recordings of any kind promoting or endorsing a terrorist organisation, individual, or crime, if they are intended for distribution or to be viewed by others with knowledge of this, shall be punished with temporary imprisonment for a term not exceeding 10 years.
- 2 Possesses or acquires any means of printing, recording, or publicising used or prepared for use, even temporarily, for printing, recording, broadcasting, or publishing the materials with knowledge of this, shall be punished similarly.

The Jordanian Anti-Money Laundering and Terrorism Financing Law No.(20 of 2021) lacks a clear provision addressing the promotion of terrorist acts, which is a legislative gap that the researcher recommends addressing by amending Article 4 to include it.

2.2 Negative impacts of cyberterrorism

Terrorist organisations typically resort to organised violence and seek to propagate it through various means and methods. They even perpetrate terrorism against their own members who violate the directives of their leaders, who are terrorists and criminals posing significant threats to national security. The severe danger associated with terrorist crimes necessitates the enhancement of international cooperation, as evidenced by the Arab Convention on the Suppression of Terrorism of 1998 (Kamel, 2014, p.84).

The negative impacts of cyberterrorism extend beyond its direct effects on individuals and groups, reaching deeper and broader implications that directly affect national security, social stability, and have repercussions on the economy and international relations. These adverse effects have been exacerbated by the widespread proliferation of the internet, particularly in recent years (Conway, 2016, p.79).

Reports indicate that Western countries previously believed that social media usage was limited in Arab countries. However, in (2011) they realised that social media platforms were growing significantly in these regions. The Western world was surprised to find that terrorist organisations were using Twitter to raise funds (Conway, 2016, p.80).

The negative impacts of promoting terrorism through digital platforms are as follows:

- 1 *Increased fear and insecurity*: This involves creating a constant state of fear and psychological instability among individuals in society, which heightens social isolation, further exacerbated by poverty and economic collapse. This is evident in some Arab countries such as Syria, Yemen, and Iraq, which have suffered and continue to suffer from the spread of terrorist organisations (Akhter-Khan et al., 2024, p.7).
- 2 *Social disruption and escalation of ethnic or religious conflicts*: This can lead to a state of chaos and instability that might result in civil wars or the collapse of state institutions.
- 3 *Damage to the national economy*: Terrorism undermines confidence in the national economy. Investors often avoid 'unstable' environments, leading to a decline in both foreign and domestic investments. For instance, the Global Terrorism Index indicates a high level of threat from terrorism in countries such as Syria (7.89/10), Iraq

(7.08/10), and Afghanistan (7.83/10) (Institute for Economics and Peace, 2023). In contrast, the UAE is considered a completely safe country, along with Saudi Arabia, Qatar, and Jordan.

- 4 *Legal and security challenges*: Cyberterrorism poses significant challenges to specialised agencies by intensifying efforts and draining resources to track terrorist content. AS this type of crime transcends geographical boundaries and requires international coordination.
- 5 *Harm to the state's global image*: Countries experiencing high levels of terrorist activity may face political and economic sanctions from the international community, affecting their diplomatic and trade relations with other nations, increasing their isolation, and weakening their ability to engage in global cooperation.

These negative impacts are accompanied by numerous challenges faced by countries in combating the spread of cyberterrorism through the internet or digital systems. These include the international nature of digital systems (Boulainin, 2013) the diversity of terrorist languages and cultures, and their methods of communication, which require a deep understanding of their trends through digital tracking. Additionally, artificial intelligence used to track terrorists may often fail to provide accurate information (Al-Adwan, 2021, p.160).

It is essential to emphasise that terrorism should not be associated with any religion, civilisation, or culture. There is also a need to address the conditions that lead to the spread of terrorist and criminal activities, uphold the rule of law, combat oppression and violations of freedoms, and enhance social and economic conditions. Effective measures should be taken to combat terrorism promotion through the internet, digital systems, social media, and new media (Abouahmed et al., 2024, pp.195–202). This will be discussed in detail in Section 3 of this study.

2.3 Challenges faced by countries in combating the spread of cyberterrorism

With the proliferation of digital systems and the ease of global connectivity, the promotion of terrorist activities online has become one of the most significant challenges facing many societies and nations (AlOmran and Al-Qassaymeh, 2023, pp.1–9). This is particularly true with the widespread interaction through social media and digital platforms, which terrorist organisations now use to disseminate their ideas and organise their members in more sophisticated, effective, and clandestine ways. This poses a threat to national security and challenges legal principles within societies.

Addressing terrorist crimes is inherently complex, requiring a balance between protecting national security and ensuring respect for individual rights. Countries face numerous challenges in combating cyberterrorism, including technological, legislative, cultural, and economic obstacles.

These challenges include:

- 1 *Advanced technologies*: One of the primary obstacles is the use of sophisticated technologies by terrorist groups, such as encryption, to transmit their messages and conceal their identities. These technologies facilitate their movement and reach their targets with relative ease.

- 2 *Balancing free expression and digital privacy*: Security measures sometimes lead to violations of free expression and digital privacy, thus infringing on individual freedoms guaranteed by constitutions (Al-Rai, 2024, p.38). For example, Jordanian law explicitly addresses this issue, stipulating that privacy may not be breached or communications intercepted except in accordance with legal provisions.
- 3 *Cross-border challenges*: The digital realm transcends national boundaries, making international coordination essential yet complicated due to differing laws and the lack of a unified application framework. Additionally, terrorist organisations operate across languages and cultures, complicating the monitoring of all relevant content.
- 4 *Weak coordination between governments and internet platforms*: Coordinating efforts between governments and private internet platforms is complex due to differing priorities and approaches.
- 5 *Failure of Technological Systems to Track Criminals*: Artificial intelligence systems often provide inaccurate information, posing a challenge for further development and reliance on these technologies to address and track terrorist crimes (Al-Rai and AlOmran, 2024, pp.246–262).

Statistics show that online promotion of terrorism is a growing phenomenon, with promotional activities increasing by an estimated 80% between 2015 and 2020. There are approximately 30,000 accounts promoting extremism on Platform X (formerly Twitter). Additionally, 70% of terrorists use social media for recruitment purposes, highlighting the need for intensified efforts to monitor and dismantle terrorist networks (Wakeford and Smith, 2020).

Furthermore, reports indicate that 60% of recently identified extremist content was protected by complex encryption techniques, adding a layer of difficulty to monitoring and analysis. This underscores the need for enhanced global efforts to combat online terrorism, potentially reducing its threat by 50% (Wakeford and Smith, 2020).

The study recommends developing robust technological infrastructure, reassessing the flexibility of Jordan's Cybercrime Law, and enhancing international cooperation between Jordan and other countries to address advanced cyber threats and ensure effective digital security. This will be achieved through a sound legal framework for combating this type of crime, which will be discussed in detail in Section 2 of this study.

3 Legal regulation of cyberterrorism promotion

Cybercrime is notably characterised by its potential to occur in one country while its effects manifest in another, and it can occur at one time while its consequences are realised at a different time. This is particularly relevant for organised criminal gangs operating across multiple countries. Consequently, the international community has recognised the importance of combating such crimes due to their global negative impact and the potential for their use by terrorist organisations to fund international terrorism and other serious crimes threatening societies (Al-Rai, 2024, p.35).

In this context, cyberterrorism promotion emerges as one of the most dangerous forms of cybercrime due to its direct negative impact on national security and social stability. The Jordanian Penal Code has addressed this by enacting the Jordanian Anti-Money Laundering and Terrorism Financing Law No. 20 of 2021 and its

amendments, which aim to combat terrorist crimes. The law includes various preventive measures, including personal precautionary measures provided in the Penal Code, which may be imposed for certain crimes. These measures include police surveillance, deprivation of rights and privileges, residence restrictions, and prohibition from visiting certain places or practicing specific professions (Al-Dhayeb, 2019, p.70).

Similarly, the UAE legislator has clearly and systematically regulated the crime of promoting terrorism, criminalising such acts through various statutes. The UAE has been more specific regarding the promotion of terrorism via electronic systems, digital platforms, or social media. This is detailed in Article 21 of Federal Decree-Law No. (34) of 2021 concerning Combatting Rumors and Cybercrimes (Said, 2020, p.200). This chapter will discuss the Legal Regulation of Cyberterrorism Promotion in Jordanian Cybercrime Law: This section will explore how Jordanian legislation addresses the crime of cyberterrorism promotion, focusing on its legal framework and applicable provisions, Legal Regulation of Cyberterrorism Promotion in UAE Cybercrime Law: This section will examine how UAE legislation specifically tackles the promotion of terrorism through electronic means, highlighting key legal provisions and enforcement mechanisms, and Legislative Solutions to Combat Cyberterrorism Promotion: This section will propose legislative solutions and recommendations to enhance the effectiveness of legal frameworks in combating the promotion of terrorism via digital platforms.

3.1 Legal regulation of cyberterrorism promotion in Jordanian cybercrime law

The Jordanian Cybercrime Law does not explicitly address the crime of cyberterrorism promotion. Instead, it addresses related offenses under Article 17, which penalises “anyone who intentionally uses the information network, information technology, information systems, websites, or social media platforms to disseminate content that incites discord or sectarianism, targets social peace, promotes hatred, advocates violence, or justifies or disparages religions, with imprisonment from one to three years or a fine of not less than 5000 Jordanian Dinars and not exceeding 20,000 Jordanian Dinars, or both”.

This text indicates that the Jordanian legislator did not specifically mention calls to commit terrorist acts. However, Article 4 of the Jordanian Anti-Money Laundering and Terrorism Financing Law No. 20 of 2021 and its amendments defines acts considered as terrorism. It states that: “A person is considered to commit the crime of terrorism financing if they:

- 1 Directly or indirectly provide or collect funds, whether from lawful or unlawful sources, knowing that such funds will be used wholly or partly to commit terrorist acts by a terrorist person or organisation.
- 2 Intentionally participate in committing the crime of terrorism financing with a group of people or support them in committing it.
- 3 Fund travel for individuals to countries other than their country of residence or nationality for the purpose of committing, planning, preparing, or participating in committing or facilitating terrorist acts or providing or receiving training on them.
- 4 Contribute to committing any of the terrorism financing crimes mentioned in this paragraph or organise or direct others to commit them”.

Nevertheless, the Jordanian Cybercrime Law includes a provision that allows the application of other relevant legal texts to crimes not specifically covered by this law. This is articulated in Article 26, which states: “Anyone who commits a crime not specifically mentioned in this law and punishable under any other legislation using the information network, information technology, information systems, or websites, or participates, intervenes, or incites its commission, shall be punished according to the penalty specified in that legislation”.

3.2 Legal regulation of cyberterrorism promotion in UAE cybercrime law

Federal Decree-Law No. (34) of 2021 on Combatting Rumors and Cybercrimes in the UAE explicitly addresses the crime of promoting terrorist groups in Article 21. This paper stipulates:

“Anyone who creates or manages a website, supervises it, or publishes information or data on the information network or using information technology for a terrorist group, association, organisation, or unlawful body with the intent to facilitate communication with its leaders or members, recruit members, promote or endorse its ideas, fund its activities, provide actual assistance, or publish methods for making incendiary devices, weapons, ammunition, explosives, or hazardous materials, or any other tools used in terrorist acts, shall be punished with life imprisonment and a fine not less than 2,000,000 AED and not exceeding(4,000,000 AED).

The penalty for anyone who downloads content from the websites mentioned in the first paragraph of this paper, retransmits, or republishes it by any means, repeatedly accesses it, or publishes any content inciting hatred, is imprisonment for up to 5 years and a fine not less than, (500,000 AED), and not exceeding (1,000,000 AED).

In cases other than recidivism, the court may, instead of the penalty mentioned in paragraph Two, sentence the defendant to rehabilitation centers or electronic monitoring and prohibit the use of any information technology during a period determined by the court, not exceeding the maximum penalty.”

The Jordanian Court of Cassation ruled that the actions of the first and second defendants, which involved promoting a terrorist organisation (ISIS), were criminal. The second defendant had introduced the first defendant to the publications of this terrorist organisation via the internet on his mobile phone, ultimately convincing the first defendant of the organisation’s ideology, which falsely claimed to implement Islamic law and support Islam. The first defendant subsequently became a supporter of the organisation and began disseminating its ideas and publications to his acquaintances and friends via social media, persuading them to adopt the organisation’s ideology. This was done to gain more supporters for the terrorist organisation. The court concluded that their conscious and deliberate actions amounted to the promotion of a terrorist organisation’s ideology, fulfilling all the elements and components of the second charge against them, thereby justifying their conviction for this offense (Jordanian Court of Cassation, 2019).

This text clearly defines the crime of promoting terrorist groups and emphasises severe penalties. The UAE legislator has been stringent in addressing terrorism promotion through electronic means. The law includes several related crimes, such as the dissemination of information harming state interests (Article 22), incitement against state security and officials (Article 23), and promotion of sectarianism and national division

(Article 24). These provisions reflect an encompassing approach to tackling various aspects of cyberterrorism and its related activities.

Though these crimes are not explicitly labelled as ‘cyberterrorism promotion,’ they cover actions closely related to it, and perpetrators can be prosecuted for attempting such crimes using electronic means and media platforms, even if the criminal act was incomplete due to arrest or other reasons beyond their control (Al-Hayes, 2018, p.173).

3.3 *Legislative solutions to combat the crime of online terrorism promotion*

Cybercrimes generally have distinct characteristics that set them apart from traditional crimes, due to advancements in technology and the widespread use of Artificial Intelligence (AI) in various sectors (Tantawi, 2020, Link): <https://democraticac.de/?p=64965>

The crime of online terrorism promotion has several unique features:

- 1 *Difficulty of detection:* Online terrorism promotion is a challenging crime to detect for several reasons. It requires specialists to uncover, and the perpetrator may possess technical skills that make detection difficult. Additionally, it leaves no tangible evidence after commission since digital tools are used in technical information systems. The crime also requires substantial technical intervention to trace its traces.
- 2 *Transnational nature:* This crime is not confined by geographical or temporal boundaries. It can occur in one country and result in effects in another. Unlike traditional crimes, it does not require physical exertion but rather technical knowledge.
- 3 *Challenges in proof:* Proving this crime is difficult and relies on advanced means, such as AI systems. Many countries, including UAE, UK, USA, China, and Estonia, use these systems to solve complex digital problems. These systems can analyse investigations and gather evidence with minimal human intervention, leading to precise results that identify the perpetrators.

To mitigate the negative impacts of this crime, it is recommended that Jordanian lawmakers, considering technological advancements, explicitly address the crime of terrorism promotion through technical and electronic systems, social media, digital platforms, and information systems. This should be like the provisions found in the UAE’s Federal Decree-Law No. (34) of 2021 on Combatting Rumors and Electronic Crimes, which will be discussed in more detail in Section 2 of this study.

4 Conclusion

This scientific study has addressed the issue of digital terrorism promotion through digital platforms and new media, analysing both Jordanian and UAE cybercrime laws. It highlighted the importance of incorporating legal provisions to criminalise online terrorism promotion via digital platforms, social media, and new media. The study concludes with several results and recommendations, which will be summarised here. Firstly, technical infrastructure issues: The technical infrastructure continues to face significant issues that allow terrorists to infiltrate, along with insufficient international

cooperation between Jordan and other countries to address advanced electronic threats and ensure effective digital security. Furthermore, absence of clear legal provisions: The Jordanian Cybercrime Law lacks explicit provisions addressing the crime of promoting terrorist acts through technical systems, unlike the UAE Federal Decree-Law No. (34) of 2021 on Combatting Rumors and Electronic Crimes. Finally, rapid evolution of cybercrime: Cybercrimes are evolving rapidly, especially with the use of AI systems, digital platforms, and new media in their commission.

4.1 Recommendations

- 1 *Enhance technical infrastructure and international cooperation*: The study recommends the development of technical infrastructure and increased international cooperation between Jordan and other countries to keep up with advanced electronic threats and ensure effective digital security.
- 2 *Legislate against online terrorism promotion*: It is recommended that Jordanian lawmakers introduce provisions similar to the UAE Federal Decree-Law No. (34) of 2021 to penalise those who promote terrorists and terrorist organisations through digital platforms and new media, especially given the challenges faced by countries in combating online terrorism promotion.
- 3 *Regular updates to cybercrime laws*: The study advises that Jordanian lawmakers periodically review and update the Cybercrime Law to keep pace with technological advancements and make necessary amendments accordingly.

Funding

The authors did not receive support from any organisation for the submitted work.

Disclaimer

This paper does not contain any studies involving animals performed by any of the authors.

This paper does not contain any studies involving human participants performed by any of the authors.

References

- Abouahmed, A., Kandeel, M.E. and Zakaria, A. (2024) 'Personal data protection in the United Arab Emirates and the European union regulations', *Journal of Governance and Regulation*, Vol. 13, No. 1, pp.195–202, <https://doi.org/10.22495/jgrv13i1art17>
- Akhter-Khan, S.C., van Es, W., Prina, M., Lawrence, V., Piri, I., Rokach, A., Heu, L.C. and Mayston, R. (2024) 'Experiences of loneliness in lower- and middle-income countries: a systematic review of qualitative studies', *Social Science and Medicine*, Vol. 340, p.116438.
- Al-Rai, A. (2024) *Penal Protection of Privacy Through Digital and Traditional Media – A Comparative Study in Jordanian, Egyptian, and UAE Legislation*, Al-thaqafa Publishing and Distribution, Amman, Jordan.

- Al-Adwan, M.H.M. (2021) 'Criminal liability for illegal actions of AI entities', *Studies Journal, Sharia and Law Sciences*, Vol. 48, No. 4, Jordan University, Amman, Jordan.
- Al-Dakhil, K. (2002) *Events of September and the Arab Paradoxes*, Palestinian Studies Center, Palestine.
- Al-Daribi, A.A. (2012) *Cybercrimes – A Comparative Legal and Judicial Study*, National Center for Legal Publications, Cairo, Egypt.
- Al-Dhayeb, M.J. (2019) *Adequacy of Legal Foundations in Anti-Terrorism Legislation*, Al-Balqa Journal of Studies and Research, Amman Arab University, Amman, Jordan.
- Al-Hayes, K.M.A. (2018) 'Use of information technology in drug crimes, especially digital, considering UAE cybercrime law', *Journal of Economic, Administrative, and Legal Sciences*, Vol. 9, No. 2, June, pp.174–175.
- Al-Hurrah Channel (2023) *ISIS in 2023: Operations Leading to the Death of 700 People in Syria*, Link.
- AlOmran, N. and Al-Qassaymeh, M. (2023) 'Authenticating the administrative contract in electronic form and its legal force in Jordanian law', *Journal of Digital Evidence and Electronic Signature Law Review*, London, pp.1–9, <https://doi.org/10.14296/deeslr.v20i.5565>
- Al-Rai, A. (2024) *Cybercrimes – Explanation of the Substantive Provisions for Information Technology and AI Crimes*, Al-Badeel Publishing and Distribution, Amman, Jordan.
- Al-Rai, A.F. and AlOmran, N.M. (2024) 'Criminal protection of electronic signatures from forgery in Jordanian and UAE legislation', *International Journal of Electronic Governance (IJEG)*, Vol. 16, No. 2, pp.246–262, <https://doi.org/10.1504/IJEG.2024.140786>
- Boulanin, V. (2013) *Arms Production Goes Cyber: A Challenge for Arms Control*, Stockholm International Peace Research Institute, Link.
- Conway, M. (2016) *Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research*, Studies in Conflict and Terrorism (2017, Vol. 40, No. 1).
- Hornby, A.S., Cowie, A.P. and Lewis, J.W. (Eds.) (1974) *Oxford Advanced Learner's Dictionary of Current English*, 3rd ed., Oxford University Press, <https://doi.org/10.1093/oso/9780194311021>
- Institute for Economics and Peace (2023) *Overall Terrorism Index Score*, Retrieved from <https://www.visionofhumanity.org/maps/global-terrorism-index/#/> (Accessed 6, August, 2024).
- Jordan News Agency (2024) *On the 14th Anniversary of the Amman Bombings: Jordan Adopts Comprehensive Counter-Terrorism Strategies*, <https://www.petra.gov.jo/Include/InnerPage.jsp?ID=117655&lang=ar&name=news> (Accessed 9 August, 2024).
- Jordanian Court of Cassation (2019) Judgment No. 1081 of 2019 – Court of Cassation in its Criminal Capacity Issued on: 2019-05-16.
- Kamel, S.S. (2014) *Organized Crime in Comparative Law*, Judicial Department, UAE, Abu Dhabi.
- Khidel, A. and Casey, Z. (2021) 'Procedures for collecting digital evidence according to the Arab convention on combating information technology crimes', *Al-Ijtihad Journal for Legal and Economic Studies*, Vol. 1, No. 11, pp.2–29.
- Le Petit, R. (1993) *Dictionnaires De La Langue Française*, Dictionaries Le Robert, Paris.
- Mannheim, K. (1991) *Ideology and Utopia*, Routledge, London, UK.
- Moualla, N. (2008) *Marketing Management: A Comprehensive Strategic Analytical Approach*, Al-Yazouri Publishing House, Amman, Jordan.
- Oxford Advanced Learner's Dictionary (1974) Oxford University Press.
- Said, M.N.E. (2020) *Criminal Approach to Promoting Extremist Ideology Using Electronic Means – A Critical Analytical Study of UAE and Egyptian Laws*, University of Sharjah Journal, Sharjah, UAE.

- Syrian Observatory for Human Rights (2024) *Special Booklet by the Syrian Observatory for Human Rights Documenting the Syrian Situation in (July 2024)*, Syria.
- Tantawi, M.S. (2020) *Legal Aspects of Artificial Intelligence and Robotics*, The Arab Democratic Center for Strategic, Economic, and Political Studies, Link (Accessed 2 February, 2022).
- Wakeford, L. and Smith, L. (2020) 'Islamic State's propaganda and social media: dissemination, support, and resilience', in Baele, S.J., Boyd, K.A. and Coan, T.G. (Eds.): *ISIS Propaganda: A Full-Spectrum Extremist Message*, pp.155–187, Causes and consequences of terrorism series, Oxford University Press, <https://doi.org/10.1093/oso/9780190932459.003.0006>