PERINATAL JOURNAL

Original Article

Perinatal Journal 2025; 33(1):917-925

https://doi.org/10.57239/prn.25.03310099

Investigating emerging threats in cyber security: Evaluating the role of international community

Jamal Awwad Alkhar[1], Jafar Ali Hammouri[2*], Ali Abd Alah Almahasneh[3], Bassam Mustafa Abdul-Rahman Tubishat[4], Mishael M. Al-Raggad[5], Fadiah khasawneh[6]

[1,2,4,5,6]Jadara University, Jordan
[3]Irbid National University, Jordan

Abstract

Cyber threats have largely received international responses through tactics, emergency facilities and strategic policies. Joint efforts of local, international, public and private sectors toward protecting cyberspace and avoiding digital phobia have been made paramount as evidenced in previous research. Most preventive and security measures have partly reduced the threats, but none stabilize online securities. The networking-link of these threats which exceed national borders intensifies the fight against cyber threats. Hence, the current study's goal is to identify, measure and heighten the efforts being made internationally toward curbing cyber fears and threats. The study was specifically limited to Arab and Africa continents using descriptive and analytical methods. The study found that one of the efficient strategies for controlling online threats include operating secretly against victims; collaborating with neighboring countries; gathering relevant information from appropriate security agencies; creating intelligence gatherings; enacting preventive laws; providing proactive strategies and preparing deterrence theory. It was equally discovered that modern technologies immensely affect these emerging threats, thus complicate the preventive measures. Therefore, toward closing these missing gaps, the existing study argued that more efforts are still needed in different strategic areas.

Keywords: Cyber-threats, Strategic-policies, Cyberspace, Digital-phobia

.

Introduction

Cybercrimes are quite different from scope, nature and means of traditional crimes. The emergence of internet and information and communication technology open room for the misuse of technology, brought modern crimes, and create new criminal phenomenon that occur infiltration, penetrations and attacks into information systems, either for the purpose of destroying or obtaining these systems. This indicates that national and international communities are at risk as regard their personal, security and sensitive information, hence ways must be found to address this phenomenon.

Cybercrime is characterized by the nature of confidentiality and leaves little trace. In addition, cybercrime has no regional or time restrictions, and can cause immediate harm to countless victims (Hammouri, 2024).

It should be noted that information security issue has exceeded mere technical concept. This implies that the strategic dimension of national security mustinclude defense, security and military alliances.

In spite of the fact that technological development draws opportunities into the world, it is however established that it also carries many dangers with it. Hence, there is urgent need for clear and specific international legislation which could confront cyber terrorism across the world (Hammouri, 2024) These legislations would in turn enhance the capabilities of every country to prevent cyber-attacks by terrorist actors against critical infrastructure. Strategic programs are also needed to restitute and mitigate cyber-attack impacts on the victims.

In theory, commercial and political conflicts between countries are often carried out on cyber-space. In other words, malicious activities such as targeting government facilities, industrial networks, research-works, infrastructure and institutions are discharged on the internet. Meanwhile, this is capable of having devastating consequences most especially when it disrupts the operation of critical infrastructure.

Cybercrime has become more complex due to the development of technology like Cloud Computing, Internet of Things and Artificial Intelligence. All of

Correspondence: - Jafar Ali Hammouri, Jadara University, Jordan, **e-mail:** Jafar_hammouri@yahoo.com, **Received:** August 13, 2025 **Accepted:** October 6, 2025

these technologies are double-edged sword which not only draws benefits to governments and states, but also to crime perpetrators.

Accordingly, one of the major reasons behind the spread of cyber terrorism act is the less-important of high-tech instrument to attack victim. The only essential step is the transmission of malware or viruses, or the conversion of other person's details with modern devices. This indeed allows the terrorist to remain anonymous, thus lowers his probability of being arrested by appropriate authority.

The most important thing that distinguishes the current era from other eras is the exciting development the world is witnessing today. Despite many positives revolution brought by humanity in facilitating the transfer and exchange of information through internet technology, there is a growing fear of the growth of breaches, negatives, side effects of this network and its exploitation by some companies, organizations, gangs and individuals to commit and circulate actions that intersect with laws, customs and morals.

For countries to control traditional crimes and track down their perpetrators, security is no longer a narrow concept. Rather, its concept has extended to a wider range than that, as it rises to the level of accommodating the African Union and the Arab security states whose strategies are economic, political and social requirements in all fields. The Arab and other countries aimed at protecting themselves, thus led to the cooperation in the field of combating cybercrime and ensuring cyber security.

The African Union operates under Arab States League, and under the umbrella of agreements. Many cooperation agreements have been concluded in the field of combating cybercrime. Thus, the main question to be answered by the study is whether international efforts through international electronic conventions have the ability to influence through the legislation and provisions established for anti-regional crimes? Were countries able to extradite criminals, or at least implement what was stated in the articles of agreements about who committed cybercrime? Hence, the research importance lies in the extent of the danger posed by crimes, affecting individual's private life sanctity, threatening national security and leading to the loss of information.

Problem of the study

The problem statement stems from the context that the objective analysis of most technical reports, statistics and studies show that the future repercussions hover between fears and exacerbation of defense dilemma in front of security gaps; the inability of the security and cyber institutions and agencies; and the inefficiency of traditional strategies set, because they use the Internet in their dealings with attacks, accidents and threats.

Therefore, it is possible to recommend agencies with unconventional capabilities to play pivotal roles in confronting this type of unconventional threats such as protecting national cyberspace, enshrining privacy and taking all necessary mean sures to safeguard citizens against digital phobia.

International agreements in combating cybercrime: Budapest convention against internet crime

This agreement is the earliest agreement for cybercrime. On the 23rd day of November, 2001, the agreement which was structured for solidarity and international cooperation purpose to combat cybercrime was signed at Budapest, Hungarian (Al-Fiil, 2004). Countries like Japan, Canada, South Africa, United States of America and European countries also subscribed to this agreement. The agreement was not specifically designed for cyber terrorism, but to track and trace the scope of terrorist threats.

In 2016, under the Budapest Convention, a Guidance Note was issued by Cybercrime Convention Committee in respect of cyber-terrorism stating that the Convention substantive offenses may also be considered as terrorism acts. Therefore, terrorism activities would be supported and facilitated from financing aspect or preparatory work.

Global efforts in combating cyber terrorism crime

There are many efforts made by countries in the global information society in order to organize the process of developing optimal policies to deal with cyber terrorism by governments. Toward protecting worldwide information infrastructure from being exposed to dangers, several initiatives were adopted by various countries at the regional and national level

(Sadiq, 2018).

In light of the digital transformations that the world is experiencing, modern security threat appeared, meanwhile the digital environment is an important factor in its spread, and these threats have come to affect not only institution security, but also individual security, and thus posed a challenge to the state in its pursuit of its national security through the conscious choice to use ICT as development tool, which increased digital information systems use across industries, public and private organizations (Hashim, 2018).

Undoubtedly, risks and vulnerabilities increase as a result of reliance on digital information systems, particularly for Critical National Information Infrastructure (CNII), which include fraud, harassment, hacking, malicious code, hacking and denial-of-attacks. From the service, all of this increases the cyber threats that threaten the electronic sovereignty of the state.

Many websites were created to combat digital security and cyber terrorism. These websites were initiatives of government, civil society, private sector and companies that specialize on information and communication technology.

The most important strategy and policies adopted by the state to combat cyber terrorism

The global leadership establishes national agency to coordinate and promote the cyber security agenda, draft laws and an inclusive plan for professionals in similar field. Attacks beyond border open avenue for countries to collaborate with cyber security experts, policy makers, entrepreneurs and trade decision makers in this region in order to enhance resilience.

To combat cyber-terrorism, many websites have been created and they have become think-tanks to support digital security. Similarly, the Ministry of Communications and Multimedia has developed strategies that focus on the country's cyber security and increasing public awareness of the wise and ethical use of digital devices.

Efforts of Arabs toward curbing electronic

The Arab countries have consistently intensified their efforts to reduce cybercrime due to the huge losses that befall institutions and individuals. The dangers of these crimes are enormous, and this shows the seriousness of details transmitted through networks and information systems, including the stored data, and the extent of data, information, and programs of all kinds. Despite the data and its broad technical implications, cybercrime influences intellectual property rights, financial rights, information rights and material rights. In fact, the Arab Council Interior Minister was also keen to fight these crimes by putting laws in place to combat this crime.

Apart from the Unified Arab Penal Code and Arab Model Law, the Arab State League succeeded in concluding a number of 1981 Arab Convention for the Protection of Copyright in the field of combating cybercrime, which was one of the most important information technology crimes adopted by the Interior Minister of Arab Council in combating cybercrime, and was dealt with on the 21st of December, 2010 in Cairo.

The Arab convention for 1981 Copyright protection

This agreement was approved on November 5, 1981 with the aim of safeguarding author's rights over literary, artistic and scientific works in an efficient and unified manner, and in response to Article 21 (of the Charter of Cultural Unity) of the Arabs issued in 1964 for the protection of property, which called on the Arab countries to put in place legislation for both literary and artistic works (Abdullah, 2018).

This agreement was recommended by Arab Culture Ministers' Conference, which was held in Baghdad in 1981. The conference called for the development of necessary legislation to protect literary, artistic and scientific properties, which may be a target for cybercrime; If it finds its way to be published on the international information network, then Article (23) of this agreement obliges members of the state to work to establish national institutions to protect artistic, literary, property and scientific rights by saying: "Members of the state shall work to establish national institutions for copyright protection, and national legislation defines the structure of this institutions and their functions".

In order to ensure the realization of the terms of this agreement and the commitment of the members of

the state to it, Article (24) states that moral and material right of the authors must be protected (Lutfi, 2018). Undeniably, the Arab Convention for Copyright Protection is considered the first agreement concluded by Arab countries in this field.

Despite the direct contact that took place between the parties preparing this agreement and the World of Intellectual Property Organization, with the aim of the protection being in harmony with the obligations of the Arab countries towards the relevant international agreements, this agreement, in the opinion of some Arab jurisprudence, had many shortcomings. The Arab jurisprudence argued that it did not rise to the level that the Arab countries wanted it at the time, and by reading the texts of this agreement, it was found that they did not adopt any reference to the provision of collective management system of copyright and related rights (Dalala, 2007).

The 2010 Arab convention for combating information technology crimes

It resulted in the signing of the efforts of the Arab League in combating electronic crimes and an Arab agreement to combat information technology crimes at the end of 2010, as it was issued after the approval of the Arab Minister of Interior Justice in their joint meeting at Cairo headquarter on 12/21/2010, and enforced as of 7/2/2014, after being expired after 30 days, and after the date the document is been presented for ratification or approval thereof by 7 Arab countries. Paragraph 3 of the agreement stipulates that: "This agreement shall enter into force after the expiration of thirty days from the date of deposit of documents for ratification, acceptance or approval by seven Arab countries (Bashir, 2019).

The agreement aims to enhance cooperation between countries to combat information technology crimes that threaten their security, interests, and the safety of their societies and individuals, including tracking users, seizing materials stored on personal computers and technical devices. Chapter Four consists of (14) articles that regulate cooperation between member states in exchanging user's information (Al-Jayashi, 2011; Mansoor et al., 2025).

The aforementioned agreement includes substantive provisions represented in the criminalization of the acts constituting information technology crimes, namely: penetration, interception, assault on data integrity and intellectual property, misuse of information technology means, forgery, fraud, pornography, information technology crimes related to cyber-terrorism, money and drug laundering, trafficking in humankind and weapons, and the use of illegal use of credit tools and electronic documents", as well as tougher penalties for technical crimes committed by means of information technology (Al-Qadi, 2011; Jam et al., 2025).

This agreement includes the crime of causing injury to users and beneficiaries intentionally and unlawfully with the intent to defraud to achieve interests and benefits, in addition to that, criminalizing acts of producing or displaying[1], distributing, coding, publishing, buying, selling, or importing pornographic or immoral materials through information technology[2], gambling and incitement to prostitution, debauchery, and crimes of public morals which have been criminalized. In addition to assaulting the sanctity of family and private life of individuals or defamation; insult and defamation; and defamation of reputation through information technology were also criminalized[3]. The Arab Convention similarly dealt with crimes pertaining to information technology terrorism, and

[1] Article 11 of the agreement stipulates that: "Fraud crime: causing harm to beneficiaries and users
Intentionally and unlawfully with the intent of fraud to achieve interests and benefits in an illegal way, for the perpetrator or for a third party, by: 1- Entering, modifying, erasing or withholding information and data. 2- Interfering with operating function systems and communication systems, or attempting to disable or change them. 3- Disabling devices, programs and websites". Article (12) of this agreement stipulates that: "The crime of pornography: 1- Producing, displaying, distributing, providing, publishing, buying, selling or importing pornographic or immoral materials using the information technology. 2- The punishment for crimes related to child pornography and minors shall be severe. 3- The emphasis mentioned in Paragraph (2) of this article includes the possession of child and minor pornography or indecent materials for children and minors on information technology or the storage medium for such technologies.

[2] Article 13 of this agreement stipulates that: "Other crimes related to pornography are gambling and sexual exploitation".

[3] Article 14 of this agreement stipulates that: "The crime of attacking private life sanctity: private life through information technology".

crimes related to organized and committed crimes[4], through information technology[5], and crimes related to copyright and right infringements[6], illegal use of electronic payment tools[7], namely (prepaid cards, banking transfers- websites or accounts[8], and the crime of attempting and participating in the commission of crimes. These two agreements are based on the efforts of Arab League and international organizations[9]. This is an effort aimed at preventing computer crime.

With reference to the 1945 Charter of Arab State League, the interpretation of the general meaning of some texts contained in this Charter may serve as efforts to combat terrorism, including what was stated in Article Two of this Charter, which clarified the purposes of this organization in achieving cooperation among the state members to preserve their independence and sovereignty[10]. It can undoubtedly be said that the purposes of the League Council is to decide on the ways of cooperating with international bodies and ensuring security and peace in the future.

African union convention on cyber security and personal data protection of 2014

There are regional efforts in the face of cybercrime led by regional organizations among countries that have a common denominator, such as the African Union. This reflects the orientations of countries towards the need to develop regional legal frameworks and systems to combat cybercrime in the absence of a unified global framework.

The priorities of efforts made by African union to reduce cybercrime and cyber-security

The beginning of the efforts made by the African Union to reduce cybercrime and security was through the extraordinary conference held in Johannesburg, South Africa in 2009, for African Union ministers of sectors related to communications and information technology for African countries. Many issues related to the growing use of communication and information technology and the impact of its misuse on African countries cyber security were discussed. Following these discussions, African Union

[4](Article 15) of this agreement stipulates that: "Crimes related to terrorism committed by information technology means: 1-Spreading and advocating the ideas and principles of terrorist groups. 2- Financing terrorist operations, training them, and facilitating communications between terrorist organizations. 3- Publishing methods of making explosives, which are used especially in terrorist operations. 4- Spreading strife sedition and aggression against religions and beliefs".

[5] Article 16) stipulates that: "Crimes related to organized crimes committed by information technology means: 1- Carrying out Money laundering operations, requesting assistance, or publishing money laundering methods. 2- Promoting narcotics and psychotropic substances or trade in it. 3- Trafficking in persons. Trafficking in human organs. 4- Illicit arms trade.

[6] Article 17 stipulates that: "Crimes related to violation of copyright and related rights: violation of copyright, as defined according to the law of the State Party, if the act was committed intentionally and for non-personal use; if the act was committed intentionally and other than for personal use.

[7] Article 18 stipulates that: "Illegal use of electronic payment tools: 1- Whoever forges, fabricates, or places any devices or materials that help to counterfeit or imitate any of the electronic payment tools by any means. 2- Whoever seizes or obtain the data of any of the tools and using them or providing them to others or facilitating their obtaining by others, use the information network or any information technology means to gain unauthorized access to the numbers or data of any of the payment tools. 4- Whoever used a counterfeit payment tool with knowledge of that.

[8] Nazim Muhammad Nuri Al-Shammari, Abdel-Fattah Zuhair Al-Abd Al-Lat, Electronic Banking, 1st Edition, Wael Publishing House, Amman, 2008, p. 80.

[9] Article 19 stipulates that: "Attempt and participation in the commission of crimes: 1- Participation in the commission of any of the crimes stipulated in this chapter, with the intention to commit the crime. 2- Attempt to commit the crimes stipulated in Chapter Two of this Agreement: 3- Any state party may reserve its right not to apply the second paragraph of this article in whole or in part.

[10] (Article 2) of the 1945 Charter of the Arab League stipulates that: "The purpose of the League is to strengthen the ties between countries participating in it, and to coordinate their political plans, in order to achieve cooperation between them, preserve their independence and sovereignty, and to consider each other according to the systems of general documents on the affairs and interests of the Arab countries. Likewise, among its purposes is the cooperation of the participating countries between themselves and their conditions in the following affairs: 1- Economic and financial affairs, including commercial exchange and customs. 2- Transportation affairs, including railways, roads, aviation. 3- Culture affairs 4- Nationality affairs, passports, visas, execution of judgments and handing over Criminals. 5- Social Affairs. 6- Health Affairs.

Commission and United Nations Economic Commission for Africa were enjoined to come up with a legal framework for African countries towards addressing all issues related to data protection, cyber security and e-commerce.

Accordingly, African Union submitted a legal proposal for the year 2011. It was a draft agreement to establish a reliable economic framework for cyberspace security, through which Member States and regional groups in Africa seek to try to define the main goals and directions of information society, and to promote subsisting systems related to cyber security, data protection and electronic commerce toward creating information society.

It should be noted that the convention mandate is not restricted to electronic crimes and cyber-security, but likewise issues of information society such as protection of personal information and electronic commerce, considering the basic human rights principles guaranteed by the provisions of domestic laws, especially the African Charter on People and Human's Rights, and also under international conventions and treaties related to human rights.

In late 2014, it was signed by (14) countries and only ratified by (5) countries among other (55) countries. The agreement seeks to establish procedural and substantive criminal law provisions to address the governance of cyber-security and combat cybercrime in the African Union countries, and to impose obligations and measure the wide-ranging framework required by Member States to develop national policies to enhance the stability of cyber-security, as well as legal, regulatory and institutional frameworks for cyber-security monitoring.

The provisions of African union agreement on cyber-security and 2014 personal data protection

There is a set of measures and procedures covered by the African Union Convention on Cyber-Security and Data Protection of a personal nature for year 2014 which were related to the procedures of National Space Security System. These measures are dealt with in Article (25) of the Convention, and it could be summarized as follows:

A- Legislations to combat cybercrime: whereby each state party is committed to adopting effective regulatory and legislative measures to criminalize all criminal acts that affect the survival, integrity and confidentiality of communication and information technology systems, and basic network infrastructures., which is in addition to taking measures, and making an effective procedure for following up and prosecuting criminals.

b- National regulatory authorities: where each state adopts regulatory and legislative measures, as well as previously existing ones. Its phases are necessary to assign specific responsibility to organizations, whether newly established or their employees, in order to give them the legal permission to act on the entire aspects of of the implementation of space security, including cyber security incident response; restorative justice cooperation and coordination, public prosecution and forensic investigations.

C- Citizens' rights: Each state is obligated to ensure that these measures do not violate citizen's rights protected by domestic laws and national constitution. These measures as well should not impede international convention rights, African Charter on People and Human's Rights, human rights, privacy rights, fair trial rights and right to freedom of expression.

d- Protecting critical infrastructure: each party is obliged to adopt any necessary regulatory and legislative measures to identify sectors sensitive to its national security and economic prosperity, in addition to ICTs regulations programmed to operate in these critical sectors as vital information infrastructure, while imposing stricter penalties for criminal acts targeting these sectors and taking measures to protect them.

National system procedures for securing cyberspace

As for the procedures of the National System for Securing Cyberspace, the provisions of Article (26) referred to several procedures, including:

A Culture of securing cyberspace: Each state party is committed to encouraging a cyber-security culture among companies, stakeholders, civil society and governments that develops, owns, manages, operates and uses information systems and networks,

provided that this culture focuses on security when developing information network systems. The state parties are also committed to promoting a cyber-security culture by preparing and implementing programs and initiatives to raise awareness of security for system and network users, encouraging cyber-security culture development, and enhancing the participation of civil society.

B- The role of governments: Each state is committed to playing a leading role in developing a culture of cyber-security within its borders, through awareness, education, training and dissemination of information to the public.

C- Partnership between public and private sectors: Each member state is committed to developing this partnership as a model toward engaging academia, civil society and industry in promoting cyber security.

D- Training and education: Each state shall undertake necessary measures to build capacities with the aim of providing training that encompasses all cyber security areas, and to encourage technical education for professionals working in information technology field.

Procedures and national structures for monitoring cyberspace security

With regard to the procedures of national structures for monitoring cyberspace security, the provisions of Article (27) dealt with many procedures including a mechanism for taking the necessary measures to establish cyberspace security governance.

A - Institution responsible for the governance of cyberspace, provided that the governance is in accordance with a national framework capable of facing challenges and addressing all issues related to the information security at national level and in the largest possible range of cyber-security areas.

b- Response to incidents and alerts, there must be appropriate institutions to combat cybercrime and ensure cross-border national monitoring and international cooperation on the problems of cyber-security.

Provisions related to international cooperation and the reduction of crimes related to information technology

Article 28 of the Convention on many matters related to international cooperation, and in the light of what measures related to international cooperation, which oblige state to ensure that regional regulatory and legislative measures adopted to combat cybercrime would enhance the possibility of harmonization as required by state parties that do not have them. Double criminality of these measures and respecting the principle of responsibility agreements for mutual assistance in cybercrime field by encouraging the signing between them in accordance with the principle of dual criminal responsibility while at the same time promoting exchanges and encouraging institution establishment for exchanging cyber threats information such as information teams to respond to computer emergencies, electronic threats and improve cyberspace security.

It is worth noting that Europe Convention Council on cybercrime is the main difference between the African Union and other conventions, in that the draft convention is similar to that of regional conventions. In the absence of any instrument related to international cooperation, the African Union cannot be used. Article 28 deems it necessary to enhance information exchange and sharing in a rapid, urgent and mutual manner by institutions of member states responsible for the application of law on the territory through bilateral or multi-frame basis.

Crimes related to communication and information technology

Article 29 talks about the crimes of illegal access or attempting to gain access to computer systems, and staying or attempting to fraud in all or part of the information system. It is an unlawful interference with the system and illegal entry of data in the computer system. The vulnerabilities discovered in producing, publishing, displaying, assigning or providing computer hardware, software or any device or data or generate password or similar access code for electronic data, specially designed or computerized, illegal, will be liable for committing conditioned and criminal activities related to illegal content, particularly the production and dissemination of child pornography, and obtaining, circulating, owning and facilitating access to such material by minors will be held liable for cyber-crime

offence. Similarly, offences including publishing racist, xenophobic material, racist attacks based on pornography, and offenses of genocide, and crimes against humanity were all regarded as crimes with information technology.

The Convention in Article 30 dealt with criminal liability of persons; to punish and prosecute offenders, as well as procedural measures relating to the use, availability, and safety of the national defense infrastructure towards taking necessary legislative measures to ensure that cyber-crimes are controlled.

Conclusion

Undoubtedly, cyber-crimes and attacks pose great risks in all its forms including data, information and programs that inflict heavy losses on governments, institutions and individuals. Several agreements and decisions were made through convention. The agreements aim at enhancing cooperation between countries toward combating ICT crimes that threaten the interests and safety of government, communities and individuals. This agreement consists of collecting information and tracking procedural articles related to the rights of authorities and users, and controlling the materials stored on personal computers and technical devices. The scope of application of this agreement shall be at the regional level through the extraordinary conference held in Johannesburg.

The efforts of the African Union since its inception culminated in South Africa 2009, a year of increasing information technology for African countries, was discussed by African Union ministers for the sectors related to communications and technology. Many issues related to the growing utilization of communication and information technology and the impact of its misuse on cyber security of African countries were analyzed. As a result of these discussions, it was decided that the United Nations Committee on Africa Economic Data Protection and African Union Commission, should design a legal framework for African countries dealing with all aspects of cyber-security and electronic commerce.

It is not necessary to unite cybercrime international and regional efforts as it has borders, but important to extend and spread to all countries of the world, regardless of its distance or proximity, the awareness among members of the community by holding courses, seminars, conferences and informing the public about the dangers of cybercrime, and giving a role in this field to scholars, clerics and specialists. Accordingly, it is equally significant to train police officers on technical and modern methods used in the necessity of crimes, and training them on the measures that must be taken in this field, in order to expedite the detection and tracking of this crime, so as not to lose the evidence.

References

1- Jafar Ali Ahmad Hammouri, The Extent to Which the Condition of Publicity is Fulfilled in The Crime Of Incitement Via Electronic Means, Pakistan Journal of Life and Social Sciences, https://doi.org/10.57239/PJLSS-2024-22.2.00862.

2- Jafar Ali Ahmad Hammouri, The Criminal Liability of Artificial Intelligence Entities, Pakistan Journal of Life and Social Science, https://doi.org/10.57239/PJLSS-2024-22.2.00662.

3-Adel, A. S. (2018). Cyberspace and International Relations: A Study in Theory and Practice. Cairo: The General Book Authority, p. 485.

4-Ali, A. A. (2011). Cybercrime: A Comparative Study, 1st edition, Beirut: Zain Legal Publications, p. 74.

5- Bilal, M. A. (2018). Copyright in Arab Laws. 1st Edition, The Arab Center for Legal and Judicial Research, Council of Arab Ministers of Justice, League of Arab States, Beirut, p. 21.

6- Khalid, H. A. L. (2018). Electronic Terrorism, the Scourge of the Modern Age and Legal Mechanisms for Confrontation. Dar Al-Fikr Al-Jami'i, Alexandria, p. 178.

7- Muhammad, S. H. Malaysia's National Cyber Security Policy: The country's cyber defense initiatives: https://ieeexplore.ieee.org/document/5978782

8- Munir, M. A. & Mamdouh, M. A. (2004). Internet and computer crimes and means of combating them, Alexandria: Dar al-Fikr al-Arabi, p. 96.

9- Nazim, M. N. S. & Abdel-Fattah, Z. A. (2008) Electronic Banking, 1st Edition, Wael Publishing House, Amman, p. 80.

10- Remy, M. Q. (2011). Combating Information Crimes in Comparative Legislation in Light of International Conventions and Charters, 1st

edition, Dar Al-Nahda Al-Arabiya, Cairo, p. 75.
11- Safaa Kazem, G. A. (2016). The Crime of Mail Piracy (A Master's thesis), College of Law, University of Babylon, p. 42.
12- Salim, B. (2019). Solving the Problem of International Criminal Jurisdiction Conflict in the Field of Combating Electronic Commerce Crimes - According to the Arab Convention on Combating Information Technology Crimes for the year 2010, Journal of Rights and Freedoms, Muhammad University Kheidar-Biskra, Algeria, Volume (5), Issue (1), p. 123.
13- Samer, M. D. (2007). International Measures in the Field of Collective Management of Copyright and Neighboring Rights Between Theory and Practice, A Comparative Study), Al-Manara Journal for Research and Studies, Volume Thirteen, Number Eight, Al al-Bayt University, Oman, pp. 221-222.
14- Jafar Ali hammouri, Subjectivity of artificial intelligence in criminal law: New challenges, Edelweiss Applied Science and Technology, 2024.
15- United Nations Report, Combating the Use of Information and Communication Technology for Criminal Purposes, p. 48.
16- Jam, F. A., Ali, I., Albishri, N., Mammadov, A., & Mohapatra, A. K. (2025). How does the adoption of digital technologies in supply chain management enhance supply chain performance? A mediated and moderated model. Technological Forecasting and Social Change, 219, 124225.
17- Mansoor, M., Khan, T. I., Jam, F. A., & Alasmari, M. (2025). From donations to devotion: how cause-related marketing frames drive brand evangelism through cognitive and social pathways in hospitality. International Journal of Contemporary Hospitality Management.