

Combating Cybercrime in Arab States: Challenges and Strategies

SAIDANI Faiza

Faculty of Law and Political Science ,University of
BOUMERDES,f.saidani@univ-boumerdes.dz,

Received: 13/05/2025

Accepted: 12/11/2025

Published:25/12/2025

Abstract:

With the rapid pace of digital development and the growing cyber threats in recent years, Arab States have witnessed a significant surge in cybercrime rates. This has placed them before urgent security, legislative and technical accelerated challenges. Combating this emerging type of crime has become an urgent necessity, imposing on Arab States to develop their legal frameworks and to strengthen their institutional and technical capacities; in order to keep pace with the complex and rapidly evolving nature of digital crime.

This research starts by analyzing the conceptual and legislative frameworks of cybercrime, in addition to reviewing the joint challenges amongst Arab States, with a focus on the Algerian model as a case study.

For those reasons, a descriptive-analytical approach, supported by a comparative method, has been adopted to highlight the key challenges faced by Arab States, as well as to monitor and evaluate national and regional strategies, including the Algerian cyber security strategy.

Keywords:cybercrime; cyber security; digital development; Arab States; cyber security strategy.

Corresponding author: SAIDANI Faiza, **e-mail:** f.saidani@univ-boumerdes.dz

1. INTRODUCTION

Digital revolution resulted in deep transformations in different aspects of life. Modern techniques today represent a fundamental pillar in economy, education, administration and communication. However, this technological development, despite its positives, was accompanied by the emergence of new types of criminal behavior, technically called “cybercrimes”, which represent a growing challenge confronting justice systems in different countries worldwide, including Arab States.

Cybercrime is distinguished by its cross-border character, its fast development and its close connection with modern digital techniques, which makes its combat a complicated issue that requires a coordinated effort at the national and regional levels.

Despite the Arab States’ attempts to confront this threat by enacting specific legislations and establishing cyber security strategies, however, reality shows the challenges continuation, either at the level of legislation, or technical infrastructure, or human competencies.

From this standpoint, this research aims to study how the Arab States efforts are successful in combating cybercrime, and to stand on the most important challenges they confront, with the analysis of adopted strategies and the suggestion of practical solutions to reinforce Arab cyber security. Therefore, the research problematic is: **To what extent were Arab States capable of establishing and executing effective strategies to combat cybercrime under legislative, technical and institutional challenges they confront?**

In that framework, we adopted in this research the descriptive-analytical method through the study of legal texts and institutional mechanisms adopted in Arab States, with the focus on Algeria as a study

module. Moreover, the case study method was employed in order to analyze Algerian strategies and practices in combating cybercrime, in addition to the comparative method to highlight other Arab experiences and to extract learned lessons.

2. The theoretical framework of combating cybercrime

Cybercrime is considered as one of the innovative phenomena, which imposed itself strongly on the legal system under the accelerated digital revolution. This called for the necessity to develop legislative and legal frameworks able to confront it.

Dealing with these crimes requires an accurate understanding for their legal nature, and distinguishing them from traditional forms of the crime, in addition to determining legal principles and theories forming the pillar of combating them.

Therefore, this axis aims to highlight the legal theoretical framework of combating cybercrime, through analyzing related legal concepts, as well as showing the foundations of criminalization and punishment, in addition to the problematics arisen by this phenomenon under the multitude of legislations and the contrast of legal systems.

2.1 Nature of cybercrime

With the development of technology and communication means, new patterns of crimes emerged, which were unfamiliar before, most notably cybercrime. These crimes are distinguished by their connection to digital space, either in terms of the means or in terms of the aim, which imposed new challenges in front of legislators at the Arab level.

In this context, this part aims to clarify the nature of cybercrime by defining it, as well as showing its characteristics and different forms.

I- Definition of cybercrime

Cybercrime is considered as one of the legal innovative concepts, which emerged as a result of accelerated development in the field of information and communication technology. There are different definitions related to this type of crimes, depending on the angle from which they are viewed, either from the legal aspect or the technical or social one. This made it difficult to reach a comprehensive definition.

Legally, cybercrime is defined as: “It is every illegal act performed using the computer or the internet network, aiming to assault persons or possessions or institutions, either for material or moral purposes”)Serour ‘ (2010. This definition emerges the technical nature of crime regarding the means, and it also focuses on the assault element as an essence of criminal behavior.

While from a wider perspective, some has defined it as: “Every illegal behavior performed via the use of electronic instruments or information networks that affects public security or assaults rights or legally protected interests”)Khadhr(1018 ‘. It is a definition that takes into consideration the wide range of cybercrime, including economic, social and political crimes.

At the Arab level, some legislations had tried to present their own specific definition, as the Arab model law concerning combating information technology crimes states that cybercrime is: “Every act committed using any of the information technology means, infringing the provisions of this law”)States(2010 ‘. This definition, despite its generality, reflects a legislative orientation to classify these crimes within determined legal frameworks.

In this context, a remarkable disparity is remarked in the definition of cybercrime amongst Arab legislations. In Algeria, the law 04-09 issued

in the year 2009 does not include a direct definition of cybercrime. However, its texts refer implicitly that: “It is every illegal use of mechanical data treatment means aiming to commit a crime or to facilitate its commission¹”.

While in Egypt, the law N° 175 of the year 2018 defines cybercrimes in a way that includes technical and social dimensions, as it stated that they are: “Every assault on any of the family principles or values in the Egyptian community, or on the private life sanctity, or every violation of information or data or electronic websites’ systems illegally²”.

While in the United Arab Emirates, the decree, by the Federal Law N° 34 of the year 2021, adopted a general flexible definition, in which it was stated that cybercrime is: “Every act that is performed using an information network or a technical information means, and that forms a law violation³”. This definition shows an orientation towards leaving a large space to estimate judiciary in the description of acts within this range.

The diversity of proposed definitions reflects the complex nature of cybercrime, and it also emerges the need to develop flexible legal approaches that take into consideration the quick changes in used means and methods while committing this type of crimes.

II- Characteristics and classifications of cybercrime

This part aims to show the most prominent characteristics of cybercrime and its classifications; in order to understand its renewable

¹People’s Democratic Republic of Algeria, Law N° 04-09 dated on August 05th, 2009, including specific rules of prevention against crimes linked to information and communication technologies and to their combating, Official Journal, Issue 49, 2009.

² Arab Republic of Egypt, Law N° 175 of the year 2018 concerning combating information technology crimes, Official Journal, Review 33 bis (N), on August 14th, 2018.

³The United Arab Emirates country, the decree by the Federal Law N° 34 of the year 2021 concerning combating rumors and cybercrimes, Official Journal, Review 712, 2021.

nature as well as the challenges coming up while confronting this phenomenon under the accelerated technological progress.

A) Characteristics of cybercrime

Cybercrime is characterized by a number of characteristics that distinguish it from traditional crimes and makes its combat more complicated. Amongst the most prominent characteristics we state:

- **The non-material character:** Cybercrimes are committed in a hypothetical environment. In most cases, they do not leave tangible material traces as the ones resulted from traditional crimes. This makes discovering and proving them more difficult)Khadr(2020 ‘.
- **The cross-border spread:** Cybercrime does not recognize geographical boundaries, as the criminal act may be committed in a state, while its result occurs in another state. This poses legal problematics at the level of jurisdiction and international cooperation)Al-Baghdadi(2019 ‘.
- **The quick technical development:** Means and methods of committing cybercrime develop in a great speed. This makes the legislator in a permanent race to keep pace with these updates)Abdelaal(2021 ‘.
- **The possibility to disappear and camouflage:** Cybercrimes’ perpetrators benefit from coding technics, private networks (VPN) and anonymity software. This makes it more difficult to track down the culprits)Hussein(2018 ‘.
- **Targeting both individuals and institutions:** Cybercrime may affect individuals, such as electronic blackmail crimes, as it may affect institutions, such as cyber-attacks against infrastructures)Abdullah(2017 ‘.

b) Cybercrime classification

Cybercrime classification varies according to numerous criteria, which emerge the different dimensions of this complex phenomenon. Amongst the most important adopted classifications we state:

- **In terms of the crime target:**
 - **Crimes of a material nature:** They aim to achieve illegal financial profit, such as electronic fraud and stealing bank cards.
 - **Crimes of moral nature:** They aim to defame or terrorize or blackmail or harm the reputation)Mohammed Al-Moumni(2016 ‘.
 - **Crimes of political or ideological nature:** Such as attack targeting the State institutions, or informational websites, for political or ideological reasons⁴.
- **In terms of the targeted victim:**
 - **Crimes against individuals:** Such as defamation, harassment and impersonation.
 - **Crimes against institutions:** Such as attacks on banks, companies and universities.
 - **Crimes against the State:** Such as cyber-attacks targeting vital infrastructures or national security (UNODC, 2013).
- **In term of the criminal act nature:**
 - **Crimes targeting information systems themselves:** Such as hacking or systems’ disable.
 - **Crimes committed through information systems as a means:** Such as drug promotion or money laundering via internet)Fawzi(2015 ‘.
- **In terms of the actor (the perpetrator):**
 - Independent individuals (Hackers).
 - Organized communities (Cybercrime gangs).

⁴Europol, « Internet Organized Crime Threat Assessment (IOCTA) », 2022, p. 19.

- International or governmental bodies (State-sponsored attacks)⁵.

This classification shows the flexibility and the numerous dimensions of cybercrime. This makes it necessary to adopt multi-specialties approaches while studying and analyzing them legally.

2.2 Legal foundations for combating cybercrime in Arab States

In modern technology era, cybercrime has become a growing threat that affects individuals, institutions and states. This requires establishing effective legal foundations in order to combat them. Given the cross-border feature that distinguishes these crimes, confronting this challenge requires a local and international legal coordination in order to ensure the informative systems protection as well as the rights of individuals.

In Arab States, the urgent need emerged to develop legal legislations that keep pace with the quick technological developments. Many of these countries worked on formulating laws specific to combating cybercrime. Some legal initiatives aiming to reinforce cyber security were adopted, and sanctions on crimes committed via internet were imposed.

This part deals with legal foundations to combat cybercrime in Arab States, highlighting laws and applied legislations, and determining challenges confronting these countries within the framework of dealing with these constantly increasing crimes.

I- Development of Arab legislations

During the last two decades, Arab States witnessed a remarkable development in the field of legislations related to combating cybercrime, as a result to the increasing cyber threats and the spread of using internet and

⁵OECD, Computer-Related Crimes, 2020, p. 14.

digital media in different fields of life. This development has come as a response to an urgent need to protect digital security of both individuals and institutions, as well as to ensure the non-exploitation of electronic space for criminal purposes.

Most of Arab States did not possess specialized laws that deal with information crimes, as they depended on general texts in the criminal law. However, these texts proved their insufficiency in front of the cybercrime specific nature, either in terms of the means or the effect or the crime's proof. This made us think about the elaboration of specific legislations.

Furthermore, and with the increase of cyber-attacks' frequency, a group of Arab States started issuing specific laws or inserting legal texts within their penal laws. These specific laws deal with crimes committed via electronic means. Amongst the most prominent examples we state:

- **United Arab Emirates:** Amongst the first Arab States that had enacted a comprehensive law to combat cybercrime, as the federal law N° 5 of the year 2012 was issued (in addition to its modifications). This latter includes detailed texts related to hacking, defamation, electronic fraud and national security threat via internet⁶.
- **Kingdom of Saudi Arabia:** It had issued the information crimes' combating system by virtue of the Royal Decree N° D/17 of the year 2007 that includes clear sanctions for a number of cybercrimes, such as systems hacking, defamation and violation of public morals⁷.
- **Egypt:** It passed the information technology crimes combating law N° 175 of the year 2018, which is one of the

⁶Federal Law N° 05 of the year 2012 concerning combating information technology crime, United Arab Emirates.

⁷The information crimes' combating system issued by virtue of the Royal Decree N° D/17 dated on 08/03/1428 AH, Kingdom of Saudi Arabia.

comprehensive laws covering crimes related to access to information systems illegally, to stealing data and to disable services⁸.

On the other hand, some Arab States were keen to join international and regional conventions in order to combat cybercrime, such as the Arab convention for combating information technology crimes (2010). This convention aims to unify legal and technical efforts amongst the member States of the Arab League)League(2010 ‘, in addition to the attempts to join or to align with the Budapest Convention, although a number of Arab States is still reserved on some of its terms for sovereign or legal reasons.

However, and despite the remarkable progress in the laws’ issuance, there are still challenges obstructing the effectiveness of these legislations, including the weakness of execution mechanisms and the lack of technical competencies at the devices in charge of applying law on one hand, as well as the slow legal update compared to the quick development of cybercrime on the other hand. In addition to the legal framework disparity that obstructs the effective judicial cooperation amongst Arab States.

II- Challenges of criminalization and sanction in the face of cybercrime

The issue of criminalization and sanction represents one of the most prominent challenges facing countries while combating cybercrime. The essence of this problematic lies in the difficulty of traditional legal rules’ suitability for the nature of crimes committed within digital environment, notably in terms of the technical characteristics of these crimes, the complexity of proving them and the multitude of concerned parties.

a) Problematic of criminal acts’ determination

⁸The information technology crimes combating law N° 175 of the year 2018, the Egyptian Official Journal, Review 32 bis.

Cybercrime is characterized by dynamism and quick development. This makes the determination of acts that must be criminalized a complex task, as the legislator often delays in understanding the new forms of these crimes. Furthermore, some acts, which are considered harmful in the digital space, do not find an explicit legal document to criminalize them within traditional criminal texts, such as hacking personal accounts or digital impersonation)Abdullah H.(2021 ‘.

b) Criminal legitimacy principle and adaptation difficulty

The criminal legitimacy principle, which states that “there is no crime and no punishment without a text”, prevents the punishment of many cybercrime perpetrators, especially when new acts, which have no accurate description in national criminal laws, are committed. This raises the legal adaptation issue, which is considered as one of the most prominent problematics faced by judiciary in cybercrimes)Azzarwali(2022 ‘.

c) Established sanctions and their deterrence extent

In many Arab States, legislations suffer from the weakness of sanctions established for cybercrimes, either in terms of their type or their severity. This poses questions about how they are effective in general and private deterrence, as dangerous crimes are often punished with simple sanctions that are not proportionate to the extent of damage, especially in crimes violating private life or those targeting sensible information systems)Adel Ben Yucef(2020 ‘.

d) Lack of legislative coherence between countries

The lack of legislative coordination between Arab States obstructs the effectiveness of combating cybercrime, especially that these crimes often exceed national boundaries. Moreover, the lack of a unified definition of cybercrime, and the contrast of imposed sanctions, both complicate the

international judicial cooperation opportunities and obstruct the extradition and information exchange mechanisms)Bousbaa(2023 ‘.

3. Challenges and strategies facing cybercrime

Through what was concluded from the first topic, where cybercrimes today take various and renewable forms, targeting privacy, security, economy and even national sovereign, and before this changing reality, the urgent need to a deeper understanding of challenges related to this type of crime emerges, in addition to searching effective strategies for prevention and confrontation, which ensures society protection and digital security reinforcement.

3.1 Institutional and technical challenges

Modern societies face several challenges at both the institutional and technical levels, especially under the accelerated changes witnessed by the world today. Furthermore, and while institutions aim to develop their performance and achieve competency, modern technics impose new requirements calling for adaptation and innovation.

From this point, the need to understand these challenges emerges in order to set effective solutions ensuring balance between institutional development and technological progress.

I- Weakness of capacities

The weakness of capacities is considered as one of the most prominent obstacles confronting the efforts of combating cybercrime, either on the institutional or at the individual level. This weakness is represented in many fundamental aspects:

a) Weakness of specialized human competencies: Many institutions, especially in developing countries, suffer from the lack of

competent managerial staff in the fields of cyber security, either in terms of number or competency. This lack affects directly the capacity to reveal cybercrimes and to confront them effectively)Al-Aoufi(2021 ‘.

b) Lack of training: Institutions often lack specialized and continuous training programs in this field. This leads to a gap between the development of cybercrime methods and the level of available qualification)Ibrahim(2022 ‘.

c) Weakness of technical infrastructure: In many cases, the modern technological means necessary for monitoring, tracking and analyzing are not available to the relevant parties. This limits their quick and effective response capacity)Moussaoui Assia(2021 ‘.

d) Lack of coordination between parties: The lack of coordination and cooperation between different institutions (security, judicial, technical) is considered as one of the institutional weakness aspects that obstruct joint work in combating these crimes ((ESCWA), 2021).

II- Lack of coordination

The lack of coordination between parties concerned with combating cybercrime is considered as one of the fundamental factors that awaken the efficiency of response to this growing phenomenon. This lack is manifested at several levels:

a) Weakness of cooperation between security and judicial bodies: Each system often works apart from the other one. This leads to the procedures’ conflict or delay, and obstructs tracking and questioning perpetrators as required)Jad Allah(2022 ‘.

b) Absence of clear communication channels: Many countries lack clear and organized mechanisms to exchange sensible information between

relevant institutions. This leads to repeat efforts or to lose important data during investigations)Al-Moumni(2023 ‘.

c) Lack of regional and international cooperation: Despite the cross-borders’ character distinguishing cybercrimes, coordination between countries is still weak, either in terms of information exchange or legal help. This grants these crimes’ perpetrators a wide margin to move without questioning (ESCWA, 2021).

d) Lack of a unified legal coordination framework: The difference of local laws and the lack of unified legislations or effective conventions lead to real difficulties in coordinating efforts and in activating cooperation in both the judicial and technical fields)Abdullah K.(2022 ‘.

3.2 National and regional strategies

With the increasing threats related to cybercrime, the need to develop effective strategies at both the national and regional levels emerged. These strategies are considered as a fundamental tool for efforts’ organization, priorities’ determination and capacities’ enhancement in both the protection and prevention fields.

Moreover, regional coordination also contributes to confront the cross-borders’ character of these crimes; through exchanging experiences and information as well as reinforcing joint cooperation.

I- National policies

National policies are considered as the foundation stone in confronting cybercrime, as they determine the general framework on which the State relies while setting plans and programs related to cyber security. These policies include several fundamental axes:

a) Setting national strategies for cyber security: Several countries worked on formulating comprehensive national strategies aiming to reinforce the cyber space security; through organizing legislations, improving digital infrastructure and supporting human capacities (ESCWA, National cyber security strategies in the Arab region, 2021).

b) Enacting cybercrime laws: National laws specialized in combating cybercrimes represent a fundamental basis in national policy; where criminal acts are defined, sanctions are determined as well as tracking and prosecution procedures are clarified)Hamdi(2022 ‘.

c) Creating specialized institutions: Some countries created national entities or centers specialized in cyber security. They are concerned with monitoring digital threats and coordinating between different parties in order to ensure the quick and effective response)Security(2023 ‘.

d) Reinforcing awareness and digital education: National policies aim as well to raise the individuals and institutions awareness of cybercrime risks; through media campaigns as well as educational and training programs in order to build a digital preventive culture)Samer(2021 ‘.

e) Encouraging partnership with the private sector: In view of the great role of private sector in digital space, modern national policies aim to integrate this sector into the electronic protection system through clear and sustainable cooperation mechanisms⁹.

II- Arab cooperation

Under the increasing cross-borders’ digital crimes, the Arab cooperation in the field of combating cybercrime has become an indispensable strategic necessity. Furthermore, the weak individual potential of some countries, the diversity of legislations and the lack of joint

⁹The Arab Center of Cyber Security, Ibid.

databases are all factors that make of regional coordination an indispensable option.

In addition to that, Arab cooperation takes many fundamental forms:

a) Setting conventions and memorandums of understanding: Via the League of Arab States and belonging organizations, Arab States aimed to set a legal and institutional cooperation by means of conventions aiming to facilitate information exchange and mutual legal help in cyber cases)States L.(2010 ‘.

b) The legislations and legal references’ unification: Some Arab initiatives work on unifying or approaching cybercrime legal frameworks; in order to avoid legal contradictions obstructing judicial cooperation between countries (ESCWA, Legislations Related to Cybercrime in Arab Region, 2021).

c) Building joint databases and information centers: There is an orientation towards developing Arab platforms to exchange information about cyber threats, potential attacks and protection methods. This makes it easier for countries to prepare and respond collectively)Technologies ‘ (2022.

d) Organizing trainings and regional workshops: Some entities, such as “The Arab Organization of Communication and Information Technology”, organize training courses and workshops specialized in cyber security, where experts participate from different Arab States in order to reinforce capacities and exchange experiences)Security A.(2023 ‘.

e) Collective work within international initiatives: Some Arab countries aim to adopt a unified position inside international organizations, such as “The International Union of Communications” and “The United

Nations Office” concerned with drugs and crime; in order to defend the Arab States digital interests globally (UNODC I. &., 2021).

4. CONCLUSION

Cybercrime has become today one of the most prominent security challenges confronting Arab communities in digital era; in view of its new character, technical complications and quick development, in addition to its cross-borders’ feature. Furthermore, this study had shown that the majority of Arab States, including Algeria, had realized the importance of combating this phenomenon by enacting new legislations, creating specialized entities and launching cyber security national strategies.

However, analyzing reality reveals the presence of a gap between theoretical frameworks and actual application, as many countries suffer from the lack of technical competencies and the weakness of digital infrastructures, in addition to failure in Arab regional coordination.

Moreover, the need to keep pace with the quick development of cybercrime methods emerges. This requires adopting comprehensive and integral approaches, which gather legal deterrence, communal prevention and technical qualification.

Recommendations:

➤ At the internal level of Arab States:

- 1. Updating and unifying national legislations** in order to keep pace with cybercrime updates, with the focus on emerging crimes (such as malignant artificial intelligence, digital sexual blackmail...).
- 2. Reinforcing training** in cyber security fields at the level of security devices, judges and Public Prosecution.
- 3. Creating specialized units** to investigate cybercrimes at the level of all the provinces inside the State.

4. **Developing cooperation between the public and the private sector**, especially telecom companies and banks, for the early reporting of digital crimes.
 5. **Launching national campaigns to aware of** internet dangers and prevention methods, especially in schools and universities.
- **At the Arab regional level:**
1. **Activating the Arab Nations League role** in security digital coordination by creating a joint Arab center for cyber security.
 2. **Signing bilateral multilateral conventions** to exchange information and experiments and to facilitate tracking criminals across borders.
 3. **Establishing a unified Arab database** of cybercrime and its types for preemption and early warning.
 4. **Encouraging scientific research** in the fields of information technology and digital security within Arab universities.

5. Bibliography List :

- (ESCWA), E. a. (2021). *Regional Cooperation of Combating Cybercrime*. United Nations.
- Moussaoui Assia .(2021) .Development of information and communication technology infrastructure is the basis of digital economy. Case study: Algeria (ICT) . (2017-2007) *Al-Manhal Al-Iqtissadi Magazine*, Volume 4, Review 3.
- Adel Ben Yucef .(2020) .*Criminal law and digital era challenges*.Tunisia,: The Arab Law Academy Publications.
- Mohammed Al-Moumni .(2016) .*Cybercrimes between reality and challenges*. Oman: Athaqafa Publication House.
- Abdul Rahman Fawzi .(2015) .*Intellectual property rights in digital environment*.Al-Fikr Al-Arabi Edition House.
- Ahmed Fathi Serour .(2010) .*The mediator in penal law- general section*.Cairo: Al-Arabiya Edition House.
- Ahmed Ibrahim .(2022) .Electronic training and digital security challenges . *The Arab Magazine of Information Technology*, Volume 15, Review 2.
- Al-Bikri Samer .(2021) .Community awareness as an entry to cybercrime prevention . *Education and Technology Magazine Series 6*, Review 1.
- Ali Abdullah .(2017) .*Cybercrimes and information security*.Oman: Law and Security Library.
- Arab Union of Cyber Security .(2023) .*The Annual Report of Arab Training and Cooperation in Digital Security*.Arab Union of Cyber Security.
- ESCWA. (2021). *Cybercrime and Regional Cooperation in the Arab World*. United Nations.
- ESCWA. (2021). *Legislations Related to Cybercrime in Arab Region*. United Nations.
- ESCWA. (2021). *National cyber security strategies in the Arab region*. United Nations.

- Fatma, « », Hamdi .(2022) .Cybercrime legal framework in Algerian legislation .*Legal Studies Magazine, Review 12*.
- Hassan Abdullah .(2021) .*Cybercrime: definition and legal challenges*.Alexandria :Al-Jamiaa Al-Jadida Edition House.
- Hicham Khadr .(2020) .*Cybercrimes in the temporary criminal law*. Alexandria: AL-Jamiaa Al-Jadida Edition House.
- Karim Abdullah .(2022) .Legal framework of combating cybercrimes in the Arab World .*The Regional Conference about Digital Legislations*.Tunisia.
- Khaled Al-Baghdadi .(2019) .*The criminal law of cybercrime*.Cairo: Annahda Al-Arabiya Edition House.
- League of arab States .(2010) .*Arab Guiding Law for combating information technologu crimes*.General Secretariat.
- League of Arab States .(2010) .*The Arab Convention of Combating Information Technology Crimes*.Cairo.
- League of Arab States .(2010) .*The Arab Convention of Combating Information Technology Crimes*.General Secretariat.
- Leila Al-Moumni .(2023) .Role of institutional coordination in combating digital crimes .*The Arab Magazine of Security Studies Volume 17, Review 3*.
- Leila Bousbaa .(2023) .International judicial cooperation in combating cybercrimes .*Law and Technology Magazine Algiers 01 University, Review 07.55* ,
- Mahmoud Hussein .(2018) .*Information technology and cybercrime*.Al-Fikr Al-Jamii Edition House.
- Mohamed Al-Aoufi .(2021) .*Cyber security in Arab World: Reality and challenges*.The Middle East Studies Center.
- Mohammed Azzarwali .(2022) .Legitimacy principle in face of cybercrime .*The Moroccan Magazine of Legal and Judicial Studies*.12 ,
- Mustapha Khadhr .(1018) .*Cybercrime in comparative law*.Beirut: Lebanon University Publication.

- Said Abdelaal .(2021) .*Criminal investigation in information crimes*.Cairo: National Center for Legal Publications.
- Sami Jad Allah .(2022) .Legal challenges in combating cybercrime .*Law and Security Magazine, Review 8*.
- The Arab Center of Cyber Security .(2023) .*Arab Experiments in Building National Institutions for Digital Security*.The Arab Center of Cyber Security.
- The Arab Organization of Communication and Information Technologies . .(2022)*Arab Joint Cyber Security Platform Project*.The Arab Organization of Communication and Information Technologies.
- UNODC. (2013). *Comprehensive Study on Cybercrime*. USA: United Nations.
- UNODC, I. &. (2021). *Cybercrime Capacity Building in the Arab States*.ITU & UNODC.