

International Cooperation in Combating Cybercrime: An Analytical Study of Qatari Legislation and International Legal Frameworks

Suggested classification: Review scientific article

Author 1

Dr Nashat Mfudi Al-Maasfeh

Assistant Professor of Criminal Law, Police Academy, Qatar

Corresponding author

Email: nalmoafsa@moi.gov.qa

Telephone: +974 5557 2681

Author 2

Dr Hani Jamil Al-Tarawneh

Assistant Professor of Criminal Law, Police Academy, Qatar

Author 3

Dr Shareh Naif Al-Otaibi

Assistant Professor of Criminal Law, Police Academy, Qatar

International Cooperation in Combating Cybercrime: An Analytical Study of Qatari Legislation and International Legal Frameworks

Abstract

International Cooperation in Combating Cybercrime: An Analytical Study of Qatari Legislation and International Legal Frameworks

This article examines the legal frameworks in Qatar and international law on cooperation in the fight against cybercrime. It investigates the concept and transnational aspects of cybercrime, the Budapest Convention, the regional instruments, Qatar's Cybercrime Prevention Law and Code of Criminal Procedure and the modalities of mutual legal assistance, information exchange and extradition through descriptive, legal-analytical and comparative approaches. The analysis presents a legislative framework for cooperation that has been put in place by the State of Qatar, while implementation is hampered by differences in criminalisation, jurisdictional issues, procedural delay, unequal criminal technical capacity and the fluid nature of digital evidence. International and regional instruments offer important standards, but need to be implemented through swift communication, harmonised procedures and trained authorities. Finally, the article recommends that Qatar should focus more on operational coordination, regularly review its domestic legislation and provide more specialised Judicial, Prosecutorial and technical training.

Keywords: cybercrime; international cooperation; Qatar; mutual legal assistance; extradition

Povzetek

Mednarodno sodelovanje pri boju proti kibernetiki kriminaliteti: analitična študija katarske zakonodaje in mednarodnih pravnih okvirov

Članek analizira, kako katarska zakonodaja in mednarodni pravni instrumenti urejajo sodelovanje v boju proti kibernetiki kriminaliteti. Z deskriptivno, pravnoanalitično in primerjalno metodo obravnava pojem in čezmejne značilnosti kibernetike kriminalitete, Budimpeško konvencijo, regionalne instrumente, katarski zakon o preprečevanju kibernetike kriminalitete in zakonik o kazenskem postopku ter mehanizme medsebojne

pravne pomoči, izmenjave informacij in izročitve. Analiza ugotavlja, da je Katar razvil pomembno zakonodajno podlago za sodelovanje, vendar izvajanje omejujejo razlike v inkriminaciji, spori glede pristojnosti, postopkovne zamude, neenake tehnične zmogljivosti in nestanovitnost digitalnih dokazov. Mednarodni in regionalni instrumenti določajo bistvene standarde, njihova učinkovitost pa je odvisna od hitrega komuniciranja, združitvi postopkov in usposobljenih organov. Članek sklene, da mora Katar okrepiti operativno usklajevanje, redno posodabljati domačo zakonodajo ter razširiti specializirano usposabljanje.

Ključne besede: kibernetika kriminaliteta; mednarodno sodelovanje; Katar; medsebojna pravna pomoč; izročitev

1 Introduction

Rapid advances in technology and the growth of electronic communication have brought significant social and economic benefits, but have also given rise to new ways of committing crime remotely, quickly and across multiple jurisdictions. Individuals, institutions and states are threatened by cybercrime as the perpetrator, infrastructure, victim and evidence can be situated in different countries. National criminal law is thus not superfluous, but if it is to be effective, it needs procedures to be coordinated internationally. Qatar has enacted national laws relating to cybercrime and criminal procedure as well as international judicial cooperation. The effectiveness of this framework is however reliant on its relationship with international and regional instruments, particularly rules relating to preservation and disclosure of electronic evidence as well as rules relating to mutual legal assistance and extradition. The main question is whether these frameworks offer adequate, assimilable, and rights-based mechanisms for transnational cases, and whether these mechanisms are sufficiently quick.

International cooperation also depends on clear multilingual legal communication and specialised training. Mutual legal assistance requests, extradition files and digital-evidence reports require accurate terminology, contextualised writing and careful review. Research on legal translation, contextualised writing, feedback and digitally mediated instruction is therefore relevant to the preparation and assessment of cross-border legal documents (Alshehab and Rababah 2020; Rababah 2022; Rababah et al. 2023; Rababah 2023; Rababah and Rababah 2024).

1.1 Research Problem and Questions

The problem of the research is that Cybercrime is one of the most pervasive and complicated means of crime in the modern era because it uses technological means that transcend the geographical boundaries of states. This has led to many legal and practical issues, including jurisdiction, gathering digital evidence, timely arrest and prosecution of offenders and a system of cooperation between states. While the State of Qatar has made good efforts through legislation and other international agreements and legal instruments to combat cybercrime, there remain several practical issues regarding the effectiveness of international cooperation, variations in national legal and procedural systems and varying national response times, information sharing and the provision of legal assistance. It is also noted that most of the previous studies have focused either on the general aspects of cybercrime or only on its international or national dimensions. It is still a need to be fulfilled by a study that integrates an analysis of the legislation in Qatar and international legal bodies under a single analytical framework, focusing on mechanisms of international cooperation and the practical issues of implementation.

The study addresses the following principal question:

To what extent do international legal frameworks and Qatari legislation contribute to enhancing the effectiveness of international cooperation in combating cybercrime?

It also considers the following subsidiary questions:

1. What is meant by cybercrime and what are its most significant characteristics that distinguish it from traditional crime?
2. What are the principal national laws and regulations in the State of Qatar relating to combating cybercrime and to what extent are they adequate with regard to prosecution, investigation and evidentiary procedures?
3. What are the principal international legal frameworks and conventions governing international cooperation in combating cybercrime?
4. What are the mechanisms of international cooperation adopted in combating cybercrime, particularly mutual legal assistance and extradition?
5. What are the main legal and practical challenges facing the implementation of international cooperation in the field of cybercrime?
6. To what extent are Qatari legislation and international legal frameworks concerning combating cybercrime consistent with one another?

1.2 Significance and Objectives

The article contributes an integrated analysis of international legal instruments and Qatari legislation, a combination that remains limited in Arabic legal scholarship. Its practical value lies in identifying operational barriers that affect investigators, prosecutors, courts and policymakers when they seek information, electronic evidence or extradition across borders.

The study has four objectives:

- to clarify the legal concept of cybercrime and its distinction from traditional crime;
- to analyse the principal international, regional and Qatari rules governing cooperation;
- to evaluate mutual legal assistance, information exchange and extradition in practice; and
- to identify legal and operational reforms that could improve cooperation.

1.3 Literature Review and Research Gap

Kharashi (2015) examined obstacles to international cooperation against information crime and treated cooperation as indispensable because of the transnational character of the offences. The present article builds on that analysis by connecting international instruments with Qatar's domestic framework and by focusing on mutual legal assistance, electronic evidence and extradition.

Al-Qahtani (2016) analysed cybercrime in Gulf society and proposed a regional strategy based on legal, practical and cooperative measures. His study provides an important Gulf context, while the present article gives greater attention to the legal interaction between Qatari legislation and international rules.

Wasel (2023) examined international conventions, mutual legal assistance and extradition and identified differences among national legal systems as a major obstacle. Moise (2023) focused more narrowly on the Second Additional Protocol to the Budapest Convention and its procedures for cross-border electronic evidence. Together, these studies show the importance of both general cooperation rules and expedited evidence mechanisms.

The research gap lies in the limited integration of these international developments with a detailed assessment of Qatari law. This article also incorporates the United Nations Convention against Cybercrime adopted in 2024 and Qatar's 2026 ratification,

developments that materially change the international context for Qatar's cooperation obligations.

2 Methodology

This study adopts the descriptive-analytical approach by describing the conceptual and legal framework of cybercrime, identifying its characteristics and distinguishing it from traditional crime. It also reviews the Qatari legislation and relevant international legal frameworks.

The study further analyses relevant legal provisions and examines their effectiveness in combating cybercrime, with particular emphasis on international cooperation mechanisms, especially mutual legal assistance and extradition.

The study also employs the comparative approach to identify areas of convergence and divergence between Qatari legislation and international rules, with the aim of assessing the effectiveness of these legal frameworks in addressing cybercrime of a transnational nature.

The analysis is based on legislation, treaties, official institutional materials and published legal scholarship. It does not use original empirical or archival data. The United Nations Office on Drugs and Crime Cybercrime Repository was used as an additional documentary source for legal instruments and case-related materials (UNODC n.d.).

3 Cybercrime as a Legal Concept

Determining the concept of cybercrime is fundamental to understanding the legal nature of this type of crime, particularly in light of the diversity of its forms and the continuous development of the means by which it is committed. Differences in legal scholarship and legislation regarding the formulation of a unified definition have resulted in the emergence of several legal approaches seeking to clarify its meaning and identify its distinctive characteristics.

Scholarly and legislative definitions of cybercrime have varied as a result of the relatively recent emergence of this form of crime and the continuous development of the means used to commit it, as well as differences in legal approaches to determining its nature. One approach has viewed the computer and the Internet merely as means of committing the crime, while another has linked cybercrime to the object of the criminal conduct itself, namely the information system or electronic data. A third approach has attempted to combine the two perspectives.

3.1 Definitions Based on the Instrument of Crime

Some legal scholars have defined cybercrime on the basis of the means employed to commit it, considering the computer or the Internet to constitute a principal tool in the criminal activity.

Tiedemann described computer crime as unlawful or socially harmful conduct committed through a computer (Al-Qahtani 2016: 17). Ajoy (2024) similarly treats cybercrime as unlawful conduct in which computer technology or communication networks function as the instrument or target of the offence.

The researchers consider these definitions important in highlighting the central role of computers and the Internet in cybercrime. However, they place considerable emphasis on the means used in the criminal activity without giving sufficient attention to the nature of the object of the criminal attack, namely information systems, networks and data.

Some of these definitions are also characterised by considerable breadth, which may result in bringing certain traditional crimes within the scope of cybercrime merely because technological means were used in their commission.

So there is no exact and complete definition of cybercrime if it is looked at only in relation to computers or the Internet, given the constant evolvement of technology and the various ways in which cybercrime currently exists. Section 3.2 Definitions is derived from the Object of Crime. Those who support this view believe that cybercrime doesn't require a computer or the Internet to be used as a method of committing the crime. However, it also includes direct attacks on information systems and electronic data, which are the objects of legal protection. This method sees violations of information systems or electronic data as the engine of cybercrime, ranging from unauthorised access to modification and destruction, copying or disruption (UNODC 2013). It is helpful because it states that it protects legal interests of confidentiality, integrity and availability, and not just the device itself. An object-based definition is not complete as technology might be used to commit a traditional offence, but is not the offence itself. Therefore, offences involving an information system, network or electronic data as a means or an object of the crime should be included in a comprehensive definition. This integrated approach also reflects the different nature of cyber-dependent and cyber-enabled offences (Holt et al. 2022; United Nations 2024).

4 International Cooperation Mechanisms

In the subject of cybercrime, evidence and activities are not confined to the jurisdiction of a single State, and it is common to find evidence and services providers, as well as suspects outside the jurisdiction of the investigating state. International cooperation is thus required to transcend those geographical boundaries of national criminal procedure and to facilitate the preservation, disclosure, investigation and enforcement. The legal framework for transnational organised crime developed at the general level is applicable, however, procedures for gathering electronic evidence should be faster and more technically specific (Farouk 2008; United Nations 2000).

4.1 Rationale for Cooperation

Information sharing helps authorities to identify criminals, infrastructure and criminal networks before the evidence is deleted or moved. Mutual legal assistance and extradition facilitates prosecution where the offenders, victims, proceeds and servers are spread between jurisdictions. The coordinated preservation and collection process is used to preserve and collect electronic evidence that maintains its authenticity, integrity and admissibility.

- Common minimum standards limit the opportunities for offenders to take advantage of variations in the national level of criminalisation, jurisdiction and procedure. Addressing unequal investigative resources among states through capacity building, joint training and technical assistance.

4.2 Principal Mechanisms

The most important ways of working together are:

- bilateral, regional and multilateral treaties and memoranda of understanding;
- police-to-police and judicial information exchange via designated contact points;
- Rapid preservation and disclosure of subscriber, traffic and stored content information;
- joint investigations and letters rogatory;
- extradition and transfer or enforcement of sentences; and
- cooperation with service providers, technical assistance and training together.

These mechanisms are effective when central authorities are clearly established, communication lines are secure, legal thresholds are compatible, and the response time is short and privacy, due process and data protection are protected. Requests cannot be fulfilled on a formal basis if they are not timely submitted or evidence cannot be transferred legally.

5 Legal Frameworks for Cooperation

International, regional and national instruments establish the offences, procedures and safeguards through which cooperation is organised. Their relationship is especially important for Qatar because domestic cooperation provisions operate alongside Arab regional rules and emerging global instruments.

5.1 International and Regional Frameworks

The Budapest Convention was opened for signature in 2001 and remains a central international framework for substantive offences, procedural powers and international cooperation. Its cooperation chapter covers extradition, mutual assistance, expedited preservation and disclosure of data and a 24/7 network for urgent assistance (Council of Europe 2001). The First Additional Protocol addresses racist and xenophobic acts committed through computer systems (Council of Europe 2003).

The Second Additional Protocol, opened for signature in 2022, responds to the difficulty of obtaining electronic evidence held in other jurisdictions. It provides tools for direct cooperation with registrars and service providers, government-to-government disclosure, emergency assistance, joint investigations and video conferencing, subject to data-protection and rule-of-law safeguards (Council of Europe 2022; Moise 2023).

Earlier Council of Europe recommendations addressed computer-related crime, cross-border search and seizure, information exchange and criminal-procedure cooperation. Recommendation R (89) 9 encouraged legislative approximation for computer-related crime, Recommendation R (95) 13 addressed criminal procedural problems connected with information technology and Recommendation Rec (2001) 11 promoted cooperation against organised crime (Council of Europe 1989; 1995; 2001b).

The Malabo Convention combines cybersecurity, personal-data protection and electronic transactions and calls for judicial, security and technical cooperation among African states (African Union 2014). The Arab Convention on Combating Information Technology Offences provides regional rules on mutual legal assistance and extradition, including dual criminality, written or secure urgent requests and grounds for refusal under the law of the requested state (League of Arab States 2010).

The United Nations Convention against Cybercrime was adopted by the General Assembly on 24 December 2024. It establishes global rules for prevention, criminalisation, electronic evidence, international cooperation and technical assistance. Qatar signed the Convention on 25 October 2025 and ratified it on 4 February 2026, subject to declared reservations (United Nations 2024; United Nations Treaty Collection 2026). This ratification gives the present analysis immediate practical relevance because domestic procedures must support the Convention's cooperation mechanisms.

5.2 Qatari Legal Framework

Qatar's principal domestic instruments are Law No. 14 of 2014 Promulgating the Cybercrime Prevention Law and Law No. 23 of 2004 Promulgating the Code of Criminal Procedure. Together, they regulate cooperation, mutual legal assistance, extradition, letters rogatory and the handling of criminal judgments.

Cybercrime Prevention Law.

The competent authority shall provide mutual legal assistance and extradition to other states in accordance with the rules established by the Code of Criminal Procedure, bilateral or multilateral agreements to which the State is a party, or the principle of reciprocity. The Law further provides that a request for mutual legal assistance or extradition shall not be executed unless the laws of both the requesting and requested states criminalize the offence that is the subject of the request or a similar offence.

The Law establishes mechanisms for receiving requests for assistance or extradition. The Public Prosecutor is responsible for receiving such requests and referring them to the competent authority for execution. In urgent cases, requests may be transmitted through the International Criminal Police organisation (INTERPOL). They may also be transmitted directly by the competent foreign authorities to the competent authority in the

State. In such cases, the receiving authority must notify the Public Prosecutor. Requests and responses may be transmitted by mail or by any other means. In all cases, requests and their annexes must be accompanied by a summarized Arabic translation.

A request must identify:

- identification of the authority requesting the measures and the name of the prosecuting authority in the proceedings, where the case is pending before a court;
- the legal provision criminalising the conduct;
- the purpose of the request;
- any relevant observations and available details concerning the identity of the person concerned, including name, social status, nationality, address and any other information necessary to identify and locate the persons concerned; and
- details of the assistance requested and any specific procedures that the requesting state wishes to be undertaken. The Public Prosecutor or competent authority may request additional information from the competent foreign authority where such information is necessary for executing or facilitating execution of the request.

It identifies several forms of mutual legal assistance, including obtaining evidence from persons or taking their statements; conducting searches, seizures and confiscations; the expedited preservation of electronic data, information and subscriber information; the real-time collection of traffic data; the inspection of objects, premises and information systems; providing information and any other assistance useful for establishing the offence; providing expert reports; and any other form of assistance that does not conflict with the laws in force in the State (State of Qatar 2014: art. 30).

A request may be refused when it was issued by an incompetent authority, does not comply with applicable law, threatens security, sovereignty, public order or state interests, concerns a matter already pending or finally decided in Qatar, appears discriminatory, fails dual criminality or lacks sufficient safeguards for the accused (State of Qatar 2014: art. 31).

Articles 39–41 regulate extradition. Extradition may be denied where the request is discriminatory, the matter has been finally decided in Qatar, prosecution or punishment is barred or there is a substantial risk of torture or cruel, inhuman or degrading treatment. The law also permits refusal in specified pending-proceeding and humanitarian circumstances (State of Qatar 2014).

Code of Criminal Procedure.

The international cooperation framework under the Qatari Code of Criminal Procedure consists of a set of rules and mechanisms regulating cooperation between the State of Qatar and foreign states and authorities in combating crime, pursuing offenders and enforcing judgments, in a manner that serves the administration of criminal justice while safeguarding national sovereignty.

Among the principal frameworks are the following (State of Qatar 2004: book 5):

The provisions governing international judicial cooperation in the Code of Criminal Procedure regulate various forms of cooperation between Qatari judicial authorities and foreign and international judicial authorities in criminal matters, subject to applicable international agreements and the principle of reciprocity.

Cooperation involves, among other things, mutual legal assistance, execution of letters rogatory, transfer of judgments and enforcement of sentences, which help combat transnational crime, protect state sovereignty and the Qatari legal system. The Code prescribes the rules governing the transfer of convicted persons and accused persons to other States. It sets out conditions that must be met for extradition, such as "dual

criminality" which means that the offence must be punishable under both Qatari law and the law of the requesting state. It also sets out conditions for when extradition is not permissible, including if the individual being sought is a Qatari national, if the offence is political, or where it has previously been finally adjudicated. The procedures for filing an application for extradition, the competency to consider extradition requests, and procedures to protect the person sought and the right to appeal to the Court of Appeal against an extradition decision are also set out in the Code. International letters rogatory are also covered by the Code. It allows foreign authorities to ask for investigations or evidence to be collected within Qatar, through the Public Prosecutor, but subject to certain safeguards, with due consideration to public order and Qatari law. Foreign courts and public prosecution authorities, on the other hand, may seek judicial cooperation from the Qatari courts and public prosecution authorities for the conduct of judicial proceedings abroad, which will be recognised as valid when conducted in accordance with the law in force in the State in which the judicial proceedings are carried out.

The Code establishes provisions governing the transfer and enforcement of sentences and the transfer of convicted persons between Qatar and foreign states, whether by transferring a Qatari convicted person to Qatar to serve the sentence or transferring a foreign convicted person to his or her state of nationality to serve the sentence. Such transfer requires the consent of the convicted person, a final judgment and compliance with the fundamental principles of the Qatari legal system.

The Code also regulates the system of controlled delivery, which permits objects derived from or used in the commission of a crime to cross borders under the supervision of competent authorities for the purpose of detecting crimes and apprehending offenders (State of Qatar 2004: arts. 407–443).

6 Discussion

The researchers consider that, despite the diversity of international cooperation mechanisms in combating cybercrime—including mutual legal assistance, information exchange, extradition and judicial assistance—the effectiveness of these mechanisms in practice remains subject to legal and scholarly debate.

From a practical perspective, international cooperation has contributed to uncovering numerous transnational criminal networks and has assisted in tracing digital transactions and cyberattacks and exchanging technical evidence among states.

These have helped to improve the capacity of competent authorities to go after criminals and limit their capacity to escape criminal liability. The technical and legal skills of states to handle cybercrime have also been enhanced through international conventions and joint security coordination, especially given the quick evolution of the communications technologies of the modern world. However, actual implementation also presents some weaknesses that can hinder the effectiveness of such mechanisms. The speed at which 'digital evidence' can be deleted or transferred electronically is one of the most important issues, and may lead to its loss or other problems in obtaining it, because of the difficulties involved with international judicial cooperation and the delays involved. Variations in the definition of cybercrime and differences among national laws could also make it difficult to implement requests for judicial assistance or extradition. Also, some state authorities could invoke the doctrine of national sovereignty as a basis of refusing to provide information and/or return a person. Moreover, state differences in technological capacity are still a major hurdle. Not all states have the technical infrastructure and specialized expertise to properly address digital evidence with complex needs. This imbalance can have a negative impact on the effectiveness and efficiency of international cooperation on this type of crime. One of the key components of cooperation on cybercrime cases is time. Subscriber data and traffic information, as well as content in the

cloud, can be kept for a restricted duration, be modified automatically, and may be transferred to a different jurisdiction. A request which is legally valid but is sent too late can thus be rendered ineffective. There needs to be a staged response to effective cooperation: immediate preservation to ensure that evidence is not deleted; fast disclosure in the event of an emergency threshold and formal mutual assistance for the use of evidence in proceedings. There are complementary pathways for these stages in the Budapest framework, its Second Additional Protocol and the United Nations Convention (Council of Europe 2001a; 2022; United Nations 2024). Applying dual criminality must be handled with caution. It ensures state sovereignty by restricting coercive assistance to actions that are recognised as criminal in both jurisdictions – but a too technical comparison of offence labels can create impediments to legitimate requests. Police should compare the conduct and protected interests, and not the exact wording of the statute. This is especially significant in cases where one state has an offence specific to a certain type of technology, while another has a general fraud/forgery or unauthorised-access offence. In such cases, templates for requests should be drafted so as to describe the conduct, the system and data involved, the alleged harm, and the legal basis for the measure requested. Procedural rights must also be maintained in the process of cooperation. Direct disclosure, emergency channels and joint investigations will help to speed up operations, but should be subject to legality, necessity, proportionality, data protection and an effective remedy. The legislation already allows for refusal of discriminatory requests and requests which would pose a serious risk of torture or degrading treatment in Qatar. The same rights-based assessment process as outlined above should be applied to requests for electronic evidence, covering the nature of the evidence requested, the time frame and the level of confidentiality and any limitations on future access. Lastly, the success of the agreement should be assessed by what it actually accomplishes, not by the number of agreements accomplished. The data collected and analysed by the agency are based on relevant indicators such as the average time to preserve and disclose data, proportion of requests that need clarification, reasons for refusal, number of urgent requests, and proportion of transferred evidence that is accepted by courts. This would assist Qatar to find out the bottlenecks in the procedure, training requirements and frequently occurring conflicts of law issues without sharing sensitive information about the case. The comparison shows significant congruence between Qatar's legislation and the primary cooperation principles in international instruments dual criminality, central transmission channels, mutual assistance, preservation of electronic data and extradition safeguards. It's an operational, not conceptual, weakness. Formal requests might still be too slow, and direct interaction with service providers could need better procedures, language rules and safeguards for data protection. The ratification of the United Nations Convention against Cybercrime in Qatar provides a chance to review the implementation and institutional responsibilities and reservations in a single programme. It establishes an international framework for the cooperation that is not limited to the states involved in the Budapest convention or the Arab convention. To be effective, there must be clear regulations, trained contact points, safe request systems and regular checks of response times and results. 7 Conclusion Cybercrime is transnational because criminals can be spread across multiple countries, victims, evidence and infrastructure can be spread across countries and multiple countries. However, Qatar has put in place a well established internal regime and it is now part of a wider international regime through its adherence to the United Nations Convention against Cybercrime. The final hurdle is to turn legal powers into efficient, technically skilled, rights-based collaboration.

7.1 Findings

- International cooperation is indispensable for preserving evidence, identifying offenders and conducting proceedings across borders.

- Qatari law provides a legal basis for mutual assistance and extradition and contains important grounds for refusal and individual safeguards.
- Differences in national law, jurisdiction, terminology and institutional capacity continue to delay cooperation.
- Electronic evidence requires procedures that operate more quickly than traditional judicial-assistance channels.
- The 2024 United Nations Convention and Qatar's 2026 ratification materially strengthen the framework for future global cooperation.

7.2 Recommendations

- Adopt implementing rules that clearly assign responsibilities under the United Nations Convention against Cybercrime and coordinate them with existing Qatari law.
- Develop secure, standardised and multilingual templates for urgent preservation, mutual assistance and extradition requests.
- Review cybercrime and criminal-procedure legislation periodically to address new technologies and emerging forms of electronic evidence.
- Expand specialised training for judges, prosecutors, investigators, digital-forensics experts and legal translators.
- Strengthen cooperation with service providers and foreign contact points while maintaining privacy, due-process and data-protection safeguards.

References

- Ajoy, P. B. (2024): Developing an Analytical Definition of Cybercrime. *IOSR Journal of Humanities and Social Science*, 29 (1, Series 6): 12–19. <https://doi.org/10.9790/0837-2901061219>.
- Al-Qahtani, M. S. (2016): Cybercrime in Gulf Society and Means of Combating It. Riyadh: General Secretariat of the Cooperation Council for the Arab States of the Gulf.
- Alshehab, M. H., and Rababah, L. M. (2020): Lexical Legal Problems Committed by Translation Students When Translating English Legal Sentences into Arabic at Jadara University in Jordan. *Asian EFL Journal Research Articles*, 27 (2.2): 193–215.
- Farouk, A. (2008): International Cooperation in Combating Money Laundering Proceeds Derived from Organised Crime and Drug-Related Offences in Light of International Law. Unpublished doctoral dissertation. Alexandria: Faculty of Law, Alexandria University.
- Holt, T. J., Bossler, A. M., and Seigfried-Spellar, K. C. (2022): Cybercrime and Digital Forensics. New York: Routledge.
- Kharashi, A. A. A. (2015): Problems of International Cooperation in Combating Information Crimes and Means of Overcoming Them. Alexandria: Dar Al-Jami'a Al-Jadida.
- Moise, A. C. (2023): Procedural Aspects of the Second Additional Protocol to the Convention on Cybercrime. *Bulletin of the Transilvania University of Braşov, Series VII: Social Sciences and Law*.
- Rabah, L. M. (2022): Contextualization to Enhance Students' Writing Ability. *Theory and Practice in Language Studies*, 12 (11): 2316–2321. <https://doi.org/10.17507/tpls.1211.11>.
- Rabah, L. M. (2023): Stepping into Language Mastery: Virtual Reality Simulations as Catalysts for EFL Pronunciation Enhancement. *Journal of Applied Learning and Teaching*, 6 (Special Issue 1): 110–122. <https://doi.org/10.37074/jalt.2023.6.S1.10>.
- Rabah, L. M., Al-Shboul, O. K., and Banikalef, A. A. (2023): Examination of the Use of Feedback in EFL Writing Instruction: A Case Study of Jordan. *Journal of Language Teaching and Research*, 14 (1): 263–268. <https://doi.org/10.17507/jltr.1401.28>.

- Rababah, L. M., and Rababah, M. A. I. (2024): Online Social Learning and Instructional Presence: Enhancing English Education at a Jordanian University. *Forum for Linguistic Studies*, 6 (6): 729–741. <https://doi.org/10.30564/fls.v6i6.7430>.
- Wasel, S. G. (2023): International Cooperation in Combating Cyber Crimes. *Journal of Law and Emerging Technologies*.

Sources

- African Union (2014): African Union Convention on Cyber Security and Personal Data Protection.
- Council of Europe (1989): Recommendation No. R (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime.
- Council of Europe (1995): Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology.
- Council of Europe (2001a): Convention on Cybercrime, ETS No. 185.
- Council of Europe (2001b): Recommendation Rec (2001) 11 of the Committee of Ministers to Member States Concerning Guiding Principles on the Fight against Organised Crime.
- Council of Europe (2003): Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, ETS No. 189.
- Council of Europe (2022): Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, CETS No. 224.
- League of Arab States (2010): Arab Convention on Combating Information Technology Offences.
- State of Qatar (2004): Law No. 23 of 2004 Promulgating the Code of Criminal Procedure.
- State of Qatar (2014): Law No. 14 of 2014 Promulgating the Cybercrime Prevention Law.
- United Nations (2000): United Nations Convention against Transnational Organized Crime.
- United Nations (2024): United Nations Convention against Cybercrime. General Assembly Resolution 79/243, 24 December 2024. Available from: <https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html> (Accessed 15.10.2026).
- United Nations Office on Drugs and Crime (2013): Comprehensive Study on Cybercrime. Vienna: United Nations.
- United Nations Office on Drugs and Crime (n.d.): Cybercrime Repository. Available from: <https://sherloc.unodc.org/cld/en/st/home.html> (Accessed 15.10.2026).
- United Nations Treaty Collection (2026): United Nations Convention against Cybercrime: Status of Treaties. Available from: https://treaties.un.org/pages/ViewDetails.aspx?chapter=18&clang=_en&mtdsg_no=XVIII-16&src=TREATY (Accessed 15.10.2026).