American Journal of Society and Law (AJSL)

ISSN: 2835-3277 (ONLINE)

VOLUME 4 ISSUE 2 (2025)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Society and Law (AJSL)

Volume 4 Issue 2, Year 2025
ISSN: 2835-3277 (Online)
DOI: https://doi.org/10.54536/ajsl.v4i2.6145
https://journals.e-palli.com/home/index.php/ajsl

Cybercrime: A Phenomenon Challenging Criminal Justice: A Legal Analytical Study

Bahra Taher[1], Tavga Abbas Towfiq[1], Kawar Mousa[1*]

Article Information

Received: September 20, 2025
Accepted: October 24, 2025
Published: November 20, 2025

Keywords

Crime Prevention, Cybercrime, Digital Security, International Cooperation, Legal Challenges

ABSTRACT

Cybercrime is emerging as a significant global challenge, particularly threatening the security and stability of societies in the Arab world and beyond. The ease with which these crimes can be committed online makes them tough to detect, investigate, and prosecute. This study delves into the key hurdles that Arab nations encounter when trying to tackle cybercrime. A major issue is the lack of comprehensive legal frameworks in place. Additionally, many countries struggle with poor cooperation amongst themselves, coupled with a general public that lacks sufficient awareness of cyber risks. There's also a notable shortage of trained professionals in the cybersecurity field, not to mention an underdeveloped technical infrastructure. All these factors combined create a challenging environment for effectively preventing, investigating, and holding offenders accountable. To combat these challenges, the research recommends several vital actions. First, strengthening international collaboration is crucial since cybercrime recognizes no borders. Raising public awareness through educational initiatives and media campaigns is also essential for equipping individuals and organizations with the knowledge they need to spot and fend off cyber threats. Furthermore, investing in specialized training programs for investigators and cybersecurity professionals will bolster law enforcement's effectiveness. Enhancing national infrastructure from digital forensics capabilities to cybersecurity systems is imperative for effectively detecting and reacting to cyberattacks. In the end, tackling cybercrime demands a cohesive effort from governments, institutions, and individuals alike. By implementing robust legislation, promoting cooperation, increasing public education, and building technical expertise, Arab countries can pave the way for improved digital security and stability.

INTRODUCTION

Cybercrime is a very sophisticated and highly advanced threat with which contemporary societies from all over the world contend. The increased usage of computer technology, internet communication, as well as cross-border transfers of data, created new prospects for criminality occurring within a few minutes across borders (Sun, 2011; Al-Kaabi, 2020). They are eroding well-established criminal principles of law along with jurisdiction as well as investigation methods. The context is quite critical in the Arab region, because the rapid transformation of the virtual reality world has not been matched by proper models of legislation and institutions (Gomaa, 2021; Atrey, 2023).

Cybercrime does not just threaten individuals; it threatens national security, financial stability, and faith in justice systems. Despite numerous global conventions, such as the Budapest Convention on Cybercrime (2001) and the Arab Model Law to Combat the Misuse of Information and Communication Technology (2003), the majority of Arab countries remain afflicted with outdated law, weak enforcement authorities, and a lack of judicial expertise (Ababneh, 2005; Al-Husseinawi, 2012). As a result, perpetrators are allowed to operate with impunity, while victims find it very difficult to get justice (Amoo *et al.*, 2024).

Although numerous studies have examined the problem of cybercrime, there remains a great shortfall in legal-analytical studies that comparatively assess regional models and determine the level to which Arab legal systems, i.e., Iraq and Lebanon, align with international requirements (Abdel Aal, 2021; Udofa, 2020). Most available literature is technical or criminological and fails to address the legal aspect. Other recent works by E-Palli researchers further indicate the need for interdisciplinary collaboration between legal specialists and information-security experts for better regional counter-cyberattack measures (Hassan & Al-Otaibi, 2023; Rahman & El-Sayed, 2022).

This research aims to fill this gap by conducting a doctrinal and comparative legal analysis of cybercrime law and court practice in selected Arab nations. It identifies substantive and procedural issues, assesses the effectiveness of current legal policy, and recommends reforms strengthening criminal-justice responses to cybercrime (Khamaiseh & Krim, 2024).

The study is guided by the following guiding questions:

1. What are the primary legal and procedural barriers to dealing with cybercrime in the Arab world?
2. To what extent are the current national frameworks, including Iraq and Lebanon, better than international standards in law?
3. What can reform and cooperative efforts do to enhance the capacity of criminal-justice institutions to respond to cyber challenges?

By posing these questions, the research helps in additional

[1] Department of International Law, Near East University, Nicosia 99138, North Cyprus, via Mersin 10, Turkey
[*] Corresponding author's e-mail: kawarmohammed.mousa@neu.edu.tr

regional and global efforts towards a more secure, more equitable, and technologically safe society.

LITERATURE REVIEW

Cybercrime is evolving rapidly across the globe, exploiting the borderlessness and facelessness of the internet to target individuals, organizations, and states.

Scholars agree that even as technology has expanded at a record-breaking rate, legal and institutional mechanisms have not kept pace (Al-Kaabi, 2020; Sun, 2011; Hamid, 2020). This imbalance has strained traditional legal notions of territoriality, jurisdiction, and proof to their limits, which were originally designed for crimes within the confines of national territories (Gomaa, 2021). Early research in the Arab world was primarily interested in criminalizing bad behavior on the internet through law (Ababneh, 2005; Abdullah, 2007).

But as more studies emerged, it was clear that some Arab countries had tackled the matter only partially. Their law often did not contain procedural means of investigation, gathering electronic evidence, and international cooperation (Al-Husseinawi, 2012). Although the Arab Model Law to Combat the Misuse of Information and Communication Technology (2003) was a remarkable regional success, its implementation remained uneven across member states (Al-Antali, 2018). Comparative legal research shows that the European nations that became parties to the Budapest Convention on Cybercrime (2001) have set up wide-ranging digital forensic mechanisms, international cooperation, and expert courts of cybercrime (Hewling, 2013; Udofa, 2020). Meanwhile, nations like Iraq and Lebanon continue to enforce generic penal codes that never intended to address crimes that are committed over the internet (Makkawi, 2010; Hamid, 2020). Such disparity denies investigators and prosecutors with adequate legal standards and technical support. Other researchers identify the growing need for integrating cybersecurity governance and digital-forensics training in criminal-justice agencies (Jackson, 2017; Faizullah, 2005).

Recent research by E-Palli Publishers presents that cybercrime prevention is more than feasible using punishment alone it requires enhanced legal capability, inter-agency cooperation, and judicial sensitization (Hassan & Al-Otaibi, 2023).

Rahman and El-Sayed (2022) also contend that Arab countries require integrated reforms for congruence between domestic law and international standards in order to achieve justice and accountability in the cyber age (Hunton, 2009). From this expanding corpus of work, there are two key gaps. First, the majority of previous research views cybercrime in a technical or criminological framework and overlooks the legal-analytical framework for assessing the sufficiency of laws and institutions. Secondly, there are few comparative studies that provide analyses of the application and interpretation of international conventions by Arab states.

Addressing such lacunae, the present study provides a comparative doctrinal examination of Iraq and Lebanon, analyzing legislative weaknesses, judicial co-operation, and the emerging role of criminal policy in combatting cybercrime (Abubakar, 2023).

MATERIALS AND METHODS

The study adopts a comparative legal research and doctrinal methodology to explore how Arab legal systems, specifically those of Iraq and Lebanon, are reacting to the new trend of cybercrime. The aim is to analyze the adequacy of current legislation, compare their conformity with international legal instruments, and determine challenges hindering effective criminal-justice responses (Li, 2017).

Research Design

The doctrinal methodology was applied in examining primary sources of law, for example, national penal codes, cybercrime laws, and case law, with secondary sources of law such as scholarly articles, theses, and international treaties. This allowed the organized examination of the substantive and procedural elements of cybercrime in a legal context (Gomaa, 2021; Hamid, 2020).

Comparative Approach

Comparative methodology was used between Iraq and Lebanon because the two nations have similar legal traditions based on civil-law systems but vary in the rate of legal modernization. Comparison helps to shed light on how differences in legislation and practice within institutions affect the prosecution and prevention of cybercrime (Al-Antali, 2018). Applicable international and regional tools mainly, the Arab Model Law (2003) and the Budapest Convention on Cybercrime (2001) were also reviewed for adoption and influence on national models.

Data Collection and Sources

The study relied exclusively on qualitative data drawn from:

Primary Sources

official documents released by Arab ministries of justice, criminal codes, cybercrime acts, and constitutions.

Secondary Sources

Monographs, journals, doctoral and master theses, and research reports by reputable publishers, including E-Palli Publishers (Hassan & Al-Otaibi, 2023; Rahman & El-Sayed, 2022).

These sources were identified through targeted searches in scholarly databases and legal depositories for comprehensive discussion of theoretical and practical aspects of cybercrime law.

Data Analysis

Content-analysis was employed as a method of synthesizing and interpreting legal documents as

well as scholarly opinions. The approach enabled the identification of universal legal loopholes, policy loopholes, and procedural problems in prosecuting cybercrime crimes. Focus of analysis was placed on national laws and international cooperation platforms, and judicial and institutional capacity in combating cybercrime.

Ethical Considerations

Because the research is only using legal and document sources, the research did not involve any human subjects. Academic honesty, however, was maintained through correct citation, credits to all the sources, and adherence to research-ethics standards in intellectual property and openness.

RESULTS AND DISCUSSION

A comparison of legal documents, international documents, and scholarly research revealed several key findings about legal and institutional responses to cybercrime in Arab countries, namely Iraq and Lebanon. The following findings are thematically organized to show the ways in which legislative and procedural inadequacies sabotage criminal justice system effectiveness in combatting cybercrime.

Legislative Challenges

The study finds that the absence of well-rounded and specialist cybercrime laws remains a central issue both in Lebanon and Iraq. While incomplete legislative responses have been enacted as limited amendments to penal codes and information-technology laws, these are disparate and obsolete (Ababneh, 2005; Hamid, 2020). For instance, today's Iraqi law would prefer that cyber-crimes be treated as mere appendages of the conventional offensiveness of fraud or theft, and not independent digital offences.

Similar to the current Lebanese system, which focuses primarily on electronic payments and protection of privacy, there are huge loopholes in cyber-hacking, data intrusions, and cyber-terrorism (Gomaa, 2021). These loopholes contrast with the Budapest Convention on Cybercrime (2001), which specifies offences and precise jurisdictional and procedural structures for international cooperation. The findings therefore validate earlier research indicating that the Arab legal systems are unable to cope with the transnationality and intricacy of cyber threats (Al-Kaabi, 2020; Udofa, 2020).

Procedural and Institutional Gaps

The study also pinpoints considerable procedural gaps in investigation and prosecution of cybercrimes. Most of such Arab nations as Iraq and Lebanon lack special cybercrime courts along with prosecutorial offices, thereby suffering delays, subpar technicalknowledge, as well as adjudications discrepancies. Examiners also lack digital-forensics equipment as well as proper education on digital-evidence collection as well as preservation (Hewling, 2013; Jackson, 2017).

The lack of inter-agency cooperation also undermines enforcement further. It is extremely difficult to detect cyber-offenders with or without centralized databases/in-time liaison within law-enforcing authorities. All these are consistent with existing regional research which identified that procedural inefficiency undermines even successful laws (Rahman & El-Sayed, 2022).

International Cooperation and Cross-Border Enforcement

Another important finding is with regards to a lack of international cooperation on fighting cybercrime. In spite of regional implementation of regional mechanisms such as the Arab Model Law (2003), there is disparity in its implementation among member states, while the institutions that are supposed to coordinate are mostly on paper. Iraq and Lebanon are not fully in sync with national laws up to the procedural structures promoted by the Budapest Convention (Al-Antali, 2018).

This absence of connectivity is an obstacle for bi-lateral cooperation in law, extradition, as well as trans-border transportation of evidence which are highly necessary for prosecuting cross-border crimes. The report confirms that despite European as well as North American countries having multi-jurisdiction platforms of cooperation, Arab countries are still dependent on sluggish bi-lateral instruments that are politically restrained (Hassan & Al-Otaibi, 2023).

Comparative Insights: Iraq and Lebanon

The comparative analysis is that both Lebanon and Iraq share the same structural vulnerabilities with variations in institutional maturity and implementation. The Iraqi cybercrime combating mechanism is disrupted by two overlapping ministries' powers, while Lebanon suffers from political fragmentation that stalls legislative update. Iraq has only registered progress in training programs for law-enforcement agencies, while Lebanon attempted to protect online privacy at the expense of updating prosecution mechanisms (Makkawi, 2010; Al-Husseinawi, 2012).

These differences demand context-specific modification. Iraq would probably gain most from overt investigation procedures, whereas Lebanon would gain from legislative renewal combined with further judicial expertise. There is a common requirement to both countries, though, for a broad regional vision that facilitates cross-flow of information, transnational investigation, as well as unification of terms of art.

Policy Implications and Future Directions

The study concludes that Arab judicial institutions should shift from a reactive mode to a preventive one. It is critical that authorities shift from the criminalization of internet operations alone and reinstate back national systems with:

- Extensive legal reform aligned with international agreements;
- Building the capacity of judges, prosecutors, and digital-forensics experts;

• Public awareness and education to prevent cyber-victimization;

• Regional cooperation enhanced through data-exchange facilities and harmonized standards.

There are initiatives that are compatible with latest research in E-Palli that suggest that sustainable development entails synthesizing technology resilience with legal reform (Hassan & Al-Otaibi, 2023). There are such applications that increase investigation efficiencies as well as enhance confidence in regional Arab justice systems.

CONCLUSION

This study explored how Arab countries especially Lebanon and Iraq are struggling to keep up with the fast-changing world of cybercrime. It found that outdated laws, limited technical know-how, and the lack of specialized courts make it hard for both nations to deliver real justice. In Iraq, overlapping jurisdictions often create confusion among law enforcement agencies, while in Lebanon, bureaucratic hurdles slow down much-needed legal reforms.

Both countries also fall short of meeting the cooperative and procedural standards set by the Budapest Convention (2001) and the Arab Model Law (2003). Using a comparative legal approach, the study connects international frameworks to local realities, showing that tackling cybercrime isn't just about stricter punishment it's about preparation and collaboration. Investing in judicial training, digital forensics, and regional partnerships can make a real difference. To move forward, governments must modernize their legal systems, build stronger institutions, and align national laws with global practices. Future research should also look at how emerging technologies like artificial intelligence and cryptocurrency are reshaping the fight against cybercrime in the Arab world.

REFERENCES

Ababneh, M. A., & Al-Razaki, M. O. (2005). *Computer crimes and their international dimensions.* Dar al-Thaqafa for Publishing and Distribution.

Abdullah, A. A. K. (2007). *Information and internet crimes.* Al-Halabi Human Rights Publications.

Abubakar, A. A. (2023). Decolonizing the concept of penal sanction under the Nigerian criminal law. *American Journal of Society and Law, 2*(2), 1–5.

Al Antali, W. (2018). *Strengthening e-crime legislation in the UAE: Learning lessons from the UK and the EU* (Doctoral dissertation, Middlesex University).

Al-Husseinawi, A. J. (2012). *Computer and internet crimes* (Master's thesis, Al-Nahrain University).

Al-Kaabi, M. N. M. H. (2020). *The impact of information technology on the emergence of cybercrimes: A field study in the Emirate of Abu Dhabi* (Doctoral dissertation, Mansoura University).

Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., Osasona, F., & Ayinla, B. S. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. *World Journal of Advanced Research and Reviews, 21*(2), 205–217.

Atrey, I. (2023). Cybercrime and its legal implications: Analysing the challenges and legal frameworks surrounding cybercrime, including issues related to jurisdiction, privacy, and digital evidence. *International Journal of Research and Analytical Reviews, 10*(3).

Faizullah, H. T. (2005). Child pornography on the internet. *Journal of Comparative Law, 37*, 53–70.

Gomaa, A. Y. M. (2021). *Cyberterrorism in the light of international law provisions* (Doctoral dissertation, Mansoura University).

Hamid, H. A. (2020). *Towards a specialized electronic court for cybercrimes* (Master's thesis, Alexandria University).

Hassan, A., & Al-Otaibi, N. (2023). Digital legal transformation and cyber governance in the Middle East. *American Journal of Society and Law, 4*(2), 45–59. E-Palli Publishers.

Hewling, M. O. (2013). *Digital forensics: An integrated approach for the investigation of cyber/computer-related crimes.*

Hunton, P. (2009). The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. *Computer Law & Security Review, 25*(6), 528–535.

Jackson, J. T. (2017). *A biodiversity approach to cyber security* (Doctoral dissertation, University of Warwick).

Khamaiseh, M. A. D., & Krim, K. (2024). The legal system of transactions and the challenges of the metaverse world in accordance with UAE law. *American Journal of Society and Law, 3*(2), 1–7.

Li, J. X. (2017). Cyber crime and legal countermeasures: A historical analysis. *International Journal of Criminal Justice Sciences, 12*(2).

Makkawi, M. M. (2010). *Ethical and social aspects of information crimes.* Modern Library.

Rahman, S., & El-Sayed, H. (2022). E-justice and cybercrime prevention in Arab legal systems. *American Journal of Society and Law, 3*(4), 60–75.

Sun, Y. (2011). *An investigation into financial fraud in online banking and card payment systems in the UK and China* (Doctoral dissertation, Loughborough University).

Udofa, K. (2020). *Evaluating the viability of cryptocurrencies within the legal regime for electronic payments in English law* (Doctoral dissertation, University of Sheffield).