

Cybercrimes: Challenges and Ways to Overcome Them in Criminal Law and Islamic Jurisprudence

- 1- Enad Ahmed Abdullah Talafheh*, Faculty of Law, Irbid National University, enadtalafheh@gmail.com, e.talafha@inu.edu.jo.
- 2- Rafat A'yesh Issa Aldghaim, Faculty of Law, Irbid National University, dghematr@gmail.com.
- 3- Akram Musleh Bani Mustafa, Faculty of Law, Irbid National University, A.Banimostafa@inu.edu.jo.
- 4- Khaled Ahmad Rasheed Amayreh, Faculty of Law, Irbid National University, Kh.alamaireh@inu.edu.jo.
- 5- Fadel Abdelrahman Taha Khasawneh, Faculty of Law, Irbid National University, f.khasawneh@inu.edu.jo.
- 6- Amin Waheed Hilal Al-Daggamseh, Faculty of Law, Irbid National University, aldaggamsehamin@gmail.com.

Corresponding Author: Enad Talafheh, enadtalafheh@gmail.com, e.talafha@inu.edu.jo.

Abstract

The article analyzes the complexities of cybercrimes and the challenges faced in their governance through contemporary criminal law and Islamic jurisprudence. The background and significance of the problem are discussed prior to elaboration on the contemporary Muslim-majority societies' legal framework. In this regard, the need for the dual-track legal system is discussed at length, based on religious and secular courts. Using both doctrinal and comparative methods, some of the challenges faced in bridging the gaps between the universally accepted penal principles and those derived from Sharia in the context of the admissibility of digital evidence and other offense definitions are analyzed. The proposed IDEF3 modeling approach considers the various system interfaces required for processes such as the identification and investigation of criminal acts, as well as the adjudication and imposition of punishment. The model incorporates the need for multidisciplinary work and a code of ethics and offers preventive measures. The results of this study showed that in the quest for an efficient anti-cybercrime framework grounded in the principles of justice and welfare, the combination of the various Islamic legal tenets in furtherance of the objective of moral responsibility is vital. Keywords: Cybercrime, Criminal Law, Islamic Jurisprudence, IDEF3 Modeling, Digital Evidence, Sharia Courts

Keywords: Cybercrime, Criminal Law, Islamic Jurisprudence, IDEF3 Modeling, Digital Evidence, Sharia Courts

INTRODUCTION

Background and Significance

Cybercrime is the use of technology to harm an individual, business, government, or institution. It is a relatively new field stemming from the use of technology to harm an individual,

business, government, or institution (Al-Salamat et al., 2023). Technically, cybercrime includes unlawful acts or criminal behaviors committed through the Internet and computer networks, for example, hacking, identity theft, cyberterrorism, and the use of cyberattack tools and software known as 'Peeling Programs' (Gharaibeh & Ibrahim, 2024; Goudjili, 2023). Given that the modern world is extremely dependent on digital infrastructures for communication, trade and governance, digital criminals utilize the criminal opportunities offered by the Internet to the maximum extent possible (Ababneh et al., 2024). With cybercrime crossing borders and operating at an international level, adopting the necessary laws within national legal frameworks is becoming more and more of a challenge (Jarrah, 2025; Al-majali, 2024).

Mass integration of internet technologies has heavily altered societal conduct and interactions. The Internet has transformed communication by removing barriers of both geography and other types (Al-Fulaij et al., 2022). The use of email, social media, video calls, and messengers removes the difficulty of sending messages over long distances (Abolouz, 2024). In addition, the use of internet technologies has been adopted by nearly all government and local agencies and businesses in improving the efficiency of management, control, and reporting systems (Dahiyat, 2019; Almatarnah et al., 2025). These technologies are geared towards improving the efficiency of finding a resolution to social, economic, and environmental problems (Ayasreh, 2024).

Using Internet technologies in government institutions is centered on the ability to manage electronic documents. This process leads to a faster and safer transfer of documents between institutions, businesses, and individuals. This helps reduce the burden of bureaucracy and corruption (Alahmed et al., 2023). As mentioned earlier, the use of technologies poses a risk. This is because of their numerous advantages and disadvantages. The greatest of these disadvantages is the matter of security and ethics (Al-Tuwaijry, 2024; Alkhawaldeh et al., 2023). Together with the development of science and technology, new challenges and crimes come into existence. Today, cybercrime is an ever-evolving field that outsmarts legislation, both national and international. Cybercrime poses a threat to the international community since the classification, detection, and countermeasures for cybercrime are still developing fields (Fetais & Abu Rahajab, 2024).

In relation to key terminology, two concepts need to be addressed: cyber-related and cyber-forming crimes (Betar & Murtaza, 2022). Cyber-related crimes include criminal acts facilitated by special equipment (computers, computer networks, and other means of communication) and include the distribution of computer viruses, hacking of servers, or other acts to capture control of network infrastructure or web pages. Such crimes are targeted towards the destruction of computer and network resources (Alsayed 2023). Cyber-forming crimes are more traditional types of crimes that also occur through the use of computers, computer networks,, and other means of communication. In contrast to the previous type, this type of crime can be perpetrated without the specific tools (Jarrah et al., 2025; Elmorchid et al., 2023). The importance of the fight against cybercrime complements the importance of adherence to the main principles of the legal framework, which is most apparent in Islamic jurisprudence (Mohammad Aljawarneh et al., 2024). In Islamic Law (Sharia), the main sources are the Quran and the Sunnah and are further elaborated by ijma and qias (Elgedawy, 2023). Traditionally, all Islamic jurisprudence supported the imposition of specific penalties for the crimes for which there is information (hudud) in the primary sources while allowing flexibility for the crimes for which there is no information in the primary sources (Elbasri, 2024). With the rising trends of globalization and digitalization, Muslim countries are confronted with the obligation to modernize the existing age principles of law to meet the growing demands of the fight against cybercrime (Issa, 2025; Al-Amoush, 2024).

Purpose and Scope

In this article, the study aims to identify the key issues in combating cybercrime by analyzing criminal law and Islamic jurisprudence. (Fig.1).

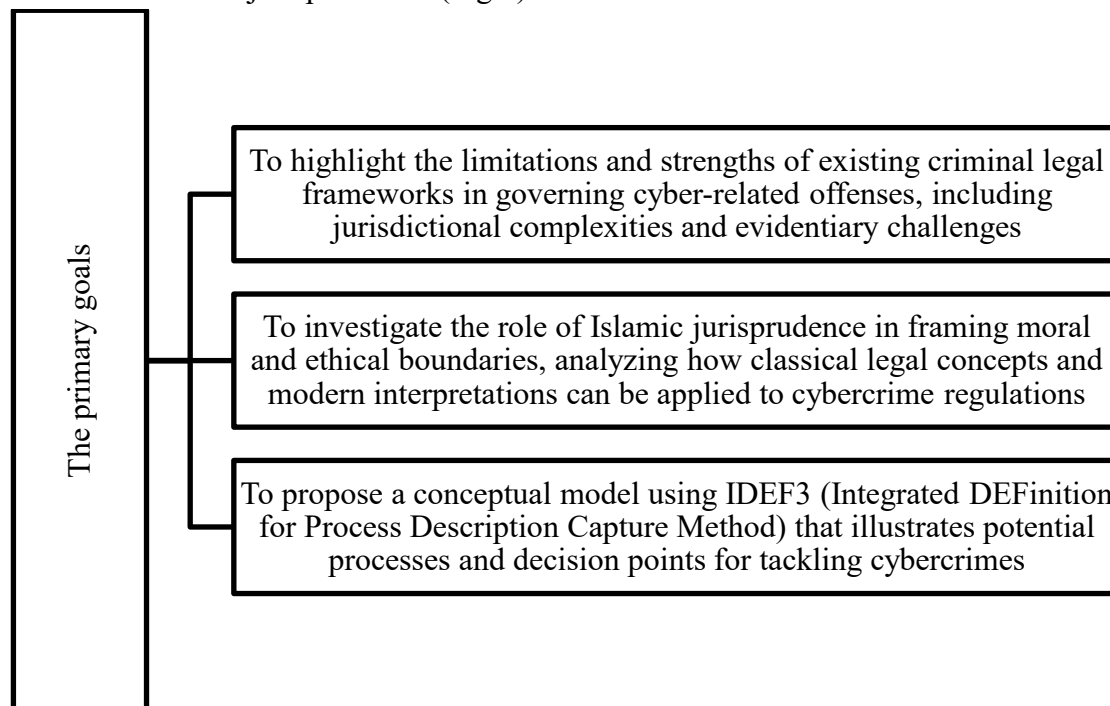


Figure 1. The primary goals

This study constructs the integration of faith-based legal views with the problems of the modern age to identify gaps in the literature. The results of this study will further the scholarly debate on the significance of balancing social values and legal traditions and the challenge of meeting the demands of the new information age, which will subsequently serve the purpose of designing viable and sophisticated anti-cybercrime mechanisms. Balanced and fair efforts directed at the control of cybercrime will, in the end, build a digital world that is just and ethical. By unpacking the secular and religious legal dimensions, this study provides a vital addition to the literature: the integration of faith-based legal norms with the challenges that worry people's faith in the age of swift technological advancements. The study seeks to propel scholarly discourse on the convergence of social values, the advancements of science and technology, and the legal tradition in order to develop adequate and appropriate responses to cybercrime and to strike a balance based on the Islamic legal tradition and contemporary legal systems.

LITERATURE REVIEW

Conceptual Foundations of Cybercrime and Enforcement

Varying complexity in cybercrime emphasizes the importance of analyzing its sociotechnical and legal dimensions. Li (2018) explains that in order to fight cybercriminals, law enforcement relies on policy, personnel, and international partners. As cross-border cybercrimes increase, so does the significance of international collaboration. On the other hand, Clough (2011) outlines the criminalization of unauthorized access to data and expresses concern that the limitations of existing legal definitions to capture digital data also apply to the valued intangible assets of traditional legal

systems. This gap in the legal definition has spawned new laws concerning the criminal justice response to data breaches and hacking and the harm caused to physical property (Fig. 2).

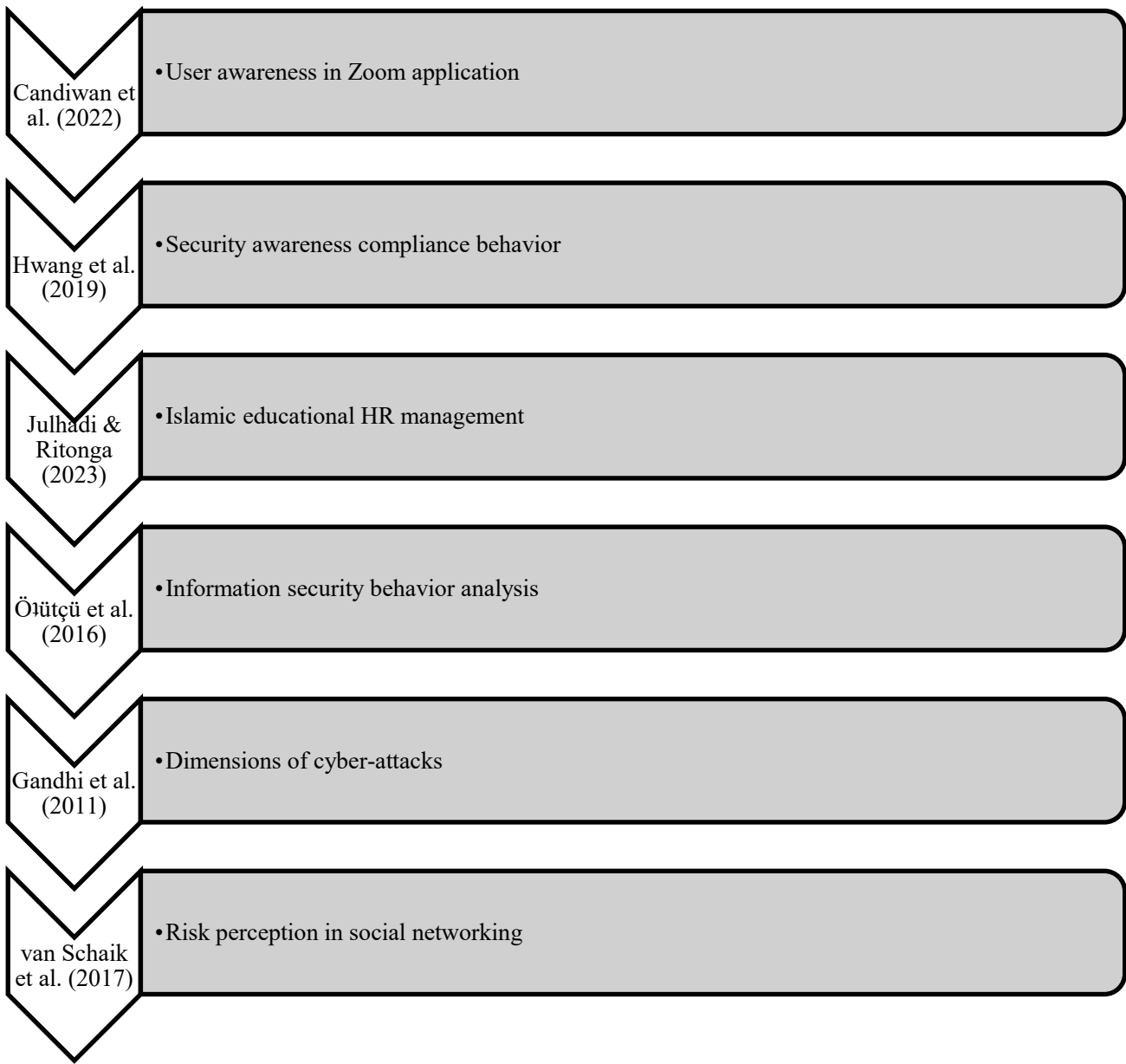


Figure 2. Literature review results

Classical theft (Sariah) and fraud (shish) in the framework of Islamic jurisprudence can include digital acts of theft. From the same perspective, Furashev (2012) distinguishes cyberspace from information space, citing that modern legal systems and religious teachings should recognize the ambiguous boundaries at which intangible harm arises. The objectives of Islamic jurisprudence create a value system as an ethical basis for prohibiting cybercrimes, including phishing and identity theft (Ilchenko et al., 2019). However, the practical enforcement of these principles requires the integration of Sharia and secular regulation.

There is a growing need for unified strategies for cybersecurity as digital services and online shopping grow. Alazzam et al. (2026) create an information model for e-commerce that integrates socio-economics with legal frameworks, focusing on the importance of customer trust to the growth of the business. At the same time, Andespa et al. (2024) examine how Islamic branding in financial

services, with a focus on ethical values, can support the advancement of sustainable development. This approach can also include cybersecurity.

METHODOLOGY

Research Design and Doctrinal Analysis

The methodology of this study uses legal analysis in combination with comparative research that focuses on both criminal law and Islamic jurisprudence. The doctrinal analysis of this study uses legislation, court judgments, and relevant scholarly elaborations. The main goal of this methodology is to illustrate how different formalized jurisdictions use legal classification and criminal prosecution of cybercrime. The methodology includes a critical evaluation of criminal codes, international policies, and regulations, as well as recent verified case studies in this regard. The research methodology, as articulated above, incorporates primary and secondary sources. Looking at Islamic jurisprudence in particular, the methodology incorporates the analysis of the Qur'an, the Sunnah, and complementary sources of Islamic legal science. For the methodology to be relevant for real legal problems, special focus is placed on how Islamic legal scholars and scholars of jurisprudence interpret various criminal acts, including theft, fraud, and infringements of the rules and regulations regarding confidentiality. This issue becomes particularly relevant because many contemporary criminal offenses committed in a digital environment expand the limits of the understanding of criminal offenses and include new offenses, vagueness, and new challenges regarding standards of proof, the existence of criminal intent, and limitations of criminal jurisdiction. The methodology that we propose will allow us to expand the existing knowledge of secular criminal laws in different countries and determine the extent to which legal acts in this analysis may conflict or be consistent with the Islamic legal provisions contained in the Islamic sacred text.

Comparative Framework and IDEF3 Process Modeling

The second phase of the research, after conducting doctrinal analysis, includes a comparative framework. This framework organizes the secular penal code and Islamic Shari'a as a basis of jurisprudence. The analysis is both qualitative and quantitative. Thus, the qualitative assessment will include a thematic analysis and identify common and unique goals or objectives. Quantitative data consists of statistics on the cases and cybercrime data, along with data on legislative amendments and the real data from the enforcement of the law in nations that use Islamic law as a component of their criminal justice system. These nations include Saudi Arabia, Pakistan, and Malaysia, among others. A significant feature of our research methodology is the incorporation of the IDEF3 (Integrated Definition for Process Description Capture Method). This method focuses on the processes by which cybercrimes are identified, investigated, and prosecuted, and the punishments prescribed by both the traditional and Islamic criminal justice systems.

The IDEF3 approach therefore emphasizes two key elements:

1. A process flow diagram, which depicts the activities and interactions of the different stakeholders, including law enforcement, judges, and cybercriminal offenders; and
2. A state-to-state transition diagram. Essentially, these diagrams illustrate how evidence and suspects will move through the various stages of the criminal justice system.

REASERCH RESULTS

Process Description and Modeling Elements

This section presents the results derived from the application of the IDEF3 modeling technique to address cybercrimes from a dual perspective: conventional criminal law and Islamic jurisprudence. IDEF3 is especially suited for capturing the sequence of activities, decisions, and interactions among various stakeholders in a dynamic environment where technical and legal domains intersect (Fig.3).

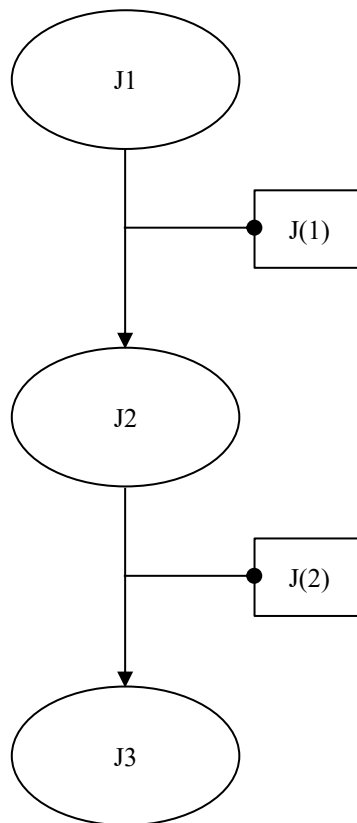


Figure 3. IDEF3 model

J1. Legislative reform and harmonization.

J11. Identify Legal Gaps

- Conduct a comprehensive review of existing criminal law and Islamic jurisprudential statutes to pinpoint deficiencies in addressing modern cybercrimes.
- Focus on specific areas like unauthorized access (hacking), identity theft, ransomware, and data protection.
- Gather input from legal experts, technology specialists, and religious scholars to ensure the review is holistic.
- Document findings and categorize them by severity and frequency of occurrence.

J12. Draft Comprehensive Legislation

- Develop laws that explicitly criminalize various forms of cyber-offenses (e.g., phishing, DoS attacks, cyber-bullying) in alignment with both secular legal norms and Islamic ethical imperatives.

- Incorporate clear definitions of digital evidence, procedural safeguards, and penalty frameworks for cyber-related crimes.
- Ensure consistency with international standards such as the Budapest Convention, while reflecting core Islamic values of justice and moral accountability.
- Engage in stakeholder consultations to refine legislative drafts before enactment.

J13. Integrate Islamic Principles

- Analyze how existing or new statutes can be interpreted and enforced in line with Sharia, particularly under ta'zir (discretionary punishments) where hudud offenses do not apply.
- Consider the role of intent (niyyah) in cyber-offenses; for instance, hacking with malicious intent could be treated differently from accidental unauthorized access.
- Encourage cross-referencing between secular legal codes and authoritative Islamic legal opinions (fatwas) to create harmony between the two systems.
- Provide guidelines for judges and muftis on how to handle digital evidence and technology-related issues in Sharia courts (Fig.4).
-

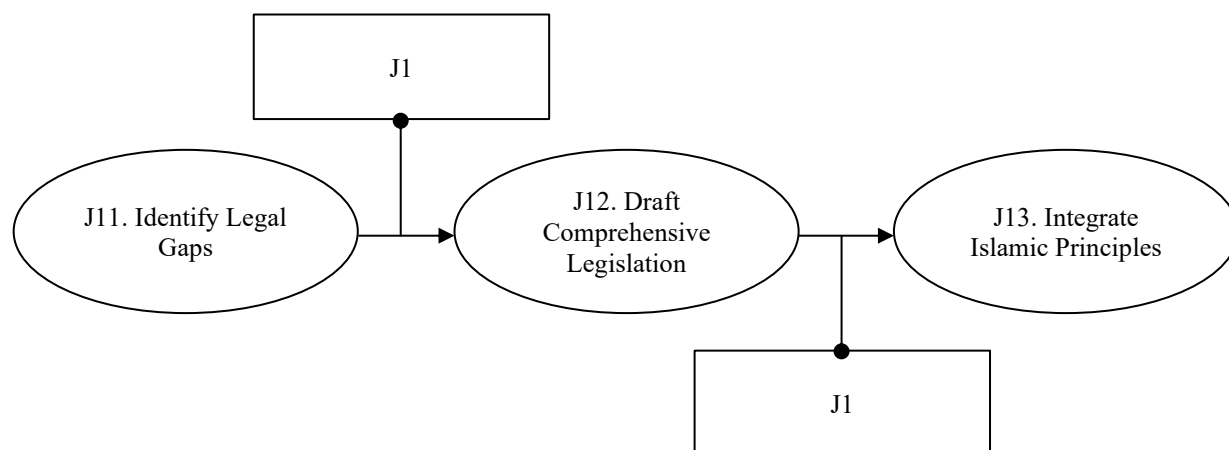


Figure 4. IDEF3 model to achieve J1

J2. Capacity building and training.

J21. Law Enforcement Training

- Implement specialized programs for police officers, prosecutors, and investigators to handle digital forensics, evidence preservation, and emerging cybercrime tactics.
- Include modules on understanding Islamic legal principles relevant to technology and privacy.
- Offer regular refresher courses to keep practitioners updated on new cyber threats and investigative methods.
- Create partnerships with universities and tech companies for continuous learning opportunities.

J22. Judicial and Islamic Scholar Education

- Organize seminars and workshops for judges, muftis, and religious scholars to deepen their understanding of cybercrime intricacies.
- Present real-world case studies that demonstrate how digital evidence is gathered, analyzed, and authenticated.
- Encourage collaborative knowledge exchange sessions between secular legal experts and Islamic jurists, fostering mutual insights.
- Ensure continuing education credits or similar incentives for active participation in training programs.

J23. Public Awareness Campaigns

- Develop educational initiatives for the general population, highlighting common cybercrimes (phishing, scams, malware) and preventive measures.
- Leverage mosques, community centers, and social media to disseminate information on both secular legal obligations and Islamic ethical teachings about online conduct.
- Emphasize the moral responsibility to protect data and privacy, tying it to Islamic principles of stewardship and trust (amanah).
- Reinforce safe internet practices and reporting channels for suspected cyber-incidents (Fig.5).

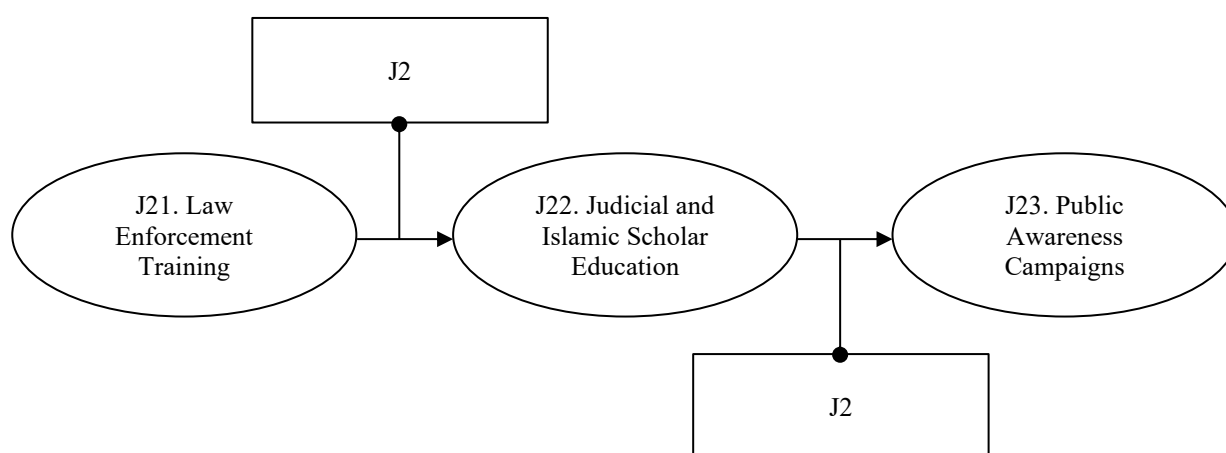


Figure 5. IDEF3 model to achieve J2

J3. Effective enforcement mechanisms.

J31. Digital Forensic Infrastructure

- Invest in forensic laboratories equipped with modern hardware and software to recover and analyze digital evidence.
- Standardize protocols for evidence chain-of-custody to meet both secular and Islamic admissibility standards.

- Collaborate with private tech firms for cutting-edge forensic tools that preserve metadata and ensure data integrity.
- Implement robust encryption and cybersecurity measures within law enforcement agencies to protect sensitive case files.

J32. Multi-Agency Task Forces

- Form inter-agency teams—comprising cybercrime investigators, prosecutors, religious scholars, and IT experts—that can rapidly respond to cyber incidents.
- Define clear lines of authority and roles, ensuring that secular and Sharia-based perspectives are integrated at each investigative step.
- Develop centralized databases to track cybercrime trends, share intelligence, and facilitate cross-border cooperation.
- Evaluate task force performance periodically, adjusting strategies according to emerging threats and operational feedback.

J33. International Cooperation

- Enhance cooperation through mutual legal assistance treaties (MLATs) that respect Islamic legal norms where applicable.
- Participate in global cybercrime prevention initiatives, exchanging best practices with non-Muslim-majority nations.
- Foster relationships with international organizations (Interpol, Europol) to streamline cross-border digital evidence gathering and suspect extraditions.
- Balance global standards with local cultural and religious considerations when negotiating international agreements.

This stage's plan seeks to create a comprehensive answer to the legal and ethical challenges of cybercrime using criminal law, criminal jurisprudence, and Islamic jurisprudence. Thoughtful legislative reform, construction of institutions, and the development of enforcement practices will enable the continuous assessment of the barriers posed by cybercrime and the demands of justice. The protection of digital ecosystems will be achieved with the integration of the principles of Islamic jurisprudence and criminal jurisprudence.

The synthesis of these components using IDEF3 illustrates important synergistic relationships and potential problematic areas that will further inform and enhance enforcement policy and strategies. The following explores how these relationships will enhance legislation, tech development, and interagency coordination to address cybercrime within the scope of criminal jurisprudence and Islamic jurisprudence.

DISCUSSIONS

Integrating Criminal Law with Islamic Jurisprudence

The literature emphasizes the need for the integration of secular and Islamic jurisprudential principles. As discussed by Dumchykov et al. (2022) and Furashev (2012), the shift to digital life requires law enforcement agencies and policymakers in predominantly Muslim countries to update and extend classical concepts of theft, fraud, and privacy to cyber-based crimes. The hacking example would fall under the ta'zir (discretionary punishments) if the boundaries of hudud (fixed punishments) are not broken. The moral and legal sanctions would serve their intended purposes and deter cybercrime (Fig. 6).

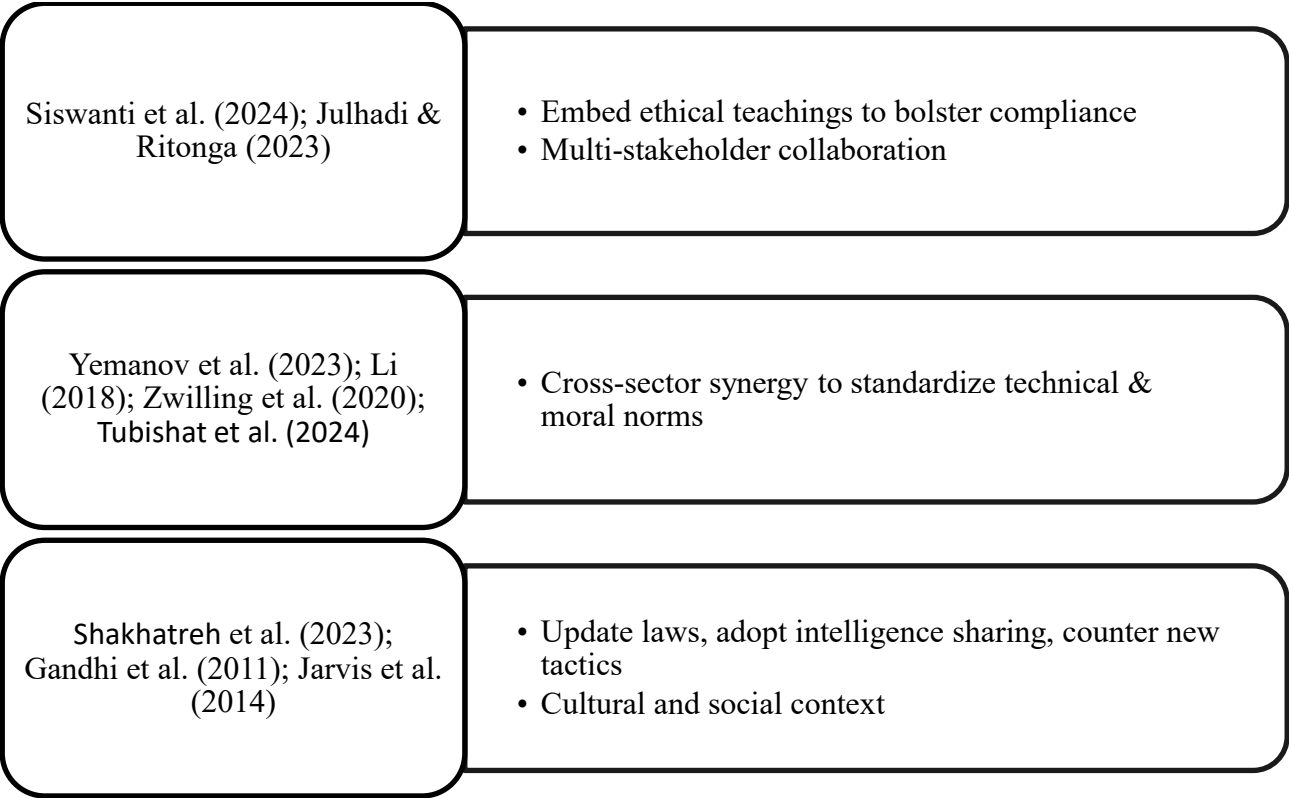


Figure 6. Key Discussion Points and Relevant Studies

In summary, literature indicates that solving the problems presented by the variance and sophistication of cybercrime will require multiple steps, such as the passage of new laws, moral education, and cooperation on an international scale. Secular criminal law and Islamic legal systems can both provide useful frameworks and, through integration, provide rigorous and ethically grounded solutions. With a combination of security awareness and collaborative governance combined with international partnerships, stakeholders can ultimately fulfill the need for improving security and policing the digital domain in line with contemporary legal systems as well as traditional religious frameworks.

CONCLUSIONS

Legal and Practical Implications

What has been discussed shows that in the context of contemporary conditions, solving the problem of cybercrime requires multi-dimensional and comprehensive solutions that integrate the rigor of contemporary criminal law with the Islamic ethical system. In practice, legal proceedings

may be procedurally difficult due to the contradiction between secular legal systems and religious legal systems. For instance, in many Islamic countries, courts are faced with challenges and issues of legal definition and classification of crimes that are usually considered to be criminal offenses in Sharia. This may lead to judicial duplication of work. In light of the above, the creation of a comprehensive and integrated legal framework that integrates relevant contemporary international instruments on combating and preventing cybercrime with classical Islamic legal concepts has become more necessary than ever before.

The Internet has connected every user globally. With that connection comes the opportunity to communicate and share ideas. Security and openness of the Internet require rules, and more importantly, autonomy. The Internet, likewise, has brought great opportunities with increased chances of identity theft and cyber terror. There is a direct correlation between tech advancement and increased vulnerability to cybercrime. Now more than ever, cybercrime is one of the most significant dangers to the public and national security. Cybercrimes manifest in many ways. From e-mail scams to large-scale infrastructural attacks, crimes online are vast and continuously developing. Efforts to counteract these crimes are made at the international and national levels, though the number and expansion of offenses in cyberspace continue. Because of the nature of these criminal activities, constant modifications to mechanisms for the protection of cyberspace are necessary.

Constant changes demand immediate adjustments from state officials, particularly when it comes to newly developed technologies and threats that emerge in the global network. Hence, these issues necessitate the development of specific mechanisms to protect human rights and meet users' demands in cyberspace. Lack of coordination in the protection of human rights in cyberspace leads to insufficient efficiency of the mechanisms in question and therefore requires analysis and suitable adjustments.

We are living in the age of the information society, where computational devices and telecommunications systems affect every facet of life, be it a state or an individual citizen. Integration of global digitalization into a society creates opportunities for the misuse of information and telecommunication technologies. Today, not only individuals but also states can be the victims of individuals or groups who operate in the virtual space. A few individuals or groups of individuals can potentially threaten the security of thousands of individuals. The rate of criminal activities in cyberspace is increasing at a similar rate to the rate of growth of the number of Internet users and telecommunication systems.

A policy agenda balancing deterrence with rehabilitation is yet another striking conclusion. While more secular laws tend to favor punishment with fines or time behind bars, Islamic law has provisions for penitence or reparations. Reforms in the law offer opportunities to incorporate such provisions and encourage perpetrators to pay their debts to society. Finally, cybercrime is a global concern for which international collaboration is of paramount importance. Muslim-majority and non-Muslim-majority countries can collaborate on binational legal assistance and common frameworks to enhance global cyber defense.

To manage and govern cybercrime efficiently, a combination of legislative, judicial, ethical, and technological initiatives is requisite. When evaluating these multidimensional responses to the challenges presented by cybercrime, it may be instructive to apply systems thinking and IDEF3 modeling to understand how stakeholders can address and overcome the challenges presented by the complicated systems. The modeling offers an ethical pathway through the principles of universal criminal justice and Islamic criminal law to resolve the challenges presented by cybercrime.

REFERENCES

1. Ababneh, A. M. D., Jarah, B. A. F., Al-Kharabsheh, A., Al-Zaqeba, M. A. A., & Basheti, I. (2024). The role of human resources management in the development of total quality management in the public and private sectors in Jordan. *Humanities and Social Sciences Letters*, 12(2), 319-330.
2. Abolouz, A. (2024). Struggling to Fit: The Case of Saudi Born Millennials from Palestinian-origin Returnees to Jordan. *Hikama*, 8(4), 68-98, doi: 10.31430/XMBC4270.
3. Alahmed, M. A., Alasfour, M. G., & Salifu, E. (2023). Users' informativity and effective communication: the banking field in Kuwait. *Arab Journal of Administrative Sciences*, 30(1), 221-260.
4. Al-Amoush, N. (2024). Rights and Public Freedoms as Stipulated in the Jordanian Constitution and their Relation to Treaty's Ratification in Jordan. *The Jordanian Journal of Law and Political Science*, 16(1). <https://doi.org/10.35682/jjlps.v16i1.674>.
5. Alazzam, F.A.F., Gharaibeh, Z.I.Y., Jarah, B.A.F., Aljabali, A.M.A., Al-Zaqeba, M.A.A. (2026). Legal and cybersecurity challenges of integrating artificial intelligence and the internet of things in financial institutions in the United Arab Emirates and Jordan, *International Journal of Data and Network Science*, 10(1), 265–272.
6. Al-Fulaij, S., Al-Qudsi, S., Arman, H., & Alawadhi, A. S. (2022). The Potential Role of Exports-Imports in Income Diversification and Sustainable Development of Kuwait. *Arab Journal of Administrative Sciences*, 29(1), 169-200.
7. Alkhawaldeh, A., Alakash, M. A. N., Akho-Rashida, H. A., Al Wahshat, Z. M., & Issa, M. S. B. (2023). The role of the geopolitical position of the Hashemite Kingdom of Jordan towards American foreign policy from 1990 to 2017. *Journal of Liberty and International Affairs*, 9(3), 281-298.
8. Al-majali, H. (2024). The The Impact of Global and Regional Powers on the Kurdish issue. *The Jordanian Journal of Law and Political Science*, 15(4). <https://doi.org/10.35682/jjlps.v15i4.590>.
9. Al-Salamat, M., Garaibeh, Z., & Alshible, M. (2023). The Effect of the Victim's Consent in the Crime of Human Trafficking Under the Jordanian Human Trafficking Prevention Law. *Pakistan Journal of Criminology*, 15(4), 363.
10. Alsayed, A. H. (2023). The Relationship between Prior Business Ownership Experience and Opportunity Identification: The Role of Cognitive Styles. *Arab Journal of Administrative Sciences*, 30(1), 220-175.
11. AL-Tuwaijry, I. (2024). The Latest in the Saudi Environmental Regulation 2020. *The Jordanian Journal of Law and Political Science*, 16(1). <https://doi.org/10.35682/jjlps.v16i1.637>.
12. Andespa, R., Yeni, Y.H., Fernando, Y., Sari, D.K. (2024). Sustainable development of Islamic banks by creating Islamic branding: Challenges, importance, and strategies of Islamic branding. *International Journal of Sustainable Development and Planning*, Vol. 19, No. 2, pp. 637-650. <https://doi.org/10.18280/ijstdp.190221>.
13. Ayasreh, E. (2024). Climate Diplomacy from a Neoclassical Realist Perspective: The Jordanian Model. *The Jordanian Journal of Law and Political Science*, 16(2). <https://doi.org/10.35682/jjlps.v16i2.702>.
14. Bani-Meqdad, M.A.M., Senyk, P., Udod, M., Pylypenko, T., Sylkin, O. (2024). Cyber-environment in the human rights system: Modern challenges to protect intellectual property law and ensure sustainable development of the region. *International Journal of Sustainable Development and Planning*, Vol. 19, No. 4, pp. 1389-1396. <https://doi.org/10.18280/ijstdp.190416>.
15. Betar, M. L., & Murtaza, M. H. (2022). The Impact of Banking Competitiveness in Economic Growth in Syria. *Arab Journal of Administrative Sciences*, 29(3). <https://doi.org/10.34120/ajas.v29i3.159>.
16. Candiwan, C., Azmi, M., Alamsyah, A. (2022). Analysis of behavioral and information security awareness among users of zoom application in COVID-19 era. *International Journal of Safety and Security Engineering*, Vol. 12, No. 2, pp. 229-237. <https://doi.org/10.18280/ijsse.120212>.

17. Clough, J. (2011). Data theft? Cybercrime and the increasing criminalization of access to data. *Criminal Law Forum*, 22(1): 145-170. <https://doi.org/10.1007/s10609-011-9133-5>.
18. Dahiyat, E. A. R. (2019). Online shopping and consumer rights in the UAE: Do we need a specific law?. *Arab Law Quarterly*, 33(1), 35-57.
19. Dumchykov, M., Utkina, M., Bondarenko, O. (2022). Cybercrime as a threat to the national security of the Baltic States and Ukraine: The comparative analysis. *International Journal of Safety and Security Engineering*, Vol. 12, No. 4, pp. 481-490. <https://doi.org/10.18280/ijssse.120409>.
20. Elbasri, A. (2024). The United Nations Early Warning Mechanism for the Prevention of Genocide and its Obstruction in the Case of Palestine. *Hikama*, 8(4), 9-43, doi: 10.31430/YWDP4468.
21. Elgedawy, M. N. (2023). The Relationship between Data Governance and Organizational Performance: The Mediating Effect of Explainable Artificial Intelligence. *Arab Journal of Administrative Sciences*, 30(1), 67-13. <https://doi.org/10.34120/ajas.v30i1.213>.
22. Elmorchid, B., & Chougrani, E., & Mansouri, B. (2023). Towards Constructing a Statistical Index to Measure Political Culture in Arab Countries: Which Methodology to Use in the Field of Political Sciences?. *Siyasat Arabiya*, 11(64-65), 73-98, doi: 10.31430/HKXN5310.
23. Fetais, A., & Abu Rajab, M. (2024). The role of the judiciary in attracting investment and protecting investors' rights: A comparative study. *The Jordanian Journal of Law and Political Science*, 15(4). <https://doi.org/10.35682/jilps.v15i4.617>.
24. Furashev, V.M. (2012). Cyberspace and information space, cyber security and information security: Essence, definition, differences. *Information and Law*, 2(5): 162-175.
25. Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., Laplante, P. (2011). Dimensions of cyber-attacks: Cultural, social, economic, and political. *IEEE Technology and Society Magazine*, 30(1): 28-38. <https://doi.org/10.1109/MTS.2011.940293>.
26. Gharaibeh, Y., & Ibrahim, Z. (2024). Legal Support for Sustainable Development in Middle East. *International Journal of Sustainable Development & Planning*, 19(4), 1439.
27. Goudjili, S. (2023). International Relations in the Arab World: A Social History of its Origins, Development and Current State of Affairs. *Siyasat Arabiya*, 11(64-65), 7-30, doi: [10.31430/ICHA8584](https://doi.org/10.31430/ICHA8584).
28. Hwang, I., Wakefield, R., Kim, S., Kim, T. (2019). Security awareness: The first step in information security compliance behavior. *Journal of Computer Information Systems*, 61(4): 345-356. <https://doi.org/10.1080/08874417.2019.1650676>.
29. Ilchenko, O., Chumak, V., Kuzmenko, S., Shelukhin, O., Dobrovinskyi, A. (2019). Fishing as a cybercrime in the internet banking system: economic and legal aspects. *Journal of Legal, Ethical and Regulatory Issues*, 22(2): 1-6.
30. Issa, M. S. B. (2025). Ontological security and foreign policy in West Asia: Identity politics after the Abraham Accords. *Social Sciences & Humanities Open*, 12, 102089.
31. Jarah, B. A. F. (2025). Application of Artificial Intelligence in Jordanian Banks and Its Impact on the Quality of Services. In *Conference on Sustainability and Cutting-Edge Business Technologies* (pp. 84-92). Cham: Springer Nature Switzerland.
32. Jarah, B. A. F., Alzubi, E. A., Ineizeh, N. I., Almatarneh, Z., Al-Khawajas, H. A., & Al-Jarrahs, M. M. (2025). The Relationship Between the Accounting Information System and Perceived Performance: The Moderating Effect of Managerial Qualifications According to Company law. *Calitatea*, 26(208), 50-59.
33. Jarvis, L., Macdonald, S., Nouri, L. (2014). The cyberterrorism threat: Findings from a survey of researchers. *Studies in Conflict & Terrorism*, 37(1): 68-90. <https://doi.org/10.1080/1057610X.2014.853603>.
34. Julhadi, Ritonga, M. (2023). Human resource management in Islamic educational institutions to improve competitiveness in society 5.0 era. *International Journal of Sustainable Development and Planning*, Vol. 18, No. 2, pp. 611-619. <https://doi.org/10.18280/ijstdp.180231>.

35. Lainjo, B. (2020). Network security and its implications on program management. *International Journal of Safety and Security Engineering*, Vol. 10, No. 6, pp. 739-746. <https://doi.org/10.18280/ijssse.100603>.
36. Leukfeldt, E.R., Lavgorgna, A., Kleemans, E.R. (2017). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research*, 23(3): 287-300. <https://doi.org/10.1007/s10610-016-9332-z>.
37. Li, X. (2018). Crucial elements in law enforcement against cybercrime. *International Journal of Information Security Science*, 7(3): 140-158.
38. Mohammad Aljawarneh, N., Abu Huson, Y., Ahmad Faleh Alazzam, F., Abdel Kader Alomari, K., & Almarashdi, F. (2026). It audit quality and digital business performance: The moderating role of digital leadership. *EDPACS*, 71(5), 71-81.
39. Ölütcü, G., Testik, Ö.M., Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers and Security*, 56: 83-93. <https://doi.org/10.1016/j.cose.2015.10.002>.
40. Shakhatreh, H. J. M., Salman, A., Aldrou, K. K. A. R., Comite, U., & Alazzam, F. A. F. (2023). Analyzing the relationship between inventory policies and CSR practices: Case of Jordanian companies. *Economics*, 11(s1), 141-163.
41. Siswanti, I., Riyadh, H.A., Prowanta, E. (2024). Digital transformation's moderating role on financing and capital quality impacts for sustainable Islamic rural banking in Indonesia. *International Journal of Sustainable Development and Planning*, Vol. 19, No. 3, pp. 991-1001. <https://doi.org/10.18280/ijstdp.190317>.
42. Tubishat, B. M. A. R., Alazzam, F. A. F., Viunyk, O., Yatsun, V., & Horpynchenko, O. (2024). Planning to improve the efficiency of open systems commercial relations to ensure uninterrupted sustainable development: Regional legal aspect. *International Journal of Sustainable Development and Planning*, 19(3), 1089-1097.
43. van Schaik, P., Jansen, J., Onibokun, J., Camp, L.J., Kusev, P. (2017). Security and privacy in online social networking: risk perception and precautionary behavior. *Computers in Human Behavior*, 78: 283-297. <https://doi.org/10.1016/j.chb.2017.10.007>.
44. Yemanov, V., Dzyana, H., Dzyany, N., Dolinchenko, O., Didych, O. (2023). Modelling a public administration system for ensuring cybersecurity. *International Journal of Safety and Security Engineering*, Vol. 13, No. 1, pp. 81-88. <https://doi.org/10.18280/ijssse.130109>.
45. Zwilling, M., Klien, G., Lesjak, D., Wiecheteck, Ł., Cetin, F. Basim, H.N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 62(1): 82-97. <https://doi.org/10.1080/08874417.2020.1712269>.