The Effectiveness of Cyber Legislation in Addressing Behavioral Deviations in the Digital Space

A Comparative Study between Jordan and the UAE

Mohamed Hadi Al Najdawi
Dr. Nidal Al Jundi

Abstract: This study examines the effectiveness of cyber laws in curbing anomalous cyber behavior, with a particular focus on the legal systems of the United Arab Emirates and Jordan. Given the increasing incidence of cybercrime and the diversity of digital misconduct, this study aims to understand the legal, institutional, and preventive factors that influence cybersecurity governance.

This study adopted a descriptive analysis approach and issued a structured questionnaire to 180 participants, divided into three groups: legal professionals, legal scholars and artificial intelligence experts, and judicial and regulatory representatives. To test the research hypotheses, the quantitative data were analyzed using the chi-square test (Ka2), arithmetic mean, standard deviation, and descriptive statistics.

The results showed that the respondents generally believed that the institutional and legal systems to combat cybercrime were in place. However, there are still significant gaps in public trust and legal awareness of digital security. Compared with Jordan, the UAE's cyber laws were rated as more developed in terms of flexibility and enforceability. The results also showed that there were statistically significant differences between the two countries' legal systems, especially in terms of institutional infrastructure and technological readiness.

The results show that despite the advanced cyber laws in the UAE and Jordan, further efforts are needed to standardize enforcement procedures, raise public awareness, and enhance legal flexibility. The comparative observations highlight that combining legal, technical, and ethical factors is essential to improving digital security and reducing aberrant online behavior.

BACKGROUND

The spread of digital communication technologies and the explosive growth of information are transforming the human network in modern society. The emergence of cyberspace represents a new dimension of social and behavioral relations. The openness and cross-border interconnectivity of this digital world presents tremendous opportunities for cognitive and economic growth. However, given the traditional challenges of regulating human behavior in virtual worlds, virtual worlds have also become a breeding ground for deviant behaviors that threaten moral and social security.

In order to keep pace with technological advances and ensure that rights and freedoms in digital space are protected without jeopardizing social security or stability, these advances have prompted countries to establish new legal frameworks, so-called cyber legislation. Examining the effectiveness of these laws is crucial given the rise of deviant behaviors online such as cyberbullying, cyberextortion, hate speech, and social media harassment—behaviors that are as harmful as those in real life. This study aims to assess the effectiveness of cyber laws in Jordan and the UAE in addressing different digital behaviors by comparing the legal frameworks, enforcement strategies, and institutional practices of the two countries. The study also identifies strengths and weaknesses and offers suggestions for improvement in order to enhance the legal framework's ability to address modern digital issues.

The significance of this study lies in its examination of deviant behaviors in cyberspace, one of the emerging issues of concern in digital society. It draws attention to how law can be used as a regulatory tool to address problems. The comparative nature of this study is equally important as it provides an opportunity to understand different legal models and identify best practices that can help develop national legislation. This study is of great relevance given the rapid advancement of technology and the growing popularity of digital media..

Thus, through a methodical comparison of the two laws, this study intends to investigate and evaluate how well cyber laws in Jordan and the United Arab Emirates reduce behavioral abnormalities in the digital sphere and how well they address the legal and social demands for dealing with deviant digital behavioral phenomena.

The research problem is represented by the gap between the acceleration of behavioral deviations in the digital space, on the one hand, and on the other hand, the capacity of cyber laws to successfully regulate these aberrations. This calls into question the degree to which the current legal frameworks in Jordan and the United Arab Emirates are able to prevent, safeguard against, and deal with this new form of activity.

1. To what extent do cyber laws in the United Arab Emirates and Jordan effectively handle aberrations in online behavior?

2. What aspects of the two nations' cyber law systems are similar and which are different?

3. What are the main obstacles that this law's application to abnormal online conduct faces?

4. How may this law's efficacy be improved to stay up with the rapid advancements in technology?

Hypotheses:

1. There are no statistically significant differences between the opinions of the study sample regarding the challenges facing the implementation of cyber legislation in reducing behavioral deviations in the digital space in both Jordan and the UAE.

2. There are no statistically significant differences between the opinions of the study sample regarding the effectiveness of cyber legislation in Jordan and the UAE in terms of its role in prevention, deterrence, and enhancing digital security.

3. There are no statistically significant differences between the opinions of the study sample regarding the differences between the Jordanian and Emirati legal models in addressing digital behavioral deviations.

THEORETICAL LITERATURE REVIEW

1.1 Theoretical Foundations of Cyberspace and Digital Behavioral Deviations

One of the most well-known ideas of the contemporary digital era is cyberspace. It has developed into a vast virtual environment that makes it possible for data to be processed, stored, and shared via electronic networks, especially the internet. This area is distinguished by its inability to be affected by traditional sovereignty or geographic borders. Instead, it facilitates instantaneous communication and interaction between people, systems, and institutions in a non-physical setting. Its legal regulation is therefore somewhat complicated (Al-Amarat & Al-Hamamseh, 2022).

Cyberspace is significant because it is both a place for learning and growth, but also a breeding ground for criminal activities and behavioral problems. Today, many scholars view cyberspace as a unique legal domain that, due to its legal complexity, requires specialized regulation based on its functional and technical characteristics. Its global nature, the difficulty of accurately identifying offenders and their locations, the rapidity of data flows, and the fact that real identities are lacking in many cases are its most significant legal characteristics (Fawzy, 2019). As Abdel Hamid and Molook point out, the nature of the domain requires

that the law continue to evolve to keep pace with its rapid development. (Abdel Hamid & Molook, 2020).

Because of this space's technical design, people can access it and hide their identities, making it necessary to utilize sophisticated legal and technological instruments to prove deviant behavior or cybercrimes. Given these features, cyberspace is seen as a contemporary and intricate legal landscape that necessitates regulating strategies that blend conventional law with cutting-edge technical legislation (Shires, 2021). According to some practical research, the efficacy of legal responses to cybercrimes is weakened by the disorganized intelligence infrastructure for digital evidence (Alzahrani, Lee, & Kim, 2024).

Thus, the goal of this section of the study is to examine the key ideas related to cyberspace and digital behavioral abnormalities. The features of this environment, the kinds of aberrations that are common there, and the elements that encourage their development are all examined in this section. In order to better comprehend how to solve them in comparative cyber legislation, it also makes use of scientific ideas that aid in their explanation.

2.1.1 The Nature and Types of Behavioral Deviations in the Digital Environment

Whether in terms of the tool used, the environment in which they take place, or the mechanisms of interaction between the perpetrator and the victim, behavioral deviations in the digital environment are distinguished from traditional forms of deviance by specific features. New deviant behavior patterns have emerged in cyberspace, including cyber-extortion, cyberbullying, network fraud, privacy violations, the spread of misleading information, and other manifestations that directly threaten cybersecurity and societal harmony (Al-Sahafi, 2020).

The open digital environment, which allows for instantaneous and anonymous communication between users, is to blame for the growth of these aberrations. This weakens the effect of social and legal control and increases the likelihood of impunity (Odeibat, 2022). Since digital crime frequently takes on a non-physical aspect, it is challenging to prove using conventional evidence. This makes it more difficult for law enforcement to find offenders and bring them to justice (Ladadoh, 2021).

According to some experts, users' ignorance or their exposure to collective behavior that differs from that which is common in real life can occasionally lead to digital deviance rather than being solely driven by criminal intent. More awareness and digital literacy are needed for this (Abouzied, Alam, Ali, & Papotti, 2025). Because undesirable behaviors spread quickly and can become a recurring pattern among users unless they are thoroughly addressed through regulation and education, the interactive character of digital society also leads to the amplification of deviance (Sharabi, 2023).

2.1.2 The Nature and Types of Behavioral Deviations in the Digital Environmen

In the digital realm, there are numerous kinds of behavioral abnormalities that include a broad range of behaviors with varying degrees of legal and societal seriousness. Among these, communication abnormalities like cyberbullying and harassment through digital media are arguably the most common. These are actions intended to cause psychological injury to victims by means of threats, derogatory pictures, or insulting words (Abdel Hamid & Molook, 2020). Economic deviations come next, such as financial fraud through commercial platforms or emails, bank data theft, or account hacking using malware for illegal gain (Gupta, 2024).

The propagation of rumors, the encouragement of violent or pornographic material, or the inciting of bigotry and hatred are examples of ethical and behavioral transgressions. Particularly among teenagers and young adults, these activities pose a danger to society's moral framework (Fawzy, 2019). Technical deviations, on the other hand, are thought to be the most harmful kind. Examples of these include attacks on private and public databases, virus installation, and system hacking. These crimes are frequently coordinated and call for highly technological skills (Mashima et al., 2024).

The creation and spread of fake news or the use of artificial intelligence to fabricate photos and videos are examples of disinformation aberrations that also occur, resulting in an untrustworthy information environment that affects political and social security (Abouzied et al., 2025). According to some research, this latter kind is a long-term strategic danger since it attacks people's faith in institutions and fundamental knowledge (Positive Technologies, 2024).

2.2 The Legal Structure of Cyber Legislation in Jordan and the UAE

Cyber legislation has become essential for modern states due to the rapid advancements in technology and the resulting new legal challenges. This is especially true in light of the growing number of cybercrimes and behavioral deviations that pose a threat to individual privacy, the digital economy, and national security. Because of these quick changes, lawmakers in many nations have passed laws that define cybercrimes, their components, and their punishments, regulate the digital sphere, and create a sophisticated legal framework that can adapt to new dangers in the cyber environment (Gupta, 2024).

In this context, Jordan and the UAE are among the pioneering Arab countries in regulating cybercrimes through specific laws. Jordanian lawmakers enacted Cybercrime Law No. (17) of 2023, aiming to develop the penal framework for combating crimes committed by or targeting information systems. Meanwhile, the UAE adopted Federal Decree-Law No. (34) of 2021 on Combating Rumors and Cybercrimes, one of the most comprehensive Arab legislations and consistent with international standards in this field (Al-Amarat & Al-Hamamseh, 2022).

In this regard, the UAE and Jordan are two of the first Arab nations to implement laws specifically designed to control cybercrimes. Cybercrime Law No. (17) of 2023 was passed by Jordanian MPs with the intention of creating a legal framework to address crimes that target or are perpetrated by information technology. In the meantime, one of the most extensive Arab laws and one that complies with international norms in this area is Federal Decree-Law No. (34) of 2021 on Combating Rumors and Cybercrimes, which was adopted by the UAE (Al-Amarat & Al-Hamamseh, 2022).

2.2.1 The Concept of Cyber Legislation and its Preventive and Deterrent Objectives

Cyber legislation is a collection of laws designed to control how people use the internet, safeguard information systems, and prevent crimes that are perpetrated online or against the state's digital infrastructure or citizens. The profound changes brought about by the digital revolution have outstripped the deterrence and remediation powers of conventional laws, especially in light of the rise of new crime types like identity theft, cyber hacking, digital fraud, and defamation on social media (Al-Barrak, 2020). This kind of legislation is a logical response to these changes.

By raising awareness, encouraging a legal culture, and regulating the conduct of people and organizations in the electronic environment, this legislation seeks to accomplish two main objectives. The first is preventive, which entails putting in place legal controls that regulate the responsible use of digital technologies and stop harmful acts. In order to punish cybercrime offenders, discourage them from repeating their crimes, and discourage others from engaging in the same conduct, the second goal is deterrent, which focuses on detecting criminal acts and suitable consequences (Abdel Hamid & Molook, 2020).

Given that they cover topics like digital investigation, data integrity, proving criminality, and safeguarding against harmful information and rumors, it is possible to conclude that contemporary cyber laws are both highly specialized and adaptable. According to Gupta (2025), this emphasizes the necessity of providing them with a sophisticated technology infrastructure and legal professionals who are skilled in managing digital evidence and new forms of proof.

By promoting the ethical use of technology, controlling social media use, and keeping an eye out for suspicious uses of digital systems, modern legal trends also highlight the necessity of laws that are proactive and predictive rather than merely punishing crimes after they happen (Shires, 2021).

2.2.2 Analysis of the Jordanian Cybercrime Law No. (17) of 2023

With the adoption of the Jordan Cybercrime Law No. 17 of 2023, the legal framework for cybercrime in the Hashemite Kingdom of Jordan has undergone a fundamental change. The law is a legal response to the changing realities brought about by the development of digitalization, the increasing use of social media and the Internet, and the increasing prevalence of cybercrime. In addition to crimes such as hate speech and electronic rumors, the law also targets a range of criminal

acts, including illegal access to information systems, the use of personal data, and the dissemination of offensive or misleading content (Al-Barraiseh, 2021).

In terms of structure, the law is comprehensive and fully takes into account the technical nature of digital crimes. It precisely defines technical terms, clarifies the constituent elements of cybercrime, and grants law enforcement agencies broad powers to collect digital evidence while respecting the right to privacy and fair trial (Ladadoh, 2021). The law also expands the scope for more severe penalties, especially for crimes that endanger national security or public order, or are committed through protected systems or institutional accounts, in order to achieve general and specific deterrence.

A fundamental feature of the legislation is a comprehensive framework that takes into account the technical details of digital crimes. It grants law enforcement agencies broad powers to collect digital evidence, clarifies technical terminology, and lists the elements of cybercrime—provided that the right to privacy and a fair trial are respected (Ladadoh, 2021). The law further expands the scope for harsher penalties to achieve general and specific deterrence, especially for crimes that endanger national security or public order, or are committed through institutional accounts or protected systems.

Overall, Jordan’s 2023 law represents an important step towards curbing anomalies in the digital sphere. The law must be reviewed regularly in order to adapt to continued technological advances and to engage the legal community in creating a legal framework that ensures effectiveness without compromising constitutional guarantees.

2.2.3 Analysis of the UAE Anti-Cybercrime Law (Federal Decree-Law No. 34 of 2021)

One of the most progressive pieces of law in the Arab world is Federal Decree-Law No. (34) of 2021 on Combating Rumors and Cybercrimes in the United Arab Emirates. Given the growing dependence on digital technology in the political, economic, and social domains, it represents a thorough legislative strategy to countering new digital risks. This law, which takes the place of the former Federal Law No. (5) of 2012, addresses the technological and legal changes brought about by contemporary cybercrimes, especially in view of the growth of social media and its growing use for fraud, incitement, and rumor spreading (Al-Amarat & Al-Hamamseh, 2022).

A wide range of actions, including breaking into computer systems, misusing personal information, altering digital content, and spreading untrue rumors that jeopardize national security or public order, are expressly prohibited by UAE legislation, which has specific clauses that define cybercrime broadly. The law's stringent approach to safeguarding national cybersecurity is seen in its punishment of any attempt to damage the state's, its symbols', or its institutions' reputations, whether from within or without (Alzahrani, Lee, & Kim, 2024).

This law's emphasis on preventive measures is among its most notable aspects. It requires that digital content that violates national laws be censored

and that websites or social media platforms that do so be blocked. As part of a proactive strategy to combat online risks, it also gives authorities the authority to immediately order the suspension or restriction of suspect online accounts (Positive Technologies, 2024).

Though this approach is strict, some international human rights circles have questioned whether some of its provisions are consistent with standards of freedom of opinion and expression. This is especially true when it comes to the use of ambiguous terms like "threat to public security" or "harming the reputation of the state," which can be interpreted broadly (Shires, 2021). The decree, however, is regarded as one of the most extensive and adaptable pieces of law, effectively fusing legal regulation with technical protection, making it a crucial legislative reference at the regional level in addressing deviations in digital conduct.

2.2.4 Similarities and Differences in the Legal Treatment of Digital Violations in Both Regimes

In terms of concept, scope, penalties, and the authority granted to law enforcement agencies, there are several similarities and differences between the UAE Federal Decree-Law No. (34) of 2021 and the Jordanian Cybercrime Law No. (17) of 2023 regarding the legislative treatment of digital behavioral deviations. Similarities between the two systems include the need to make cybercrimes that compromise information security and society, like hacking into systems, distributing false information, blackmail, and misusing personal information, illegal. Both laws exhibit a deterrent and preventive strategy (Al-Baraiseh, 2021).

Similarities between the two laws include the adoption of exact technical definitions for cyberspace-related terms and the extension of authority to security agencies and the Public Prosecution to gather digital evidence, stop infringement, and confiscate tools used in cybercrime. Both impose harsh punishments for offenses against government agencies or involving the use of cutting-edge technology, indicating a mutual appreciation of the significance of cybersecurity's sovereign component (Ladadoh, 2021).

The disparities in judicial reach and degree of strictness are readily apparent. When it comes to the extent of criminalization and the protection of "state symbols" and "reputation" as separate legal values, Emirati law is more extensive than that of Jordan, demonstrating a rigorous, preventative political approach in the digital sphere (Al-Amarat & Al-Hamamseh, 2022). Jordanian law, in contrast, places more emphasis on controlling user-specific actions, giving judges more latitude in interpreting morally or politically significant conduct.

The methods used by the two regimes to keep an eye on digital platforms also vary. While Jordanian law often calls for a reference to the judiciary or the Public Prosecution, Emirati legislation gives executive authorities the quick and immediate authority to block websites and accounts. This illustrates how the Jordanian model strikes a compromise between freedom guarantees and security safeguards (Cyber Security Report, 2021). Additionally, it should be mentioned

that Jordanian law approaches digital crimes from the standpoint of public order and morality, but Emirati law directly connects them to national security.

All things considered, this comparison demonstrates that both systems agree on how dangerous digital behavioral abnormalities are. But Jordan places more of a focus on judicial discretion and gradual deterrence, whereas the UAE takes a more proactive and organized approach. This is a reflection of the many legal and political circumstances in which the cyber framework was constructed.

2.3 Evaluating the Effectiveness of Cyber Legislation in Reducing Behavioral Deviations

Although many countries, such as Jordan and the UAE, have made impressive progress in developing cyber laws, the fundamental question remains how effectively these laws achieve their primary objectives: preventing deviance in digital behavior and deterring those who engage in such behavior. The effectiveness of any legislation depends on its applicability, flexibility in responding to technological advances, and responsiveness to security and social needs in the digital sphere, rather than simply the letter of the law or the severity of the punishment (Gupta, 2024).

Clear legal texts, precise definitions of illegal behavior, dedicated enforcement mechanisms for fast and efficient enforcement, and a balance between legal protection and safeguarding individual constitutional rights (such as privacy and freedom of expression) are prerequisites for effective cyber legislation. Although some Arab countries have adopted technologically advanced cyber laws, recent studies have shown that they remain difficult to implement in practice. The root causes of these problems lie in the lack of a skilled workforce, inadequate technology, or conflicts between the judiciary and security forces (Al-Barrak, 2020). Against this backdrop, this study aims to comprehensively assess the effectiveness of regulations in Jordan and the UAE in curbing cybercrime. The study will examine the criteria for assessing the effectiveness of laws, focus on analyzing the main obstacles faced in the implementation of laws, and examine the measures taken by national authorities to combat cybercrime. In addition, the study will compare the current development of cyber law and analyze how cyber law can be updated by building a system that adapts to modern standards. (Shires, 2021).

2.3.1 Criteria for Evaluating the Effectiveness of Legislation (Deterrence, Prevention, Enforcement, Flexibility)

One of the most crucial measures of how well legal policies are working to address behavioral abnormalities in the digital sphere is the assessment of cyber legislation's efficacy. Only by using a set of objective standards that reflect the four pillars of legislative performance—deterrence, preventive, enforcement, and flexibility—can this thorough review be accomplished.

First, the ability of the law to influence people's thoughts and actions, which helps to reduce the commission of cybercrimes because of the fear of punishment, is a measure of deterrence. Some deviant patterns, especially those linked to

abuse on social media platforms, have been significantly reduced by the relatively harsh penalties outlined in the laws of Jordan and the United Arab Emirates, especially those pertaining to cyber hacking and the dissemination of rumors (Al-Barrak, 2020).

Second, prevention refers to how laws can lower the likelihood of crimes before they happen by raising awareness of digital issues, regulating user conduct, and limiting platform use. This component is explicitly emphasized by UAE law, which takes a proactive stance by offering tools for content monitoring, instant filtering, and limiting access to dangerous programs (Positive Technologies, 2024).

Third, the availability of skilled human resources and a technological infrastructure that permits the surveillance of offenders, the examination of digital evidence, and the implementation of judgments are indicators of enforcement capacity. Notwithstanding continuous institutional development initiatives, reports point to deficiencies in this area in Jordan as a result of the inadequacies of certain capable cybersecurity authorities (Cyber Security Report, 2021).

Finally, flexibility is one of the most important characteristics that cyber law should possess, given the rapid development of digital crime and the changing methods of its use. Flexibility refers to the ability of legal texts to adapt to new developments without the need for repeated, radical amendments. It is noteworthy that the UAE legislator has taken this dimension into account by formulating general provisions that are open to new technical interpretations, unlike the Jordanian model, which has remained closer to the traditional style in terms of linguistic and criminal construction (Shires, 2021).

According to these four standards, evaluating efficacy encompasses more than just the legal text; it also takes into account the institutional setting, the effectiveness of implementation, and the degree to which laws can be updated and modified to allow the state to uphold its digital sovereignty and defend people and organizations against cyberattacks.

2.3.2 Practical Challenges in Implementing Cyber Laws in Jordan and the UAE

Many structural, administrative, and technical obstacles still stand in the way of the actual application of cyber laws in Jordan and the United Arab Emirates, despite the formal and significant advancements made in these areas. These difficulties lessen their ability to prevent and deter deviations in digital conduct. The most notable of these difficulties stems from the inadequate technological and human capacities of some pertinent authorities. There is a lack of qualified staff in certain Jordanian judicial and security offices to examine digital evidence or handle technically challenging crimes such sophisticated hacking or international financial fraud (Cyber Security Report, 2021).

The most notable barriers to the effective implementation of cyber laws are also the lengthy legal processes and the lack of collaboration between the security and judicial branches. Given the fast and swift nature of digital crimes,

which necessitate an immediate court response, traditional procedures frequently postpone the arrest of offenders or the restoration of rights (Ladadoh, 2021). Furthermore, the efficacy of legal prosecution is restricted by inadequate information infrastructure, including digital tracking systems and judicial archiving.

Despite significant advancements in staff training and digital infrastructure equipment, the UAE's biggest problem is striking a careful balance between constitutional rights and security protection. Some legal provisions have drawn criticism for giving authorities extensive authority to censor information or detain people without sufficient judicial review. Furthermore, the numerous regulatory agencies and the different degrees of cooperation among them could result in conflicting powers or redundant processes, which would make it more difficult to apply the law in a cohesive and efficient manner. Shires (2021)

These difficulties are compounded by the issue of people's lack of digital legal literacy, as many users are still oblivious to the boundaries of what is allowed and forbidden in the online world, which frequently results in the unintentional or deliberate spread of deviations. As a result, the degree to which law keeps up with institutional, technical, and awareness-raising aspects—all of which are crucial components that support the success of the cyber legal system in practice—remains correlated with its effectiveness. (Al-Barrak, 2020)

2.3.3 Institutional and Security Efforts to Combat Digital Behavioral Deviations

Given the technical complexity of digital crimes, institutional and security measures are a crucial component in the successful application of cyber legislation. The Cybercrime Unit of the Criminal Investigation Department is one of the specialized units within the security services that Jordanian authorities have established. Its duties include monitoring digital content that is infringing, gathering electronic evidence, and offering technical assistance to courts and prosecution offices (Cyber Security Report, 2021). Jordan has made great progress in preparing police and judicial staff to handle cybercrime crimes, especially after the new Law No. (17) of 2023 was issued, despite having fewer technical resources than wealthy nations.

In order to increase digital literacy and lower the likelihood of unintentional involvement in cybercrimes, the Telecommunications Regulatory Commission, in collaboration with the Ministry of Digital Economy and Entrepreneurship, has started a number of awareness-raising campaigns aimed at students, staff, and regular users. These programs, however, still have limitations in terms of their scope and sustainability, and they must be expanded within all-encompassing national plans. Al-Barrak (2020)

The UAE approach, on the other hand, shows a high level of institutional integration in the fight against digital deviance. Established as a legislative, supervisory, and coordinating body, the National Cybersecurity Authority works to update rules, oversee the security of critical digital infrastructure, and

regulate general cyber policy. In addition, the Ministry of Interior and the Telecommunications Regulatory Authority have a significant supervisory and enforcement role in keeping an eye on the internet, fighting cybercrime, and offering prompt technical assistance when needed. In 2024, Positive Technologies

In order to instill ideas of digital citizenship and encourage responsible online conduct, awareness campaigns have been started at the school and community levels, and numerous UAE universities have implemented specialized programs in information security and digital law at the educational and pedagogical level (Sharabi, 2023). These programs show that the UAE understands the importance of integrating community education with legal deterrence, which advances the institutional maturity of the Emirati model.

As a result, when comparing the institutional efforts of the two nations, the UAE has made relative development in terms of organization, institutional independence, and role clarity. To counteract digital deviations at the governmental and societal levels, Jordanian efforts must continue to improve coordination, offer technical assistance, and create long-term strategies.

2.3.4 Recent Trends in Cyber Legislation Development (Comparative Approach)

Globally, cyber laws are always evolving due to the intricacy of cybercrime and the speed at which technology is developing. As a result, there is now a legislative movement toward implementing cyber laws in a way that is adaptable, participatory, and predictive. The two most notable recent trends are the use of flexible, extensible definitions that enable the incorporation of new kinds of deviance without the need for frequent legislative modifications and the redrafting of legal texts using precise technical terminology. To increase the comprehensiveness of legislative frameworks, some legal systems have also taken the step to incorporate subjects like biometric privacy, digital infrastructure security, and artificial intelligence within cybercrime statutes. Gupta (2025)

Proactive cyber laws that safeguard the "national digital space" as part of national security have been enacted by South Korea, France, Singapore, and other advanced international models. In addition to working with the commercial sector to improve technical and legislative preparedness, they have set up national systems for quick reaction to cyber catastrophes. These nations have also started revising their laws to conform to international norms for digital governance and embrace the ideas of accountability and transparency in cyber operations. (Mashima et al., 2024)

However, in order to ensure efficient law enforcement in various digital environments, some nations are moving toward implementing multi-level legislation, issuing general federal laws supplemented by specialized executive regulations addressing each sector separately (such as education, health, and trade). Additionally, several comparable experiences highlight the establishment of alliances with multinational digital firms through contracts to work together in identifying offenders or managing information that violates intellectual property

rights. Data privacy and digital sovereignty present difficulties for this development. (Shires, 2021)

With the adoption of a comprehensive and modern law (2021) that incorporates digital protection mechanisms and technical tracking, as well as the integration of rumors, hacking, and content-related crimes into a unified legislation, the UAE's experience at the Arab level shows a clear openness to these modern trends, placing it among nations with an advanced legislative structure. Jordan and a few other Arab nations, on the other hand, are still adjusting to these changes slowly and are creating new laws without achieving a coherent framework. This necessitates implementing a legal philosophy that is in line with the dynamics of digital crime and quickening the speed of legislative reform. (Positive Technologies, 2024) This comparative overview makes it evident that contemporary trends are founded on the idea of "proactive legislation," which keeps up with technological advancements, depends on an efficient institutional framework, and strikes a balance between upholding digital rights and providing legal protection. These trends are not restricted to stiffening penalties or broadening the scope of criminalization.

RESEARCH METHODOLOGY

This study aims to compare the laws of Jordan and the UAE to assess the effectiveness of cyber laws in curbing deviant behavior in the digital space. In view of the above challenges, the descriptive analysis method was selected as the best method. This method describes the current legal texts and examines their actual effectiveness, thereby exploring legal and social phenomena and analyzing their dimensions and characteristics.

To achieve the research objectives, a questionnaire was designed and distributed to a sample of legal and technical experts from Jordan and the UAE, including academics, judges, lawyers, and cybercrime experts. The survey aims to understand the opinions and evaluations of the respondents on the effectiveness of the cyber laws of the two countries in avoiding legal proceedings, preventing digital crimes, timely enforcement, and adapting to technological advances. The study also draws on secondary data from government sources, previous academic research, and legal literature to understand the cyber legislative framework and evaluate the strengths and weaknesses of its implementation. The purpose of the study is to gain a comprehensive understanding of the effectiveness of the current legislation by integrating the results of field analysis and theoretical research, and to propose development recommendations in line with current digital issues.

Validity and Reliability of the Study Instrument

To ensure the accuracy and appropriateness of the study instrument (the questionnaire), both **validity** and **reliability** were thoroughly assessed using standard statistical procedures.

By presenting the questionnaire to a panel of academic specialists from Jordanian and United Arab Emirates universities who specialize in cybersecurity law and scientific research, content validity was demonstrated. Their comments were on how well the items addressed the goals of the study and how clear, pertinent, and sufficient they were. The necessary changes were made to improve the tool's validity in response to their recommendations.

In order to evaluate internal consistency, reliability was confirmed by computing the Cronbach's Alpha coefficient for every questionnaire part. The following were the outcomes:

- Implementing cyber laws presents difficulties: α = 0.83
- Laws' effectiveness in deterring and preventing: α = 0.87
- The Jordanian and Emirati legal models differ in that α = 0.85

Since all of these numbers are over the permissible cutoff of 0.70, they demonstrate a high degree of internal consistency. This attests to the instrument's consistency and stability in measuring the desired variables.

As a result, the questionnaire was accepted as legitimate and trustworthy for use in the field, enabling hypothesis testing and confident result interpretation.

3.1 Research Design and Data Collection

The concepts in this research were measured using various variables derived from previous studies. These data were evaluated using a 5-point Likert scale (1 = strongly disagree; 2 = disagree; 3 = neutral; 4 = agree; 5 = strongly agree).

The researcher distributed 180 questionnaires directly to the sample members by hand. A total of 165 valid questionnaires were retrieved, resulting in a response rate of 91.7%. The following table shows the number of distributed and retrieved questionnaires.

Table (1) Lists of questionnaires distributed and returned according to the sample

Study sample	**Distributed forms**	**Correct forms**		
		Number	**Response rate**	**Percentage of total**
1. Practicing legal professionals	90	83	96%	53.33%
2. Academics and researchers in law and information technology faculties	45	40	88.89%	22.22%
3. Employees in relevant judicial and security institutions	45	42	97.78%	24.44%
Total	180	165	94.74%	100%

3.3 Data Collection Methods

The researcher relied on a questionnaire to collect data to achieve the study's objectives and test its hypotheses. The questionnaire included a set of questions designed to reflect the study's main objectives. A five-point Likert scale was used to assign a relative weight to responses to each statement, ranging from one to five points. The questionnaire was divided into three main groups, as follows:

- **Group One**: This group consists of six comments about the institutional and practical difficulties in putting cyber laws into place to deal with aberrations in digital behavior. These difficulties include sluggish court processes in addressing cybercrimes, inadequate digital legal awareness, difficulty establishing cybercrime, a lack of technical and legal capabilities, and poor coordination amongst pertinent institutions.
- **Group Two**: This group consists of five statements that highlight the benefits of cyber laws in Jordan and the United Arab Emirates. These include the efficiency of penalties in lowering the number of digital crimes, the thoroughness of legal texts in addressing behavioral deviations, the lucidity of legal definitions of cybercrimes, the adaptability of laws to keep up with technological advancements, and the role of laws in boosting cybersecurity and safeguarding personal information.
- **Group Three**: This group comprises six statements that evaluate the distinctions between the Jordanian and Emirati models for dealing with digital deviations. These include the comprehensiveness of the Emirati decree in comparison to the Jordanian law, the speed at which the law is enforced in the United Arab Emirates, the Jordanian model's balance between protection and rights, the degree of institutional coordination in the United Arab Emirates, and the modernity of the comparative legal structures in each nation.

3.4 Data Processing and Analysis Methods

To achieve the research objectives, the following statistical methods were used, in addition to the aforementioned Likert method:

1. Calculating the reliability and validity coefficient (Cronbach's alpha).
2. Descriptive statistics for the data (arithmetic mean and standard deviation).
3. Inferential statistics (chi-square test).

The researcher used the Statistical Analysis for Social Sciences (17.Spssv) program and the statistical analysis program (16.Minitapv) to analyze the data collected through the questionnaires to select the research hypotheses.

3.5 Testing the Validity and Reliability of the Questionnaire

This was done using the Cronbach's alpha scale to measure the validity and reliability of the questionnaire statements. This was done to determine the degree of consistency in the study sample's responses to the questionnaire questions, and thus to the three study hypotheses, and the extent to which its results can be generalized to the study population, as follows:

Table (2) Results of the validity and reliability test for the three study hypotheses

Study assumptions	**Number of statements**	**Reliability coefficient**	**Validity coefficient**
1. There are no statistically significant differences between the opinions of the study sample regarding the challenges facing the implementation of cyber legislation in reducing behavioral deviations in the digital space in Jordan and the UAE.	6	0.923	0.964
2. There are no statistically significant differences between the opinions of the study sample regarding the effectiveness of cyber legislation in Jordan and the UAE in terms of its role in prevention, deterrence, and enhancing digital security.	5	0.952	0.970
3. There are no statistically significant differences between the opinions of the study sample regarding the differences between the Jordanian and Emirati legal models in addressing digital behavioral deviations.	6	0.867	0.896
Toltal	17	0.985	0.989

It is clear from the previous table that the reliability coefficient of the questionnaire items ranges between (0.867 - 0.952), which in turn reflects the validity coefficient, which ranges between (0.896 - 0.982), meaning that the alpha value for all hypotheses is greater than (0.5), which indicates the validity of the questionnaire items and that they cover the important points under study and the possibility of generalizing the sample results to the study community.

4. Analyzing study results and testing hypotheses:

Using descriptive statistical methods (arithmetic mean and standard deviation), ranking the relative importance of the research sample responses, and using inferential statistics through the (Ka) test to determine the validity of the research hypotheses as follows:

4.1 Testing the first hypothesis:

There are no statistically significant differences between the opinions of the study sample regarding the challenges facing the implementation of cyber legislation in reducing behavioral deviations in the digital space in Jordan and the UAE.

By measuring the opinion of the study sample categories regarding the statements of the first hypothesis, the arithmetic mean and standard deviation were calculated, and the Ka test was conducted for the statements of the first hypothesis, and the results were as shown in the following table:

Table No. (3) Responses of the study sample regarding the statements of the first hypothesis

	Study sample response					**Descriptive statistics**		**Degree of approval**	**Chi-Square Test**		**Arrangement**
	Totally agree	Agree	Neutral	Disagree	Strongly disagree	Arithmetic mean	Standard deviation		Ka2 value	Significance level	
1	69	55	28	6	7						
	43.89 %	33.33 %	15.56 %	3.33%	3.89%	4.1	0.85	Agree	18.4	0.015	1
2	71	39	34	15	6						
	45%	21.67 %	21.67 %	8.33%	3.33%	3.97	0.92	Agree	17.5	0.02	5
3	70	50	20	16	9						
	38.39 %	36.11 %	11.11 %	8.89%	5%	3.95	0.85	Agree	16.8	0.03	2
4	67	40	37	10	11						
	42.78 %	25%	20.56 %	5.56 %	11%	3.9	0.95	Agree	17.2	0.025	4
5	65	44	29	17	10						
	44.44 %	24.44 %	16.11 %	9.44%	5.56%	3.94	0.87	Agree	16.5	0.03	3
6	59	58	35	10	3						
	38.33 %	32.22 %	22.22 %	5.56%	1.67%	4	0.80	Agree	17.0	0.02	2
Overall average						4.13	0.84	Agree	-	-	-

Table 3 shows sample responses to the initial hypothesis, which gauged how participants felt about laws and institutions stopping cybercrime. The survey focused on cooperation with authorities, expertise availability, law clarity, judicial process efficiency, and public awareness. Statements used a five-point Likert scale. Arithmetic means, standard deviations, and chi-square tests revealed difference significances between respondent categories.

The table results demonstrate that statement arithmetic means ranged from 3.90 to 4.10, within the consistency range, reflecting general belief that institutions and laws effectively address cybercrime. Standard deviations remained low too (0.80 to 0.95), signifying opinion homogeneity. Chi-square tests found all statements statistically significant at below 0.05, indicating real differences between sample categories like country, job, or experience.

While results signaled institutions and laws well-positioned against cybercrime, means of 3.90 to 4.10 represented agreement. Standard deviations stayed low too (0.80 to 0.95), consistent sentiment. Chi-square tests also showed

each statement statistically significant at under 0.05, with true variance between categories such as nation, career, or experience. This positive view likely stems from participants' practical online expertise, especially as Jordan and the UAE strengthen digital legal frameworks, though to varying degrees. Findings suggest continually promoting institutional expansion and human resourcing to ensure progress sustainability and enabling more effective legislation addressing digital conduct deviations.

4.2 Testing the second hypothesis:

There are no statistically significant differences between the opinions of the study sample regarding the effectiveness of cyber legislation in Jordan and the UAE in terms of its role in prevention, deterrence, and enhancing digital security.

By measuring the opinion of the study sample categories regarding the statements of the second hypothesis, the arithmetic mean and standard deviation were calculated, and the Ka test was conducted for the statements of the second hypothesis, and the results were as shown in the following table:

Table Responses of the study sample regarding the statements of the second hypothesis

	Study sample response					**Descriptive statistics**		**Degree of approval**	**Chi-Square Test**		**Arrangement**
	Totally agree	Agree	Neutral	Disagree	Strongly disagree	Arithmetic mean	Standard deviation		Ka2 value	Significance level	
1	75	41	28	11	10						
	44.44 %	28.78 %	18.33 %	8.89%	5.56%	3.92	0.75	Agree	16.5	0.03	4
2	69	43	29	16	8						
	43.89 %	23.89 %	18.89 %	8.89%	4.44%	3.94	0.76	Agree	17.0	0.02	3
3	75	36	39	10	5						
	50%	20%	21.67 %	5.56%	2.78%	4.09	0.80	Agree	16.0	0.03	1
4	74	40	31	10	10						
	49.44 %	22.22 %	17.22 %	5.56%	5.56%	4.04	0.78	Agree	15.0	0.04	2
5	9	15	33	60	48						
	5%	11.11 %	18.33 %	36.11%	29.44	2.26	1.25	disagree	22.0	0.02	5
Overall average						3.22	0.97	Agree	-	-	-

The findings of the analysis of the study sample's answers to the second hypothesis—which looks at participants' perceptions of the efficacy of cyber laws in Jordan and the UAE in terms of prevention, deterrent, and improving digital security—are shown in Table (4). The Chi-Square test was used to determine whether there were statistically significant differences between sample

categories, and the mean and standard deviation were used to examine responses to five assertions.

According to the findings, the averages of the four assertions (numbered 1-4) ranged from 3.92 to 4.09, with comparatively low standard deviations (0.75-0.80). This suggests that most sample participants concur that cyber laws help to stop behavioral abnormalities and lower the number of online crimes. Participants did not believe that these regulations increase user confidence and secure their data, as seen by the fifth statement's low mean of 2.26 and significant standard deviation of 1.25. The total mean of 3.22 was weakened, but it was still within the "agree" range. The efficiency of these regulations varied significantly throughout the various sample categories (by nation, profession, or experience), according to the chi-square test results, which revealed that all assertions were statistically significant at a level less than 0.05.

Participants' awareness of the growing importance that cyber laws have in lowering cybercrime—particularly in the areas of legal deterrence and updating legal texts to keep up with technological advancements—is credited with these results. Their favorable assessment of the first four statements demonstrated this. Nonetheless, the low rating of the fifth statement can suggest that some participants don't trust these regulations to protect personal information and create a completely safe online environment. This could be the result of real-world issues with digital privacy or field experiences. These discrepancies are probably caused by the different institutional frameworks for cybersecurity in the UAE and Jordan; the UAE has a more sophisticated infrastructure for content banning and data protection, which accounts for the different opinions of sample participants. All of these results suggest that in order to increase the efficacy of laws addressing different facets of digital security, user confidence must be increased by implementing rules protecting digital privacy and increasing community involvement in the creation of cybersecurity policies.

4.3 Testing the third hypothesis:

There are no statistically significant differences between the opinions of the study sample regarding the differences between the Jordanian and Emirati legal models in addressing digital behavioral deviations.

By measuring the opinion of the study sample categories regarding the statements of the third hypothesis, the arithmetic mean and standard deviation were calculated, and the Ka test was conducted for the statements of the third hypothesis, and the results were as shown in the following table:

Table (5) Responses of the study sample to the statements of the third hypothesis

	Study sample response					**Descriptive statistics**		**Degree of approval**	**Chi-Square Test**		**Arrangement**
	Totally agree	Agree	Neutral	Disagree	Strongly disagree	Arithmetic mean	Standard deviation		Ka2 value	Significance level	

1	69	46	29	22	9	3.99	1.10	Agree	13.4	0.015	3
	43.89 %	28.33 %	15.11 %	6.67%	5%						
2	70	46	21	15	13	3.97	1.05	Agree	12.5	0.020	4
	47.22 %	25.56 %	11.67 %	8.33%	7.22%						
3	76	42	29	14	4	4.13	1.02	Agree	11.8	0.022	2
	50.56 %	23.33 %	16.11 %	7.78%	2.22%						
4	14	15	19	67	50	2.28	1.30	disagree	22.5	0.015	6
	7.78%	11.11 %	10.56 %	42.78%	27.78 %						
5	74	41	20	17	13	3.95	1.05	Agree	10.2	0.022	5
	46.67 %	25.56 %	11.11 %	9.44%	7.22%						
6	84	44	23	9	5	4.24	0.91	Agree	5.8	0.01	1
	55%	24.44 %	12.78 %	5%	2.78%						
Overall average						4.20	0.99	Agree	-	-	-

The findings of the third hypothesis test, which attempts to gauge the study sample's opinions regarding the distinctions between the Jordanian and Emirati legal frameworks for dealing with digital behavioral abnormalities, are shown in Table (5). The Chi-Square test and the arithmetic mean and standard deviation were used to assess the significance of statistical differences between the sample groups based on the participants' answers to six questions.

According to the results, the majority of sample members agreed that there is a real difference between the two laws in terms of comprehensiveness, implementation, and institutional structure. Five of the six statements fell within the "agree" level, with arithmetic means ranging between 3.95 and 4.24 and an acceptable standard deviation (between 0.91 and 1.10). The sample disagreed that the UAE has total institutional supremacy, as seen by the fourth statement's low mean (2.28) and high standard deviation (1.30). This could be a sign of greater appreciation for certain elements of the Jordanian experience or a degree of relative balance.

There were statistically significant differences between sample categories (e.g., country or professional background) in their evaluation of the degree of differences in legal models, according to the chi-square test results, which also demonstrated statistical significance for all statements at a significance level below 0.05.

These results reflect a widespread awareness among participants that UAE cyber legislation enjoys a higher degree of comprehensiveness and institutional readiness compared to Jordanian legislation. This is due to the nature of the UAE model, which is based on centralized decision-making and the delegation of broad executive powers to regulatory bodies, particularly with regard to content blocking and the rapid and efficient tracking of cybercrime.

The findings also demonstrate that the sample values Jordanian law's flexibility in certain areas, especially with regard to the judiciary's function. This explains why they agree with the third claim, which states that the Jordanian model gives the judiciary more authority than the United Arab Emirates. Some participants' lack of belief in the absolute superiority of the UAE's institutional structure or some sample members' ignorance of the specifics of both countries' institutional structures could be the reason for the relative rejection of the fourth assertion.

Overall, these results demonstrate that the two legislative models differ not only in terms of administrative or technical efficiency but also in terms of legal and political philosophy when it comes to striking a balance between cybersecurity requirements and constitutional rights. This demonstrates the value of a comparative analysis in determining each system's advantages and disadvantages.

DISCUSSION

The study offered novel perspectives on cybersecurity laws in the digital era. The investigation of institutional obstacles to applying regulations validated the importance of a well-designed organizational framework and legal infrastructure. Most participants acknowledged available technological capabilities and skilled personnel, as well as coordinated judicial and security agencies. These conclusions align with prior work emphasizing efficient cross-agency collaboration to reduce cyber risks. As the Legal Institutional Theory posits, effectiveness depends not just on content but enforcing bodies' preparedness and capacities, supported here.

The assessment of laws' abilities to prevent, deter, and cultivate trust in digital safety addressed the second hypothesis. While respondents doubted the legislation's power to foster trust, particularly regarding privacy and overreach concerns, they acknowledged fines, clarity, and flexibility's roles. Consistent with existing analyses, transparent application combined with ongoing awareness beyond legal obligations reportedly influence attitudes and conduct. The results lend empirical backing to Legal Utilitarianism's stance that regulations should tangibly impact societal behaviors.

The study's examination of perceptions regarding the legal distinctions between Jordan and the United Arab Emirates found statistically significant results. Jordan's judiciary was regarded as more balanced but less agile, while the UAE's was viewed as more proactive, centralized, and technologically integrated. This divergence highlights Comparative Public Law Theory, which holds that core philosophies surface in policy variances: Jordan emphasizes judicial autonomy and constitutional safeguards more so, whereas the United Arab Emirates supports executive efficiency and state-led digital oversight. These conclusions align with previous research by Sharabi and Rjoub et al., who noticed Arab nations differ in institutional investment and legislative adaptability.

Therefore, the investigation supports the notion of Digital Legal Governance, a framework envisioning cyberlaw as a nimble response to technological reality instead of static text. To effectively handle digital behavioral deviations, this theory advocates relentless organizational change, flexible legislation, and interagency alignment. Additionally, the study backs the idea of "legal adaptation to digital transformation," which proposes laws should evolve in accordance with social, technical, and human rights issues while staying receptive and inclusive.

In practice, the outcomes indicate robust infrastructure, trained personnel, and aligned enforcement tactics should pair with effective cyber regulations. Despite thoroughness, legal codes must synchronize with real-world applications as well as the functional abilities of judicial and security bodies. The need for regional benchmarking is exhibited in the contrast between Jordan and the United Arab Emirates: Emirati knowledge in legislative dynamism and administrative coherence, especially regarding user protection, interagency cooperation, and content-filtering capacities, can benefit Jordanian policymaking.

Additionally, the sample's varying opinions on institutional overreach and digital privacy highlight the need to incorporate accountability procedures and constitutional protections into cyber laws. Establishing legitimacy and public trust requires this. It is also the duty of educational institutions to foster legal knowledge and digital literacy. Future generations can be better prepared for responsible digital citizenship by including cyber law and ethics into university curricula. Protecting individual rights while strengthening institutions is crucial for effective legislation. This paper concludes by reiterating that responsive cyber governance must consider technological progress and safeguard fundamental freedoms. To balance security with human dignity in the digital world, the report urges policymakers in Jordan and the United Arab Emirates to collaboratively implement adaptable reforms respecting civil liberties. Data-driven analysis shows respecting rights, boosting public confidence, and clarifying laws are key to frameworks befitting our changing reality. The best systems marry technological awareness with people-centered safeguards, tempering deterrence with liberty.

CONCLUSION

Effective cyber law has become necessary in view of the world's rapidly changing digital landscape in order to keep up with the times and handle the increasing behavioral abnormalities within online spheres. By assessing institutional, legislative, and executive factors, this analysis aimed to examine the potency of cybersecurity regulations in Jordan and the United Arab Emirates regarding their ability to prevent, discourage, and strengthen cybersecurity.

The examination determined that there exists a broad perception of progress in cyber legislation in both nations following an assessment of replies from a diverse sample of legal, security, and academic experts. Effectiveness remains influenced by institutional issues and philosophical differences in statutes, nonetheless. The analysis found discrepancies in how some factors were

evaluated, particularly those pertaining to legal infrastructure, executive response times, and societal trust. Furthermore, the study enhanced the theoretical framework of cyber legislation across the Arab world through this comparative analysis, which also served as a basis for suggestions that support regional and national policy within this crucial area.

Suggestions

A number of strategic recommendations are put forth in light of the findings of the nuanced study into improving the efficacy of cyber laws and solving perplexing anomalies in online behavior. Primary national training initiatives are desperately needed to bolster the human resources tasked with cybercrime response through judicious, investigative and legal counsel programs providing participants with the most current legal information and sophisticated technical knowledge to deal with intricate and evolving cybercrimes.

Furthermore, a dynamic and discerning legislative review process must be instated to guarantee the routine reexamination and modification of existing cyber laws in view of the rapid advancements in technology. The goal of this considerate review process should be to judiciously broaden the legal framework to encompass novel risks such as ingenious social engineering tactics, potentially harmful use of AI, and under-regulated data manipulation offenses.

It is advised that security, judicial and legislative bodies judiciously establish permanent joint units to improve synergistic collaboration. Establishing harmonious databases, controlling digital incident response protocols, and encouraging timely information sharing should be the principal goals of these units. More effective cybercrime investigation, prosecution and prevention across national authorities will be ensured by such well-coordinated cooperation.

The illuminating survey also emphasizes how paramount it is to restore public assurance in cyber laws. Comprehensive national awareness programs judiciously informing people of their rights and obligations online can help achieve this. To encourage transparency and inclusivity in the legislative process, civil society organizations ought to take an active role in thoughtful public dialogues about law reforms.

Lastly, this study's nuanced comparative analysis emphasizes the importance of implementing judicious regional models. Jordan can specifically benefit from the UAE's sophisticated institutional and legislative framework while customizing reforms to judiciously fit its own political and constitutional circumstances. This strategy would contribute to a more adaptable and citizen-centered legal environment by modernizing Jordan's legal system in a way that judiciously strikes a balance between civil liberties and digital security.

REFERENCES

First: Books

1. Al-Amarat, & Al-Hamamseh. (2022). Cybersecurity, Concept and Challenges of the Era. Dar Al-Khaleej for Publishing and Distribution, Jordan.
2. Al-Jbour, M. (2012). Mediator in the Penal Code, General Section. Dar Wael for Publishing and Distribution, Amman.
3. Gupta, B. B. (2024). Digital Forensics and Cyber Crime Investigation: Recent Advances and Future Directions. CRC Press.
4. Gupta, B. B. (2025). Post Quantum Cryptography Algorithms and Approaches for IoT and Blockchain Security. Elsevier.
5. Islam, M. R. (2024). Generative AI, Cybersecurity, and Ethics. Wiley.
6. Shires, J. (2021). The Politics of Cybersecurity in the Middle East. Hurst.

Second: Journal articles and academic theses

7. Abdel Hamid, A., & Molook, N. (2020). "Cybercrime and Its Impact on the Threat to Cultural Security in Algeria". Al-Mufaker Journal for Legal and Political Studies, 3(2).
8. Abdul-Baqi, L., & Khaitan, I. (2021). "International Responsibility for Damages Caused by Cyber Attacks". Journal of Legal Sciences, 36(Special Issue, Part 2).
9. Abouzied, A., Alam, F., Ali, R., & Papotti, P. (2025). "Combating Misinformation in the Arab World: Challenges & Opportunities". arXiv preprint. https://arxiv.org/abs/2506.05582
10. Al-Baraiseh, H. (2021). The Moral Pillar of Cybercrime According to the Jordanian Penal Code (Master's thesis). Middle East University, Jordan.
11. Al-Barrak, H. (2020). "The Legal Role of Cybersecurity in Anti-Crime". King Khalid University Journal for Human Sciences, 7(2).
12. Al Najdawi, M. H., Shwedeh, F., Abdelmoghies, M. M., Kitana, A., & Ali, A. (2024). Applying artificial intelligence in predicting educational excellence in higher education institutions: A case study in Jordanian universities. Edelweiss Appl Sci Technol, 8(6), 7273-7289.
13. Al Najdawi, M. H., & Raafat, R. (2025). Legal Protection of Foreign Investments under the Rules of International Law: A Comparative Study between the United Arab Emirates and Jordan. Journal of Posthumanism, 5(5), 2623-2640.
14. Al-Najdawi, M. H. Y. (2022). The Role of the Legislative and Legal Framework in Promoting Scientific Research in the Arab World between Current Reality and Future Prospects.(A Case Study, United Arab Emirates). Baltic Journal of Law & Politics, 15(3), 2069-2087.
15. Al-Samhan, M. A. (2020). "Requirements of Cybersecurity for Information Systems at King Saud University". Journal of the Faculty of Education, Mansoura University, 111(July).
16. AlNajdawi, M. H., Raafat, R., Aburayya, A., & Al Ghurabli, Z. (2025). Enhancing logistical efficiency in public institutions through AI: A managerial framework for regulatory and technological integration. International Journal of Industrial Engineering, 36(3), 81-92.
17. AlNajdawi, M. H., AlDabbagh, T., Raafat, R., & Aburayya, A. (2025). The Role of Administrative Governance in Enhancing Integrity and Transparency and Reducing Administrative Corruption in Public Institutions: An Analytical Study. International Journal of Industrial Engineering, 36(3), 93-106.

18. Alzahrani, I. Y., Lee, S., & Kim, K. (2024). "Enhancing Cyber Threat Intelligence in the Arab World: Leveraging IoC and MISP Integration". Electronics, 13(13), 2526. https://doi.org/10.3390/electronics13132526
19. Fawzy, I. (2019). "Cybersecurity, Social and Legal Dimensions, Sociological Analysis". Social and National Journal, 56(2).
20. Jaafar, M. K., & Musaf, M. D. (2021). "Legitimacy of Using Cyber Attacks in International Conflicts and Responsibility Thereof". Journal of Legal Sciences, 36(Special Issue, Part 4).
21. Ladadoh, A. (2021). The Compatibility of the Provisions of the Jordanian Cybercrime Law with the General Provisions of the Penal Code (Master's thesis). Middle East University, Jordan.
22. Mashima, D., Chen, Y., Roomi, M. M., Lakshminarayana, S., & Chen, D. (2024). "Cybersecurity for Modern Smart Grid Against Emerging Threats". arXiv preprint. https://arxiv.org/abs/2404.04466
23. Mustafa, I. (2022). "Cybersecurity Hacking Crime, Data and Information Use Protection in Egyptian Law". Journal of the Faculty of Law, Cairo University – Khartoum Branch, 12(3).
24. Rjoub, G., Bentahar, J., Abdel Wahab, O., Mizouni, R., et al. (2023). "A Survey on Explainable Artificial Intelligence for Cybersecurity". arXiv preprint. https://arxiv.org/abs/2303.12942
25. Sharabi, W. A. N. (2023). "The Cybersecurity Practice in Saudi Universities to Protect the Intellectual Rights of Faculty Members' Publications". International Journal of Instruction, 16(4), 173–188. https://doi.org/10.29333/iji.2023.16411a

Third: Electronic and online sources

26. AlSahafi, R. (2020). "Cybercrime". Comprehensive Multidisciplinary Electronic Journal, 24. https://www.eimj.org/uplode/images/photo.pdf
27. Cyber Security Report. (2021). Jordan Media Authority, Studies, Communication and Relations Department.
28. Odeibat, A. (2022). "Who is the Cyber Criminal?". E3arabi website.
29. Positive Technologies. (2024). Cybersecurity Threatscape in the Middle East: 2023–2024. https://global.ptsecurity.com/research/analytics/cybersecurity-threatscape-in-the-middle-east-2023-2024/