Pakistan Journal of Criminology
Vol. 16, No. 04, October—December 2024 (111-127)

Cybercrime in the Middle East: A Comparative Analysis with Global Trends

Ali Jabbar Salih[1],
Farouq Ahmad Faleh Alazzam[2]

Abstract

This article aims to present a modern methodological approach that will allow the selection of the optimal strategy for combating cybercrime in the Middle East. The research methodology requires using methods that would enable the assessment of the study problem and help solve it effectively; thus, the hierarchy analysis developed by T. Saaty was widely used by researchers and practitioners in solving economic problems. The method of paired comparison and the involvement of experts through the Delphi method was also used. This paper explicitly defends the choices made for countering cybercrime, stressing that these choices should be tailored to the changes in the Middle East. The study acknowledges this restriction by concentrating only on the features of cybercrime in Middle Eastern nations. To gain a more profound understanding of the problem, future studies should investigate cybercrime in other areas, such as EU nations.

Keywords: law, cybercrime, Middle East, Modeling, Global Trends, Strategy

Introduction

Cybercrime has become an essential global problem for most countries. This is mainly due to the widespread use of digital technologies and the growing digital dependence of modern society on this technology. The Internet has become integral to various spheres of public life, including the economic and financial systems, healthcare, public administration, and others. Individuals who commit criminal acts in digital environments and cybersecurity commonly seek vulnerabilities in existing software, allowing them to acquire material resources, finances, or confidential information illegally. The problem is exacerbated by the fact that the Internet transcends geographical and national boundaries, allowing cybercriminals to commit offences from anywhere in the world. Furthermore, the lack of international cooperation also facilitates their criminal activities.

Cybercrimes are broad and ever-changing, reflecting technological breakthroughs and organisations' increasing data protection strategies. A typical

[1] Faculty of Law - Jadara University, Irbid, Jordan. Alijs@jadara.edu.jo, Orcid ID : 0000-0003-1975-1173
[2] Faculty of Law – Jadara University –Irbid – Jordan. Email: f.alazzam@jadara.edu.jo, Orcid ID: 0000-0001-7407-4828

form of cybercrime is Phishing, when attackers deceive victims into disclosing sensitive information. Ransomware attacks occur when cybercriminals encrypt a victim's files and demand payment for their release and to Identity theft occurs when personal information is stolen and exploited for fraud (Alazzam et al., 2024).

Cybercriminals often target businesses and governments with sophisticated hacking techniques that can lead to critical financial and operational disruptions. These activities cause immediate financial loss and long-term damage to the reputations of the affected organisations, as well as leading to damage to public trust (Alazzam et al., 2024; Applegate, 2015; Saleh et al., 2020). Combating cybercrime mainly requires cooperation among various stakeholders, including governments, private corporations, and international bodies. Additionally, legal frameworks and cyber laws should be continuously updated to address new challenges cyber threats may pose (Yemanov et al., 2023).

Furthermore, there is an increasing investment in cyber security measures such as advanced encryption technologies, multi-factor authentication, and continuous IT infrastructure monitoring. Despite these efforts, the dynamic nature of cyber threats and the pace at which new technologies are adopted mean that the battle against cybercrime is ongoing. Education and awareness campaigns are critical to equipping individuals and organisations with the knowledge and tools to protect themselves from cyber attacks (Fig.1) cited from Chen, Hao, Ding, Jiang, Dong, Zhang, and Gao, (2023) presents the average of cyberattacks globally.

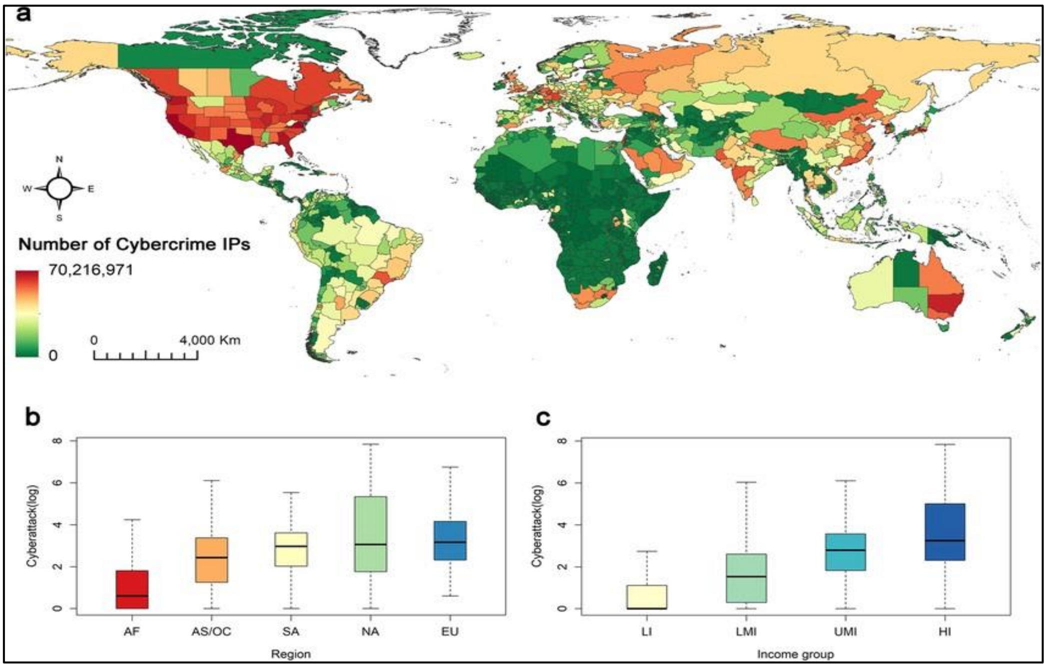
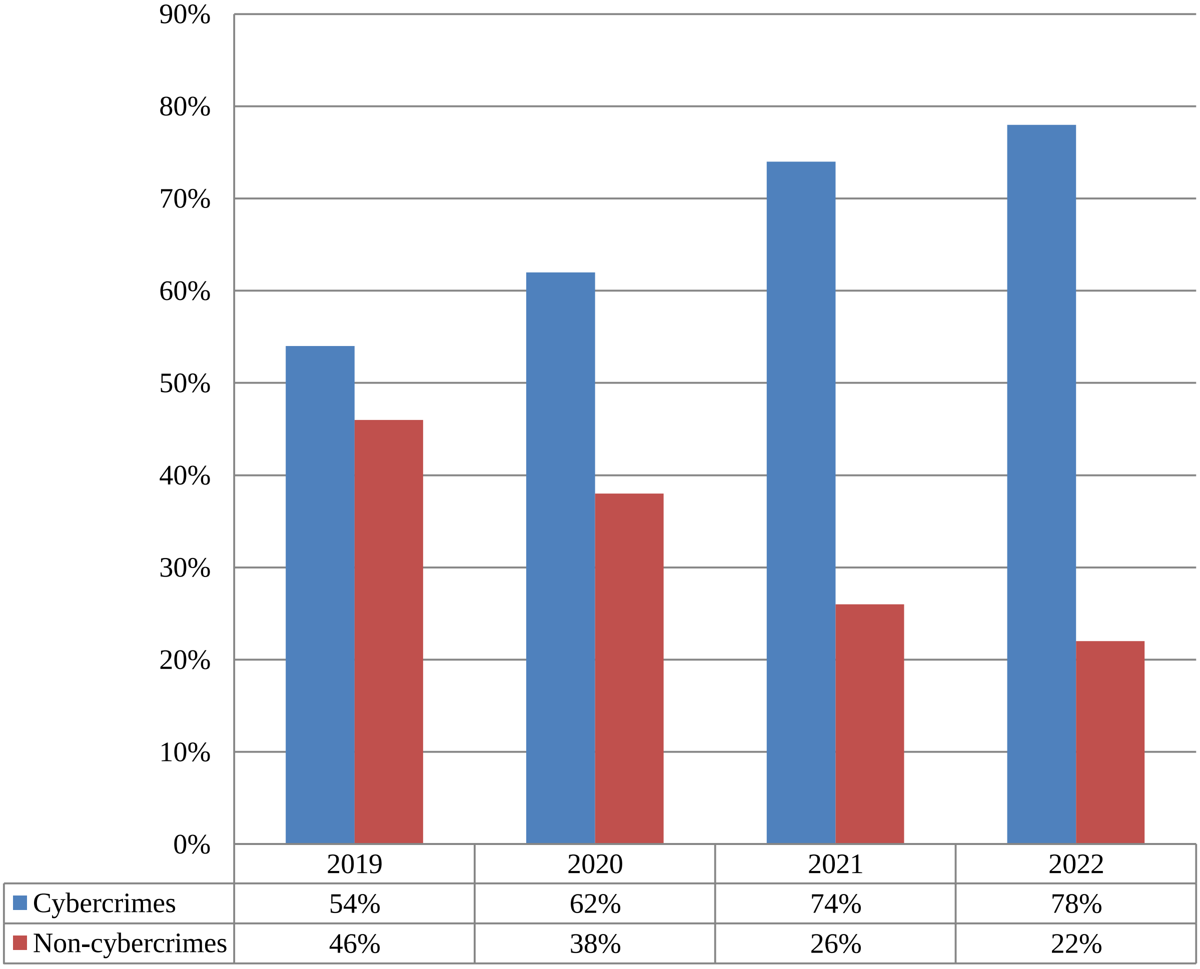


Figure 1. Global Cybercrime: World Trends (Chen et al., 2023).

The Middle East's fast-developing digital landscape and geopolitical complexity have contributed considerably to an upsurge in cybercrime. As Middle Eastern countries spend extensively on digital infrastructure and technology to diversify their economy away from oil dependency, the digital world has expanded enormously. This expansion has provided fraudsters with more opportunities to exploit flaws in systems that may not yet have fully built cybersecurity safeguards (Alazzam et al., 2024).

The region's strategic importance also makes it a target for cyber espionage and state-sponsored attacks, further complicating the cybercrime landscape (Fig.2).



	2019	2020	2021	2022
🟦 Cybercrimes	54%	62%	74%	78%
🟥 Non-cybercrimes	46%	38%	26%	22%

Figure 2. Cybercrimes in Middle-East

Cybercrime in the Middle East takes various forms and types, from individual types of financial fraud to the implementation of multiple types of phishing schemes aimed at destabilising the activities of individuals or large enterprises and ending with massive cyber-attacks on the digital networks of government agencies. Moreover, major cyber-attacks are aimed at disrupting the operation of critical infrastructure, stealing large amounts of crucial confidential information and other actions that can pose a real threat to national security (Alazzam et al., 2024).

Examining cybercrime in the Middle East, one can notice that the region often uses advanced persistent threats (APTs), which can go unnoticed by responsible authorities for a long time. The growth in mobile banking and e-commerce users has only increased the number of these types of cyber-attacks, opening up new ways for attackers to obtain confidential information and the possibility of committing financial fraud (Alazzam et al., 2023).

Active cybercrime has urged the government and commercial sectors to intensify their efforts to combat these threats. Many Middle Eastern countries have begun to establish more effective digital regulatory frameworks and cybersecurity security measures. A significant aspect of these activities is the active participation of the business and public sectors, intending to increase the effectiveness of these projects. Investing in protection and monitoring technologies is also crucial in combating cybercrime. This essay provides a modern analytical approach to determining the best strategy for combating cybercrime in the Middle East. The purpose of the article is to present a modern methodological approach that will allow the selection of the optimal strategy for combating cybercrime in the Middle East. Therefore, the object of study is cybercrime in the Middle East.

Literature Review

When analysing the potential impacts of cybercrime in the Middle East, conducting a thorough and detailed review of the relevant literature on the topic is crucial. Such an analysis will allow us to draw preliminary conclusions and identify possible ways for further scientific research to identify more effective ways to combat cybercrime.

For example, Morina et al. (2023) explored the management system's nuances and analysed the effectiveness of combating cybercrimes. The study provides a clear understanding of the range of modern cybersecurity procedures, identifying possible problems. In particular, the role of the regulatory framework in these processes. Romsaiyud et al. (2017) made a significant scientific contribution to cyber threats, an essential issue in cybersecurity today. Their automated discovery system using template patterns provided a valuable basis for further scientific research.

A study by Yemanov et al. (2023) formulated models for integrating cybersecurity measures into state and regional governance systems. The study provided an understanding of modern hierarchy and modelling methods in cybersecurity and the protection of critical infrastructure from cyber threats. In addition, the conclusions made by scientists regulate the importance of effective communication between government authorities and the private sector.

Dumchykov et al. (2022) examined cybercrime as a national security threat, offering insights that can be paralleled in the Middle Eastern context where similar geopolitical and cyber threats prevail. This comparative analysis helps understand nations' shared and unique vulnerabilities at the periphery of Europe and the Middle East.

Alazzam et al. (2024) discussed the impact of cybercrime on business management strategies, emphasising the need for adaptive approaches in commercial activities to mitigate cyber risks. This study is particularly relevant for the Middle East, where economic diversification efforts rely heavily on digital technologies. Lainjo (2020) investigated network security's implications on program management, providing insights that are crucial for organisations in the Middle East aiming to secure their operations against cyber threats. The principles outlined are applicable globally, demonstrating the universal challenges and strategies in network security. Jarvis et al. (2014) delved into cyberterrorism, a significant concern for the Middle East, given its geopolitical landscape. The findings, derived from a survey of researchers, offer a nuanced view of cyberterrorism's perceived threats and realities, which are essential for regional security analysis. Rahmat et al. (2023) presented a novel approach to classifying cybercrime cases under Indonesian law, which can inform legal and regulatory strategies in the Middle East. Their methodology, using a hybrid of mutual information and support vector machines, demonstrates the potential of machine learning in legal contexts. This technique could be replicated in Middle Eastern jurisdictions (Table 1).

Table 1. The main gaps in the literature review

Gaps	**Characteristics**

Regional Specificity and Global Applicability	While focusing on the Middle East is essential due to its unique socio-political and technological landscape, there is a notable gap in comparative analysis with other regions. The literature tends to silo regional studies, which might overlook the potential learnings and applications from areas that have faced similar cybersecurity challenges. This limitation can restrict the broader applicability and adaptability of the strategies developed solely for the Middle East. Future research could benefit from analysing how strategies developed in other regions, such as the EU or Asia, where cybercrime also presents significant challenges, can be adapted or might influence cybersecurity practices in the Middle East.
Integration of Interdisciplinary Approaches	The existing literature often focuses on economic and technical strategies for combating cybercrime, using tools like the Analytic Hierarchy Process and the Delphi method for expert opinions. However, there is a gap in integrating approaches from other relevant disciplines, such as psychology, sociology, and law. Cybercrime is not only a technical issue but also involves significant human and societal elements. Understanding the motivations of cybercriminals, the social impact of cybercrime, and the legal frameworks governing cyber activities is crucial. An interdisciplinary approach could enrich the research's methodological rigour and practical outcomes.
Dynamic Nature of Cyber Threats	Another critical gap in literature is the static nature of many cybercrime studies. Cyber threats evolve rapidly, with new methods of attack developed as quickly as old ones are mitigated. Literature that fails to address these threats' dynamic and ever-evolving nature may soon become outdated. There is a need for ongoing, real-time, or near-real-time studies that can adapt to new data and trends. This would involve developing adaptive methodologies that are responsive to current threats and predictive of future vulnerabilities.

Addressing these gaps could significantly enhance the effectiveness and relevance of strategies developed to combat cybercrime in the Middle East. It could provide a blueprint for other regions grappling with similar issues. The scientific task is to create a modern methodological approach to choosing the optimal strategy to combat cybercrime in the Middle East.

Methodology

Our chosen methodology will provide a qualitative synthesis of qualitative and quantitative research methods to provide a comprehensive understanding of the nature of cybercrime and the effectiveness of different types of countermeasures. Our study used a mixed-methods approach, combining analysis of existing datasets with qualitative information from experts in cybersecurity, cybercrime and the Middle East. The approach we chose was formed to conduct a qualitative assessment of strategies to combat cybercrime and adapt to the realities of the functioning of the Middle East.

The Analytic Hierarchy Process (AHP), developed by Thomas L. Saaty, is utilised to handle complex decision-making and to help prioritise the elements that most significantly impact cybercrime defence strategies. AHP helps in breaking down the decision problem into a hierarchy of more easily comprehended sub-problems, each of which can be analysed independently.

The Delphi method incorporates expert opinions and achieves a consensus on the most effective strategies for combating cybercrime. This technique involves a series of questionnaires sent to a panel of experts, with feedback provided in multiple rounds. The experts remain anonymous to each other to prevent bias, and the iterative process continues until a consensus is reached on various elements of cybercrime strategy. Quantitative data on cybercrime's prevalence, type, and impact in the Middle East are collected from multiple cybersecurity databases and reports. This data is then analysed using statistical tools to identify trends and patterns. Qualitative data from expert responses is coded and analysed to extract thematic insights on cybercrime strategies.

Ethical considerations, including the confidentiality of expert identities and the secure handling of sensitive data, are rigorously maintained throughout the research process. By employing these methodologies, the study aims to provide a systematic and strategic framework to guide the selection of effective cybercrime countermeasures in the Middle East, contributing valuable insights into regional and global cybersecurity contexts.

Results

The method of analysing hierarchies consists of constructing a hierarchical model, determining the sums of the elements of the columns of square inversely symmetric matrices, and checking the consistency of the results. The method is based on taking into account the opinions of experts, formed according to the scale of relative importance of objects, which is given below:

1. Comparable equivalent global trends.
2. One trend is slightly superior to the other.
3. One global trend is superior to another.
4. One global trend is significantly superior to another.
5. One global trend is absolutely superior to another.

On the advice of experts, for the needs of this stage of the study, some global trends in the external environment, which are logically connected, were "united."

Thus, we will highlight the most significant ones and provide them with the appropriate mathematical designation:

GT1. Ransomware Attacks. Ransomware has become one of the most prevalent and disruptive cyber-attacks globally. These attacks involve malware that encrypts the victim's data, with the attackers demanding a ransom to provide the decryption key. This trend has seen significant growth due to the lucrative payouts from organisations needing access to critical data. Such attacks highlight the necessity for robust backup systems and advanced security protocols.

GT2. Phishing Scams. Phishing remains a primary method for cybercriminals to exploit users to provide sensitive information, such as login credentials and credit card numbers. This trend has evolved with more sophisticated social engineering techniques that manipulate users by mimicking legitimate sources more convincingly. Understanding phishing tactics is crucial for developing effective awareness and training programs.

GT3. IoT Vulnerabilities. With the exponential growth of Internet-connected devices, from smart home products to industrial IoT, vulnerabilities in these devices have become a major concern. Cybercriminals exploit these weaknesses to gain unauthorised access, disrupt services, or enlist devices in botnets for distributed denial-of-service (DDoS) attacks. This trend stresses the importance of security in the development lifecycle of IoT devices.

GT4. Cloud Security Threats. As more organisations migrate to cloud-based services, the security of cloud platforms has become a critical concern. Cyber attacks targeting cloud services can lead to significant data breaches. This trend necessitates enhanced security measures from both cloud service providers and users, including multi-factor authentication and end-to-end encryption.

GT5. State-Sponsored Cyber Activities. Cyber operations conducted or sponsored by nation-states have become more prominent, including espionage, the spread of disinformation, and interference in foreign political systems. These activities often target critical infrastructure and have significant geopolitical implications. This trend requires international cooperation and robust cybersecurity policies to mitigate threats state actors pose.

Two strategic approaches can be developed to effectively address and adapt to the global trends in cybercrime, particularly within the context of the Middle East. These strategies should aim to counteract prevalent threats while considering the unique socio-economic and technological landscapes of the region:

AS1. Comprehensive Cyber Resilience Framework. Develop and implement a comprehensive cyber resilience framework that enhances the ability of organisations and governments to prepare for, respond to, and recover from cyber incidents, particularly ransomware attacks and cloud security threats. Launch extensive training programs and public awareness campaigns to educate about phishing scams and other social engineering tactics. This can significantly reduce the incidence of successful attacks.

AS2. International Collaboration and Legal Framework Enhancement. Strengthen international collaborations and enhance legal frameworks to address state-sponsored cyber activities and sophisticated phishing campaigns, fostering a cooperative approach to cybersecurity and law enforcement. Update and harmonise cyber laws to cover a broad spectrum of cyber crimes, including new forms of digital fraud, cloud breaches, and the misuse of IoT devices. Establish clear legal ramifications for cybercrimes to deter potential cybercriminals (Fig.3).

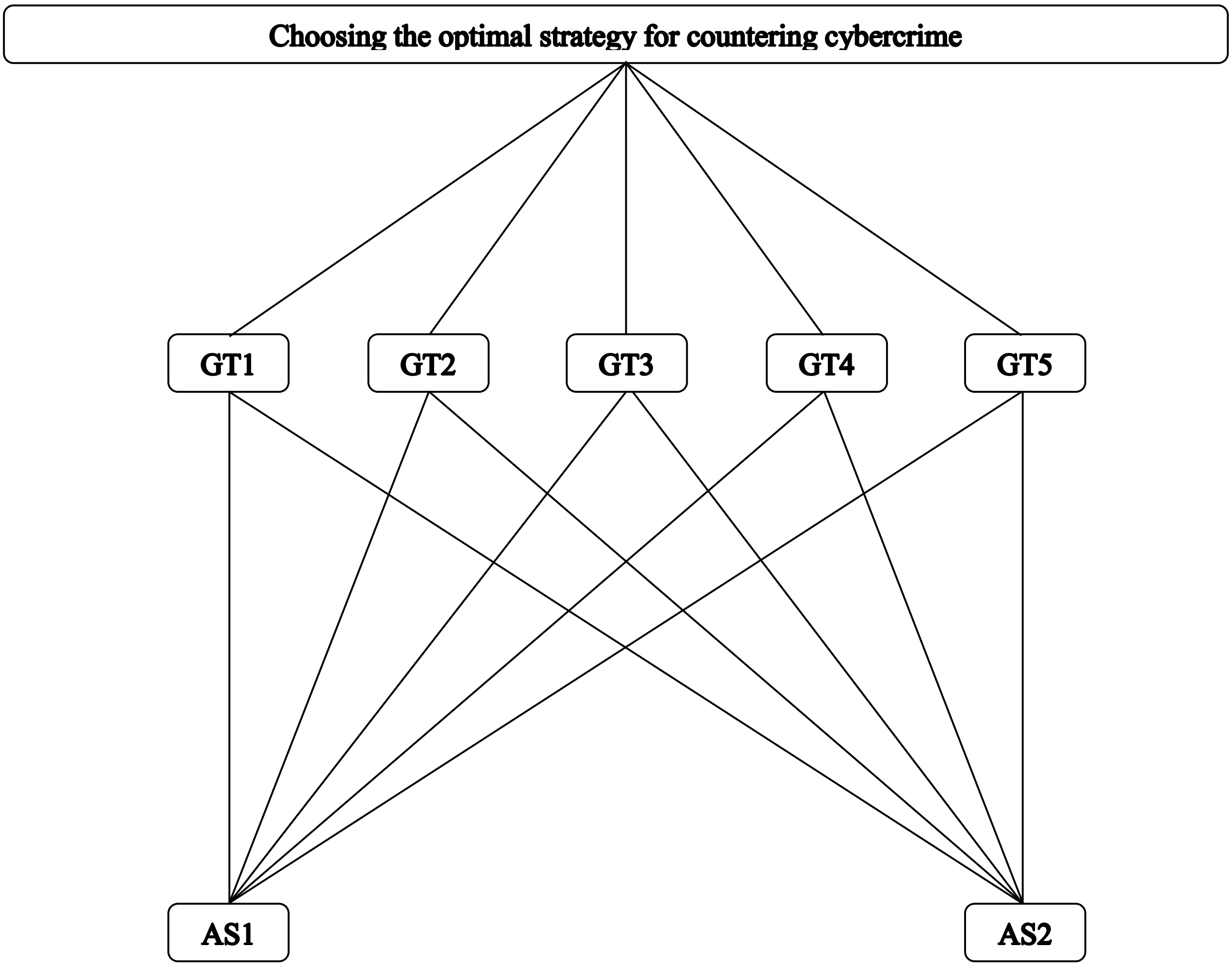


Figure 3. Cybercrimes in Middle-East

Different forms of countermeasure strategies should be evaluated now. For this, the following calculations should be performed based on this (1):

$$\frac{n*(n-1)}{2} \qquad (1)$$

Where n is the number of global trends at one level, in our case, there are five different global trends. For two compared trends, the choice of a strategy to combat cybercrime, depending on their importance and the measure of influence on the process, will have the proposed values of the corresponding element of the paired comparison matrix (Table 2).

Table 2. Matrix of results comparing global trends in cybercrime

	GT1	**GT2**	**GT3**	**GT4**	**GT5**
GT1	Value:[=1]	Value:[=1/2]	Value:[=1/3]	Value:[=3]	Value:[=2]
GT2	Value:[=2]	Value:[=1]	Value:[=1/2]	Value:[=3]	Value:[=4]
GT3	Value:[=3]	Value:[=2]	Value:[=1]	Value:[=4]	Value:[=5]
GT4	Value:[=1/3]	Value:[=1/3]	Value:[=1/4]	Value:[=1]	Value:[=2]
GT5	Value:[=1/2]	Value:[=1/4]	Value:[=1/5]	Value:[=1/2]	Value:[=1]
Sj	0.17	0.27	0.42	0.08	0.06

Next, we compare the most proposed strategies to combat cybercrime. Since there are two alternatives and five global trends in the hierarchy, it is necessary to carry out (2):

$$n\frac{m*(m-1)}{2} \qquad (2)$$

where m is the number of strategies and five comparisons of pairs of alternative strategies for countering cybercrime. Let us present the results of the calculations (Table 3).

Table 3. The main innovation in our study

Trends	**AS**
GT1	$\begin{pmatrix}1 & 3\\ 1/3 & 1\end{pmatrix}$
GT2	$\begin{pmatrix}1 & 5\\ 1/5 & 1\end{pmatrix}$
GT3	$\begin{pmatrix}1 & 1/2\\ 2 & 1\end{pmatrix}$
GT4	$\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}$
GT5	$\begin{pmatrix}1 & 4\\ 1/4 & 1\end{pmatrix}$

The selection of a cybercrime countermeasure strategy, Ui, is carried out according to the formula (3):

$$\mathrm{Uj}=\sum_{i=1}^{n} wiuij$$

(3)

By (3), we have the following options for calculating strategy values for all alternative scenarios: U_1=0.6; U_2=0.4.

The obtained results allow us to state that the AS1 Comprehensive Cyber Resilience Framework is the most acceptable. Adaptive Strategy 1 (AS1), focusing on developing a comprehensive cyber resilience framework, can be considered more effective for several reasons, particularly in its immediate impact and practical applicability across various organisations. This strategy directly targets the foundational aspects of cybersecurity: prevention, response, and recovery. By enhancing these areas, organisations and governments can improve their readiness and capabilities to handle cyber incidents as they occur, ensuring minimal impact on their operations. Furthermore, AS1 includes extensive training programs and public awareness campaigns that tackle the human element of cybersecurity, such as phishing scams and other social engineering tactics. This is crucial because human error often remains the weakest link in cybersecurity defences. Educating individuals and organisations about these threats can significantly reduce the incidence of successful attacks, making this strategy both preventative and empowering for ongoing cyber safety. In contrast, while AS2's focus on international collaboration and legal framework enhancement is crucial for long-term global cybersecurity improvement, its effects may be more diffuse and take longer to materialise, making AS1 more immediately beneficial in strengthening cyber defences.

Discussions

For example, Applegate (2015) focused on cyber conflicts and strategic operational frameworks of the digital environment, which different countries can use to shape. This study focuses on the importance of using a strategic and methodological approach to combating cybercrime. But while Applegate (2015) explored cyber strategy issues globally without delving into the specifics of individual regions, our study focuses on a specific area, declaring the importance of considering a particular region's regional, cultural, historical and other characteristics. Such specifications can make the selected strategies more effective and adapted to the realities of a specific area.

Efficiency and Economic Aspects of Cyber Activities: Bondar et al. (2020) explored the efficiency of using cryptocurrencies as an investment asset, which indirectly touches upon the issues related to cybercrime, such as money laundering and financial fraud through digital currencies. By incorporating expert feedback and a hierarchical decision-making process, our methodology could be adapted to evaluate and improve strategies aimed explicitly at economic cybercrime aspects, offering a rigorous framework that Bondar et al. suggest is necessary for assessing the risks and returns of cryptocurrencies. The explosion of e-commerce, as discussed by Jasińska-Biliczak (2022), provides a direct link to our focus on cybercrime, as the rise in digital commercial activities invites increased cyber threats. This expansion aligns with our findings that emphasise the need for adaptive strategies that can evolve with changing commercial environments, a concept also supported by Zhang, J., Zhang, C., and Yu (2018) in their study on e-commerce services powered by data mining. Saleh et al. (2020) delve into the legal management of cryptocurrency in national security systems, which complements our research's emphasis on legal and regulatory frameworks for combating cybercrime. Both studies highlight the importance of robust legal structures capable of adapting to the novel challenges posed by digital currencies and cyber transactions, suggesting that the methodologies used in our study could be extended to legal studies for more integrated cybersecurity legislation.

Phillips et al. (2022) provided a comprehensive overview of cybercrime definitions, typologies, and taxonomies that enrich the understanding necessary for developing effective countermeasures. Our study's use of the AHP and Delphi methods could further enhance these typological frameworks by adding structured, expert-driven insights into prioritising response strategies based on these typologies (Table 2).

Table 2. The main innovation in our study

Innovations	Characteristics
Application of the Analytic Hierarchy Process	One of the key innovations of the study is the application of the AHP to the field of cybersecurity in the Middle East. AHP is utilised to dissect the complex problem of cybercrime into manageable components by establishing a multi-level hierarchical structure of objectives, criteria, and sub-criteria. This structured approach allows for a detailed and nuanced analysis, enabling decision-makers to systematically evaluate different strategies and prioritise them based on their effectiveness, feasibility, and impact. By applying AHP, the study addresses the immediate need for effective cybercrime strategies. It provides a replicable model for other regions or contexts, enhancing the strategic planning capabilities within the cybersecurity domain.

Integration of Expert Insights via the Delphi Method	The second innovation involves using the Delphi method to harness the knowledge and consensus of a panel of cybersecurity experts. This methodological choice is particularly innovative in its application to cybercrime strategy development, as it involves iterative rounds of surveys to refine expert opinions and reach a consensus on the most critical aspects of cybercrime and its mitigation. The Delphi method helps filter the collective intelligence of a diverse group of professionals, leading to more informed and robust conclusions. This approach enriches the strategic development process and ensures that the strategies are grounded in current, real-world applications and expert foresight.

In synthesising these perspectives, it is clear that while our research has innovatively applied structured decision-making tools to combat cybercrime in the Middle East, there is broad applicability and potential for integration with global trends and findings. The comparison with the studies above validates our approach's relevance and underscores the potential for further interdisciplinary and cross-regional research to refine and adapt these strategies across different cyber environments.

Conclusions

In summary, we can say that this study has contributed a significant scientific legacy to the understanding and systematisation of measures to combat cybercrime in the Middle East. Using HP and Delphi methods, we created a hierarchical structure of the decision-making process to formulate effective measures to combat cyber threats in the region under study. This combination of methods makes it possible to carry out a comprehensive assessment of various types of strategies to combat cybercrime and highlight a consensus expert decision on this issue, which will guarantee the effectiveness of the chosen strategy.

The findings from this research underscore the dynamic and multifaceted nature of cybercrime in the Middle East, highlighting specific challenges such as rapid technological advancements, regional geopolitical tensions, and varying levels of cybersecurity maturity among nations. Through the strategic application of AHP, we were able to prioritise critical factors and strategies that are most effective in mitigating cyber threats. This prioritisation is based on a rigorous analysis of factors such as effectiveness, cost, implementation feasibility, and potential for regional collaboration. Moreover, the involvement of a diverse panel of experts through the Delphi method has enriched the study, providing a depth of insights grounded in current practice and theory. This engagement has led to a consensus on several critical strategies, such as enhancing legal frameworks, improving technological infrastructures, and developing regional cybersecurity alliances. These strategies are designed not only to combat existing threats but also to anticipate and mitigate future vulnerabilities.

In conclusion, this research advances the field of cybersecurity by providing a strategic framework that other regions might adapt to their own needs, thereby extending the impact of this study beyond the Middle East. The methodology and findings encourage ongoing dialogue and cooperation within the region and internationally, highlighting the importance of a collaborative approach to addressing the global challenge of cybercrime. Future research should expand upon this foundation, exploring the adaptation of these strategies in different cultural and technological contexts and examining their long-term effectiveness in a rapidly evolving digital world.

Recommendations:

- Strengthen and harmonise legislative frameworks to properly manage cybercrime and digital currency issues throughout the region.
- Encourage cooperation and information exchange among Middle Eastern governments to strengthen coordinated responses to cyber threats.
- Use the Analytic Hierarchy Process (AHP) and the Delphi technique to systematically analyse and prioritise cybersecurity initiatives.
- Improve cybersecurity by investing in cutting-edge technologies for detecting, preventing, and responding to cyber attacks.
- Create specialised units and tactics to combat financial fraud and money laundering using cryptocurrency.

References

Alazzam, F. A. F., Tubishat, B. M. A.-R., Storozhuk, O., Poplavska, O., & Zhyvko, Z. (2024). Methodical approach to choosing a business management strategy within the framework of a change in commercial activities. *Business: Theory and Practice*, 25(1), 1–10. https://doi.org/10.3846/btp.2024.19676

Alazzam, F.A.F., Shakhatreh, H.J.M., Gharaibeh, Z.I.Y., Didiuk, I., Sylkin, O. (2023). Developing an information model for E-Commerce platforms: A study on modern socio-economic systems in the context of global digitalisation and legal compliance.*Ingénierie des Systèmes d'Information*, 28(4), 969-974. https://doi.org/10.18280/isi.280417

Applegate, S. (2015). *Cyber conflict: Disruption and exploitation in the digital age. In: Lemieux F. (eds) Current and Emerging Trends in Cyber Operations*. Palgrave Macmillan's Studies in Cybercrime and Cybersecurity. Palgrave Macmillan, London. https://doi.org/10.1057/9781137455550_2

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*, 19(4),1389-1396. https://doi.org/10.18280/ijsdp.190416

Bondar, M. I., Stovpova, A. S., Ostapiuk, N. A., Biriuk, O. H., &Tsiatkovska, O. V. (2020). Efficiency of using cryptocurrencies as an investment asset. *International Journal of Criminology and Sociology*, 9, 2944–2954. https://www.lifescienceglobal.com/pms/index.php/ijcs/article/view/8078

Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., ... & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities and Social Sciences Communications*, 10(1), 1-10.

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*, 12(4), 481-490. https://doi.org/10.18280/ijsse.120409

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

Jasińska-Biliczak, A. (2022). E-commerce from the customer panel: the phenomenon of the pandemic increase and future challenge. Business, *Management and Economics Engineering*, 20(1), 139–151. https://doi.org/10.3846/bmee.2022.16752

Lainjo, B. (2020). Network security and its implications on program management. *International Journal of Safety and Security Engineering*, 10(6), 739-746. https://doi.org/10.18280/ijsse.100603

Morina, M., Azemi, F., Eren, M., Zejneli, I., & Papajorgji, E. (2023). Crime Scene in Cybercrime Criminal Offenses: Evidence Management and Processing.

Academic Journal of Interdisciplinary Studies, 12(2).179. https://doi.org/10.36941/ajis-2023-0041

Pawar, S.C., Mente, R.S., Chendage, B.D. (2021).Cybercrime, cyberspace and effects of cybercrime. International Journal of Scientific Research in Computer Science, *Engineering and Information Technology*, 7(1): 210-214. https://doi.org/10.32628/CSEIT217139

Phillips, K., Davidson, J.C., Farr, R.R., Burkhardt, C., Caneppele, S., Aiken, M.P. (2022).Conceptualising cybercrime: definitions, typologies and taxonomies. *Forensic Sciences*., 2(2): 379-398. https://doi.org/10.3390/forensicsci2020028

Rahmat, R.F., Aziira, A.H., Purnamawati, S., Pane, Y.M., Faza, S., Al-Khowarizmi, Nadi, F. (2023). Classifying Indonesian cyber crime cases under ITE law using a hybrid of mutual information and support vector machine. *International Journal of Safety and Security Engineering*, Vol. 13(5), 835-844. https://doi.org/10.18280/ijsse.130507

Romsaiyud, W., Nakornphanom, K.N., Prasertsilp, P., Nurarak, P., Konglerd, P. (2017). Automated cyberbullying detection using clustering appearance patterns. *2017 9th International Conference on Knowledge and Smart Technology* (KST), pp. 242-247.https://doi.org/10.1109/KST.2017.7886127

Saleh, A.J., Alazzam, F.A.F., Aldrou, K.K.A.R., Zavalna, Z. (2020). Legal aspects of the management of cryptocurrency assets in the national security system. *Journal of Security and Sustainability Issues*, 10(1): 235-247. https://doi.org/10.9770/jssi.2020.10.1(17)

Shi, L.L., Liu, S.H., Petrović, S. (2019). Cryptanalysis of a pseudorandom generator for cross-border *E-commerce.Ingénierie des Systèmes d'Information*, 24(4), 361-365.https://doi.org/10.18280/isi.240401

Yemanov, V., Dzyana, H., Dzyanyi, N., Dolinchenko, O., Didych, O. (2023).Modelling a public administration system for ensuring cybersecurity. *International Journal of Safety and Security Engineering*, 13(1), 81-88. https://doi.org/10.18280/ijsse.130109

Zemlickienė, V. (2018). Adaptation set of factors for assessing the commercial potential of technologies in different technology manufacturing branches. *Business, Management and Economics Engineering*, 16, 206-221. https://doi.org/10.3846/bme.2018.5402

Zhang, J., Zhang, C., Yu, H. (2018). Research on e-commerce intelligent service based on data mining. *In MATEC Web of Conferences*, 173: 03012.https://doi.org/10.1051/matecconf/201817303012

Zhang, Y., Wei, Z.F. (2022). An image classification and retrieval algorithm for product display in e-commerce transactions. *Traitement du Signal*, 39(5), 1865-1871. https://doi.org/10.18280/ts.390547