-

KNOWLEDGE WORDS PUBLICATIONS
INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN PUBLIC POLICY AND GOVERNANCE

INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN PUBLIC POLICY & GOVERNANCE

www.kwpublications.com
ISSN: 2312-4040

Cybercrimes in the United Arab Emirates: Characteristics and Countermeasures

Mohamed S. Alyammahi, Sulaiman Shakib Bin Mohd Noor

To Link this Article: http://dx.doi.org/10.6007/IJARPPG/v9-i1/7441 DOI:10.6007/IJARPPG/v9-i1/7441

Received: 02 *November 2023, **Revised:*** 28 November 2023*, **Accepted:*** 05 December 2023

Published Online: 29 December 2023

In-Text Citation: (Alyammahi & Noor, 2023)

To Cite this Article: Alyammahi, M. S., & Noor, S. S. B. M. (2023). Cybercrimes in the United Arab Emirates: Characteristics and Countermeasures. *International Journal of Academic Research in Public Policy and Governace*, *9*(1), 108–122.

Vol. 9, No. 1, 2023, Pg. 108 - 122

http://kwpublications.com**/index.php/pages/detail/IJARPPG** | **JOURNAL HOMEPAGE**

INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN PUBLIC POLICY & GOVERNANCE

www.kwpublications.com

ISSN: 2312-4040

Cybercrimes in the United Arab Emirates: Characteristics and Countermeasures

Mohamed S. Alyammahi, Sulaiman Shakib Bin Mohd Noor

Faculty of Social Sciences and Humanities, Universiti Teknologi Malaysia (UTM), Malaysia

Corresponding Author's Email: abu_mus1b_82@hotmail.com

Abstract

This study investigated cybercrime in the United Arab Emirates (UAE), focusing on the Emirate of Sharjah, including its characteristics, causes, motivations, and countermeasures. Utilizing quantitative methodology, the research found that the majority of the study sample were male with bachelor's degrees. The motives and causes of cybercrime exhibited minimal variation, suggesting the absence of a dominant criminal trend. However, sexual harassment emerged as the most prevalent content, nature of the young society in the UAE. Twitter was identified as the first-ranked platform for electronic violations, surpassing Facebook due to its popularity across age groups in the country. The data indicate a high level of public awareness regarding cybercrime measures and regulations in the UAE, attributable to the well-educated population and the awareness campaigns conducted by relevant authorities in this regard.

Keywords: Social Media, Cybercrime, Cybersecurity, UAE

Introduction and Problem Background

The information revolution has emerged as one of the defining features of the twenty-first century, providing numerous advantages at all daily life levels. In the second decade of the twenty-first century, life began to increasingly rely on electronic means in various aspects of daily life, exerting a strong and impactful influence in all daily aspects (Al-Khulaiwi, 2017). With the onset of the current decade, the digital revolution has taken another accelerated trajectory, particularly with the emergence of fifth generation (5G) technologies, artificial intelligence (AI), and the Internet of Things (IoT), in a manner that evokes fascination and apprehension (Mahdi et al., 2021; Rao and Prasad, 2018). Social media applications lie at the heart of this rapid development, having witnessed significant stages of evolution, from early social networking technologies such as email in the 1990s to the rise of public social media platforms at the beginning of the new millennium (Tropotei and DEAC, 2019). In the early years of the second decade, instant messaging and visual social communication applications began to emerge and proliferate (Elishar-Malka, 2020), enabling instant sharing of images and videos, high-quality live streaming, and opening up new avenues for creators of visual content. Today, the world stands on the brink of a radical transformation represented by augmented reality and the Internet of Things, allowing for interaction and exchange of information and data among various devices and tools, including household appliances, cars, wearable devices, and more, without direct human intervention. Digital applications are characterized by their interactive and bidirectional nature, in contrast to traditional media that rely on one-way communication, such as television and radio. In other words, social media enables interaction between the sender and the recipient in terms of interaction at the same time (Enke and Borchers, 2021; Goodyear et al., 2019; Kent and Li, 2020). This feature has added a significant new dimension to the patterns of mass media, which typically consist of one-way products sent from a central source, such as newspapers, television channels, or radio stations, to consumers. Furthermore, consumers have the ability to choose the sources of information and entertainment they desire, at their preferred time and in the format they prefer (Enke and Borchers, 2021; Salim, 2023). Moreover, digital applications are characterized by a variety of search and display elements that provide consumers with more options to choose content that aligns with their needs and motivations for communication. This content is presented as a bundled package that can be accessed at the chosen time and location, catering to customers' multiple and evolving needs. Additionally, digital applications offer ease of archiving, easy access to media content, mobility, and the ability to overcome cultural and geographical barriers due to the global nature of the internet that transcends geographic boundaries and the interconnectedness of the internet. The prevalence of video content and the widespread use of instant translation tools have also contributed to the dissemination of these features (Kent and Li, 2020). Despite the aforementioned advantages of new media, such as easy access to media content, reaching audiences beyond cultural and geographical boundaries, and interactivity, there are numerous concerns regarding the reliability and credibility of the vast amount of content being disseminated on the internet. Additionally, there is a security challenge in terms of the difficulty of subjecting it to national or security oversight compared to traditional media (Muamer, 2019).

Literature Review

According to the relevant studies (Almansoori, 2021; Asongu, 2019; Al Mansoori, 2020), the term cybercrime refers to unlawful actions that exploit digital technology as a medium for committing crimes. It encompasses various illegal activities involving the unauthorized use and penetration of digital systems or networks, aiming to gain unauthorized access to confidential information, engaging in electronic fraud, identity theft, cyberbullying, and incitement of hatred and violence. This means that cybercrime manifests in various forms, such as fraud, cyberbullying, privacy violations, dissemination of extremist or sensitive content, and more. Several previous studies have examined the spread of cybercrime based on various factors such as economic conditions, ethnic diversity, and religious factors. Previous research indicates that there is not a significant correlation between income levels and overall rates of cybercrime, but variations and diversity have been observed among cybercrime patterns across different countries (Williams, 2020). Other studies have compared similarities between traditional crimes and internet crimes by analysing crime rates and reporting behaviour (van de Weijer, 2019). The results indicate lower levels of reporting for cybercrimes compared to traditional crimes, with high-severity cybercrimes being more likely to be reported while others are often overlooked. The results indicate lower levels of reporting for cybercrimes compared to traditional crimes, with high-severity cybercrimes being more likely to be reported while others are often overlooked. This could be attributed to the overlapping privacy concerns of cybercrimes with the sensitive privacy aspects of the targeted individuals, leading them to accept the damages without disclosing their privacy to others. Therefore, there are many unrecorded and unreported cybercrimes. Regarding efforts to combat cybercrime and monitor potential criminals' behaviour, some studies have provided insights and recommendations for law enforcement agencies to understand and analyse the behaviour of potential criminals on social media and the degree of extremism reflected in their content (Ristea, 2020). Al Mansoori er al (Al Mansoori, 2020) suggest that by collecting data from content or messages and studying similar cases, law enforcement agencies can predict the occurrence of any cybercrime before it accoure. In this context, the current study aims to explore aspects of cybercrime in the United Arab Emirates, including the measures, laws, and regulations developed to combat this emerging type of crime, as well as enhancing awareness of the importance of digital safety and promoting necessary security measures to mitigate the impact of cybercrimes on individuals and communities.

The Significance and Scope of Study

The significance of this study lies in its examination of a security-pertinent topic, aiming to augment efforts in cybercrime combat. It offers both theoretical and practical insights. Theoretically, it sheds light on the interplay between modern communication technology and its exploitation by criminal groups, aiming to enrich the Emirati academic landscape with data on digital technology's role in terrorist activities and addressing research gaps on modern crime from an Emirati viewpoint. Practically, the research seeks to empower stakeholders to devise robust policies and legislations, fostering safer interactions with modern communication tools, enhancing police efficiency through a comprehensive security database, guiding security policy formulation with a community-partnered strategy, and proposing evidence-based countermeasures against the misleading ideologies propagated by criminal groups, especially from an Emeriti lens.

In the context of the research scope, the present study's purview is systematically bifurcated into spatial and institutional aspects.

The spatial aspect specifically zeroes in on the Emirate of Fujairah within the United Arab Emirates (UAE), attributed to its critical commercial role and strategic positioning as a primary hub for oil distribution. Furthermore, the governmental bodies within Fujairah, earmarked for this investigation, represent an untapped domain in scholarly pursuits. On the institutional front, the research narrows its focus to security entities within the Emirate of Fujairah in the UAE. An ensuing illustration delineates the specific entities wherein members were subjected to the survey.

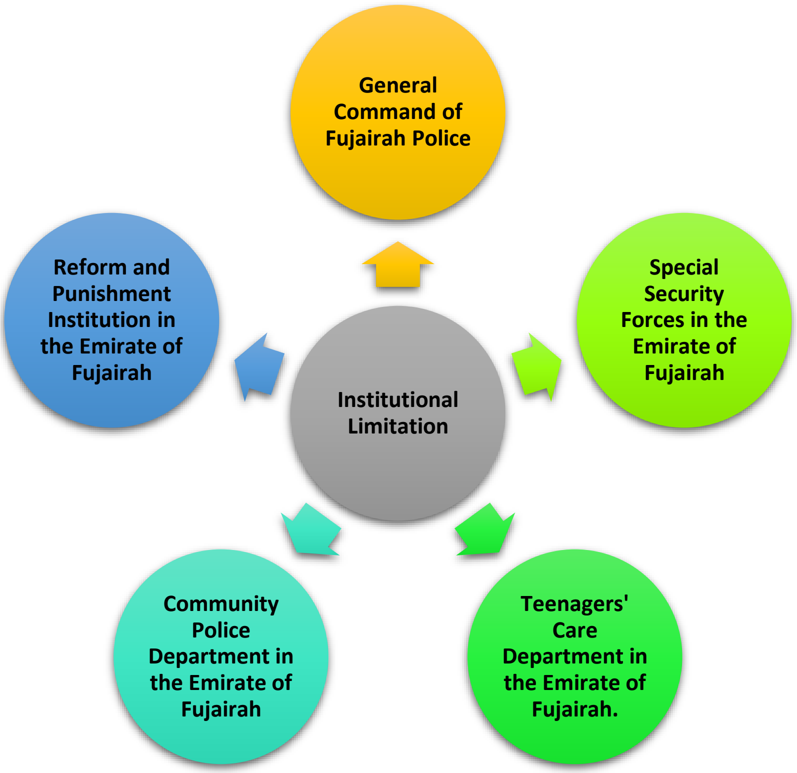
General Command of Fujairah Police
Reform and Punishment Institution in the Emirate of Fujairah
Special Security Forces in the Emirate of Fujairah
Institutional Limitation
Community Police Department in the Emirate of Fujairah
Teenagers' Care Department in the Emirate of Fujairah.

Fig. 1: The institutional limitations of the study

Methodology

The present study utilized a quantitative methodology to gather and analyze data from a selected sample of participants. The causes of utilizing the quantitative approach were the regular distribution of the study sample, and the collection of a maximum number of responses in order to minimize the potential impact of personal biases of the studied sample on the research outcomes. The study population consisted of employees and workers in sectors related to combating modern cybercrimes, specifically from five government institutions in the Emirate of Fujairah, United Arab Emirates. These institutions included the Special Security Forces Command, Fujairah Police General Command, Community Police Department in Fujairah Emirate, Rehabilitation and Punishment Institution in Fujairah Emirate, and the Teenagers Care Department in Fujairah Emirate. The study sample consisted of 126 participants, which falls within the recommended and permissible sample size (>30). Several studies (Fan, Thompson, and Wang 1999; Hill 1998; Tawahir, 2022) have indicated that a sample size of fewer than 30 participants does not adequately represent the characteristics of the target population. Hence, statistically significant differences in means can be obtained from a larger sample size, and the appropriate sample size depends on the specific type of study being conducted. The study community, comprising employees and workers involved in the field of combating cybercrimes, is both limited and homogeneous. It has been argued that increasing the sample size in completely homogeneous communities does not necessarily lead to more reliable results. While increasing the sample size is desirable in less homogeneous communities, it does not significantly impact the study outcomes in almost entirely homogeneous communities, which is applicable to the current study. In relation to determining the sample size for quantitative studies, some studies recommend that if the population exceeds 1000, the sample size should not be less than 5%. For study populations ranging from 500 to 1000, the sample size should range between 10% and 20%

of the population, and for populations fewer than 500, the sample size should be between 25% and 30% (Fan, Thompson, and Wang, 1999; Hill 1998; Tawahir, 2022). By applying these considerations, while taking into account the security protocols and the homogeneity of the targeted study community (which comprises fewer than 1000 individuals), the study sample of 126 which are obtained in the current study, meets the specified criteria for selecting the sample size. Based on that, a questionnaire was developed to collect data from the study sample, and the possible agreement levels for each question were determined using a Likert five-point scale. Each statement in the questionnaire corresponds to a response scale ranging from 1 to 5, representing varying degrees of agreement. A higher score (closer to 5) indicates a higher level of agreement with the statement, while a lower score indicates disagreement. The reason for using this scale is to gain insights into the feelings and opinions of the respondents. The scale can be used to measure agreement, intensity, likelihood, quality, or importance. The following table illustrates the degree of agreement for the questionnaire items using the Likert scale

Table 1
Scale Levels Used in the Questionnaire

Response	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Degree	5	4	3	2	1

To calculate the statistical measure for interpreting the arithmetic means of participants' responses to the questionnaire items, the following gradual scale was used to assess the arithmetic means, according to the following equation:
Category Length = (Highest Value - Lowest Value) / Number of Categories = (5 - 1) / 3 = 1.33

Table 2
Statistical Scale for Interpreting the Arithmetic Means of Study Participants' Responses to the Questionnaire Items

Low Evaluation Level	Moderate Evaluation Level	High Evaluation Level
1 - 2.33	2.34 - 3.67	3.68 - 5

The questionnaire consists of three sections where, the first section consists of demographic data of the respondents (gender, job position, years of experience). The second section consists of four parts, each part containing five statements except for the third part, which includes seven statements (with a total of 22 statements). It focuses on the characteristics of electronic crimes themselves. Similarly, the third section consists of two parts, each part containing five statements, with a total of 10 statements. It relates to the countermeasures. Table 3 illustrates the procedure for interpreting the results. It is observed from Table 3 that the length of the scale used is (5/4), approximately 0.80. The length of the scale was calculated based on the assumption that the numbers five in the scale (1, 2, 3, 4, 5) are divided into four intervals. As for the percentage, it was calculated by dividing the mean by the scale (Mean/5 × 100).

Table 3
The procedure for interpreting the results

Arithmetic Mean	Percentage (%)	Approval Rating Interpretation	
		Verbal Assessment	Evaluation Level
Lower than 1.8	Lower than 36%	Strongly Disagree	Very low
Between 1.8–2.6	Between 36%–52%	Disagree	low
Between 2.6–3.4	Between 52%–68%	Neutral	moderate
Between 3.4–4.2	Between 68%–84%	Agree	high
Between 4.2–5	Between 84%–100%	Strongly Agree	Very high

Results and Discussion

Sample Characteristics

The characteristics of the study sample were evaluated based on four dimensions: gender, age, academic qualification, and years of experience. The selection of these four dimensions to describe the study sample can be justified as they provide a suitable impression of the awareness, expertise, physiological aspects resulting from experience, and gender differences within the research sample. As shown in Figure 1, the male participants constituted the majority of the sample, accounting for 90%. In contrast, the female participants represented 8%, which aligns with the nature of work in this type of profession and the conservative Emirati society. Additionally, Figure 1 illustrates that the age group ranging from 30 to 40 years accounted for the highest percentage (32.6%), followed by the age group less than 30 years, with a percentage of 30.9%. The age group from 40 to 50 years accounted for 22.2% of the sample, while the age group over 50 years represented the lowest percentage at 14.3%. This can be attributed to the youthful nature of the UAE society and the early retirement age in the United Arab Emirates (60 years). Similarly, Figure 1 shows that individuals with a bachelor's degree constituted the highest percentage of the sample (53.2%), followed by those with a diploma and master's degree, with percentages of 20.6% and 16.7%, respectively. Individuals with a doctoral degree represented 9.5% of the sample. Regarding the distribution of the study sample based on years of experience, participants with more than 20 years of experience ranked first with a percentage of 36%. Those with 15 to less than 20 years of experience ranked second with a percentage of 30%, followed by those with 10 to less than 15 years of experience at 26%, and finally, those with less than 10 years of experience at 8%. This indicates that the majority of the sample has considerable experience, which will provide more objectivity to their responses regarding the study dimensions.

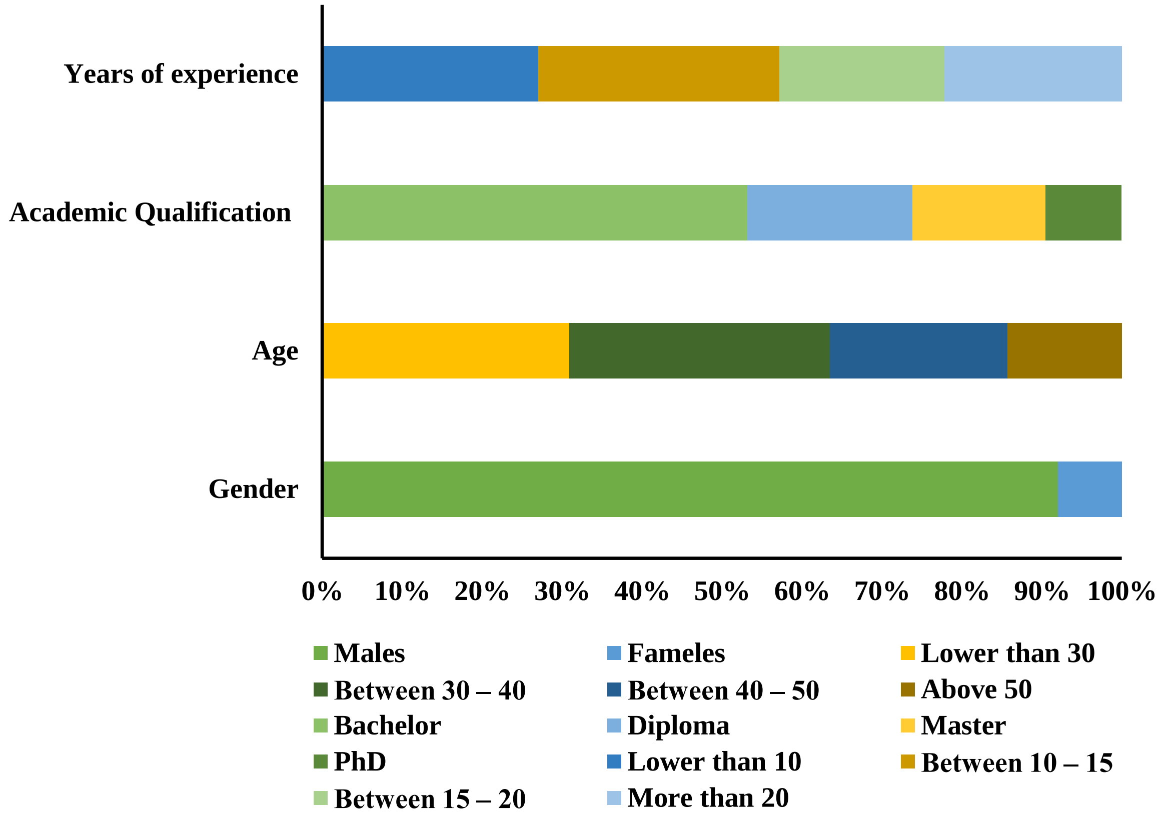

Fig 2: Study sample characteristics

Characteristics of Cybercrime and the Targeted Group

Motives and Reasons

Table 4 illustrates the overall mean scores of the questionnaire statements related to the motive and reason part, which was around 3.436, with a standard deviation of 1.48, indicating a higher mean than the hypothetical mean (3). The highest mean score for the statement in this part was 3.461, associated with spying and extortion. This can be attributed to the fact that most reported cases involve threats and extortion in order to pre-emptively avoid any physical harm to the targeted individuals. On the other hand, the lowest mean score was 3.405, with a percentage of 68% and a standard deviation of 1.471, related to the fame and publicity statement. This is primarily due to various factors, including the lack of popularity of the idea, as it is often confined to a single individual, making it a weak motive, unlike those based on religious motivation or financial gain that justifies the risk. Moreover, its impact on others is relatively low, reducing the level of response and reporting. Finally, the results indicate a consensus among the study sample regarding their agreement on the studied motives and reasons for committing cybercrimes, with mean scores ranging from 3.461 to 3.405, which are higher than the hypothetical mean (3) of the five-point scale categories, indicating the agreement of the study sample with the validity of the mentioned reasons. The high response rate can be attributed to the validity of the study sample. The results also suggest that there was minimal variation in the mean scores related to the motives and reasons for committing cybercrimes in the Emirate of Sharjah, indicating the absence of a prevalent criminal phenomenon, and instead pointing to a natural state indicating the stability of society in the United Arab Emirates.

Table 4
The mean scores, standard deviations, and level of response for the motive and reason dimension

Motive or Reason	Mean	Std	Percentage (%)	Evaluation Level
Fame and the desire for publicity	3.4056	1.471	68	moderate
Financial fraud	3.4333	1.409	69	High
Spreading rumours and violating privacy	3.4278	1.609	69	High
Promoting extremist intellectual content	3.4556	1.434	69	High
Espionage and blackmail	3.4611	1.479	69	High
Overall mean score	3.436	1.48	69	High

Content

Table 5 demonstrates that the overall mean score for the questionnaire items related to the independent variable (content) reached 3.405 with an agreement rate of 68% and a standard deviation of 1.531. Based on the aforementioned results, it is evident that the content related to security and political violations is the least observed content by relevant authorities, indicating the political and security stability in the country. On the other hand, content related to sexual harassment ranked first, which can be attributed to the nature of the young society in the United Arab Emirates. Moreover, there is a slight variation in the agreement among the sample participants regarding the type of promoted content, ranging from neutrality to agreement. The statement related to content and sexual harassment had the highest mean score of 3.4722 with a agreement rate of 69%, possibly due to many young people seeking sexual excitement on social media platforms while concealing their identities. Conversely, the statement related to security violations had the lowest mean score of 3.211 with an agreement rate of 64% and a standard deviation of 1.124, reflecting the prevailing security and political stability in the country.

Table 5
The mean scores, standard deviations, and level of agreement for the content dimension.

Motive or Reason	Mean	Std	Percentage (%)	Evaluation Level
The content related to sexual harassment	3.4722	1.413	69	High
The content related to extremist religious ideologies and sectarian incitement	3.2111	1.124	64	moderate
The content aimed at financial fraud	3.4556	1.411	69	High
The content related to political violations	3.1167	1.440	62	moderate
The defamation of beliefs and religions as a right of expression	3.3122	1.413	66	High
The overall mean score for this part	3.405	1.531	68	High

Platform

Table 6 displays the scores for the questionnaire statements related to the part of the platform or the most attractive electronic means for perpetrators of cybercrimes. It is evident that the overall mean score for this part reached 3.647 with an agreement rate of 69% and a standard deviation of 1.471, and an agreement percentage of 73%. The highest mean score in this part was attributed to the platform Twitter, with a mean score of 3.911 and an agreement rate of 78%. This high rate can be attributed to the large user base of Twitter in the United Arab Emirates and the Arab Gulf countries in general. Additionally, the high privacy policy provided by Twitter and Snapchat has made them the most attractive platforms for content sharing in the UAE. On the other hand, the high rate of TikTok usage can be attributed to its popularity among younger age groups, which creates a suitable environment for sexual harassment specifically. In contrast, the platform Facebook had the lowest mean score in this dimension (3.1307) with a rating of average and a standard deviation of 1.632. This could possibly be due to the lack of popularity of this platform in the Arab Gulf region, as well as the fact that its audience tends to be older age groups with less activity on social media platforms.

Table 6

Mean scores, standard deviations, and response level for the platform part.

Motive or Reason	Mean	Std	Percentage (%)	Evaluation Level
YouTube	3.4611	1.390	69	High
Twitter	3.9111	1.378	78	High
WhatsApp	3.4667	1.736	69	High
Tick Tok	3.6611	1.488	73	High
Snap Chat	3.7389	1.367	75	High
Facebook	3.1307	1.632	63	moderate
Others	3.7236	1.347	74	High
The overall mean score for this part	3.64778	1.4718	73	High

Targeted Population Awareness

Table 7 indicates that the overall mean scores for the questionnaire items related to the dependent variable of awareness among the targeted population of the necessary measures to be followed reached 3.693 with an agreement rate of 74% and a standard deviation of 1.4372. The results also demonstrate a consensus among the study sample regarding their agreement on the existence of sufficient awareness about the necessary measures to be followed and satisfactory cooperation from the reporting individuals with relevant security authorities. The highest mean score for statements in this part was for the item related to the clarity of the person to the target in revealing the details of the violation they have experienced, with a mean score of 3.733 and an agreement rate of 75%. This can be attributed to the willingness of the targeted party to facilitate the work of the relevant control agencies. On the other hand, the lowest mean score in this part was related to the statement of the nature of the targeted party (individual or institution) (3.3722), with a rate of 67% and a standard deviation of 1.408. This could be attributed to the ease of targeting ordinary individuals compared to institutions that have more protective systems compared to individuals. Furthermore, reported cybercrimes by institutions mainly focus on financial crimes and data theft, unlike the wide range of crimes targeted at individuals, such as harassment, threats, and extortion.

Table 7
Mean scores, standard deviations, and response level for the part of awareness among the targeted population of the necessary procedures to be followed.

Motive or Reason	Mean	Std	Percentage (%)	Evaluation Level
I have previously received a complaint about a crime or fraud through electronic means.	3.67	1.42	73	High
The targeted party was fully aware of the necessary procedures to be followed when subjected to an electronic crime or fraud.	3.37	1.41	67	High
The targeted party was cooperative and transparent in revealing the details of the violation they experienced.	3.70	1.41	74	High
The targeted individual was willing to disclose their privacy to the relevant authorities upon request during the reporting process.	3.73	1.49	75	High
Criminals often leave digital evidence that enables the police to identify their identities and track their online activities.	3.64	1.46	73	High
The overall mean score for this part	3.69	1.44	74	High

Efforts to reduce cybercrime

Ensure the information safety of individuals and institutions

Table 8 illustrates that the average level of information security for individuals and organizations, as perceived by the participants of the study, is high, with a mean of 3.456 and a standard deviation of 1.10, representing a percentage of 69%. The item indicating the existence of effective response mechanisms and plans for reporting cybersecurity incidents and digital threats in the United Arab Emirates ranked first with a high mean score of 3.74, a standard deviation of 1.27, and a percentage of 75%. This can be attributed to the readiness of individuals, the availability of resources, and legislative regulations for dealing with cybercrimes and violations. In contrast, the item which states that individuals and organizations in the United Arab Emirates have sufficient awareness of the importance of information, digital, and cyber safety, ranked last with an average score of 3.04, a standard deviation of 1.34, and a percentage of 61%. This can be attributed to the significant cultural diversity that hinders the effectiveness of targeted awareness programs. Additionally, the table demonstrates that all the mean scores for the items, as well as the overall score for information security for organizations, exceeded the hypothetical average of 3, with a calculated t-value indicating significance at the 0.01 level.

Table 8
Mean scores, standard deviations, and rankings for items on information security for individuals and organizations

Motive or Reason	Mean	Std	Percentage (%)	Evaluation Level
Effective response mechanisms and plans are in place for cybersecurity incidents and digital threats in the United Arab Emirates.	3.74	1.27	75	High
Relevant authorities in the United Arab Emirates provide individuals and organizations with plans and guidelines to protect their sensitive data and information.	3.54	1.25	71	High
Periodic monitoring and surveillance operations are conducted to ensure the safety and security of digital systems and networks in the United Arab Emirates.	3.52	1.27	70	High
Individuals and organizations in the United Arab Emirates have access to consultancy services and network and system security assessments to identify vulnerabilities and enhance security.	3.44	1.23	69	High
Individuals and organizations in the United Arab Emirates have sufficient awareness of the importance of information, digital, and cyber safety.	3.04	1.34	61	moderate
The overall mean score for this part	3.456	1.10	69	High

Relevant Regulations

Table 9 shows that the mean for the part of the availability of regulations organize use of social media platforms, from the perspective of the study sample, was high with a mean of 3.444, a standard deviation of 1.22, and a percentage of 69%. The item stating the availability of guidelines and principles for individuals and companies to comply with security and safety requirements in using social media networks ranked first with a high degree and an average of 3.58, a standard deviation of 1.29, and a percentage of 72%. On the other hand, the item indicating the public announcement and accessibility of updates and new amendments to the regulations on combating cybercrime and regulating the use of social media networks ranked last, with a medium degree and an average of 3.24, a standard deviation of 1.39, and a percentage of 65%. It can be observed that there is very little variation in the average scores and standard deviations in this dimension, which can be attributed to the coherence, clarity, and wide dissemination of policies related to regulatory regulations.

Table 9

Means, standard deviations, and rankings for items related to the availability of regulations organize using social media platforms

Motive or Reason	Mean	Std	Percentage (%)	Evaluation Level
Guidelines and regulations are available for individuals and companies to comply with security and safety requirements in using social media networks.	3.58	1.29	72	High
The latest update to the regulations on combating cybercrime and the use of social media networks includes new applications of technology or new concepts in this field.	3.56	1.31	71	High
The regulations related to the regulation of social media network usage and combating cybercrime are periodically reviewed and updated in the United Arab Emirates.	3.50	1.34	70	High
Mechanisms are provided to the public and organizations to stay informed about the latest updates and amendments to the regulations concerning the fight against cybercrime and the use of social media networks.	3.34	1.35	67	moderate
Announcements of new updates and amendments to the regulations on combating cybercrime and regulating the use of social media networks are made publicly and are available to the public.	3.24	1.39	65	moderate
The overall mean score for this part	3.444	1.22	69	High

Conclusion

This study investigated the characteristics of cybercrime in the United Arab Emirates, specifically in the Emirate of Sharjah, as well as its causes, motivations, and the efforts made by relevant authorities to combat it. The study relied on quantitative methodology to summarize the results, given that the study sample is known, defined, homogeneous, and distributed in a homogeneous manner. The results related to the characteristics of the studied sample indicated that the majority of the sample consisted of males with a bachelor's degree, which is an expected outcome in this type of profession. Additionally, the results showed very little variation in the means related to the motives and causes of committing cybercrimes in the Emirate of Sharjah, indicating the absence of a prevailing criminal phenomenon and instead suggesting a natural state of societal stability in the United Arab Emirates. The content related to security and political violations had the least observed content by relevant authorities, indicating the political and security stability experienced in the country. On the other hand, content related to sexual harassment ranked first, which can be attributed to the nature of the young society in the United Arab Emirates. Twitter emerged as the preferred platform for electronic violations, while Facebook ranked lower, reflecting the high popularity of Twitter among different age groups in the Gulf Arab countries, while Facebook is perceived as a refuge for older age groups who are less active, and dynamic compared to younger age groups. Additionally, there is a prevailing belief in the privacy policy of Twitter compared to other platforms. Statistical data also indicates a high level of public awareness in the United Arab Emirates regarding measures and regulations, which is expected due to the high level of education among the population and the awareness campaigns conducted by relevant authorities in this regard. The statistical results indicated the availability of regulations, systems, and necessary personnel for analyzing and monitoring digital data related to combating cybercrime by relevant authorities, which are accompanied by various restrictions and controls during investigation, monitoring, and surveillance. This can be attributed to the modernity, preparedness, and contemporaneity observed in the security sectors in the United Arab Emirates.

References

Al-Khulaiwi, & Saleh, R. B. A. (2017). Rumors on social media and their relationship to intellectual security among university students.

Almansoori, A., Alshamsi, M., Abdallah, S., and Salloum, S. A. (2021). “Analysis of Cybercrime on Social Media Platforms and Its Challenges.” In Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2021), Springer, 615–25.

Simplice, A., Nwachukwu, J., Orim, S., and Pyke, C. (2019). “Crime and Social Media.” Information Technology & People.

Elishar-Malka, V., Ariel, Y., and Weimann, G. (2020). “Rethinking Political Communication in the Digital Sphere.” The Journal of International Communication 26(2): 190–210.

Enke, N., and Borchers, N. S. (2021). “Social Media Influencers in Strategic Communication: A Conceptual Framework for Strategic Social Media Influencer Communication.” In Social Media Influencers in Strategic Communication, Routledge, 7–23.

Fan, X., Thompson, B., and Wang, L. (1999). “Effects of Sample Size, Estimation Methods, and Model Specification on Structural Equation Modeling Fit Indexes.” Structural equation modeling: a multidisciplinary journal 6(1): 56–83.

Goodyear, V. A., Parker, M., and Casey, A. (2019). “Social Media and Teacher Professional Learning Communities.” Physical Education and Sport Pedagogy 24(5): 421–33.

Hill, R. (1998). “What Sample Size Is ‘Enough’ in Internet Survey Research.” Interpersonal Computing and Technology: An electronic journal for the 21st century 6(3–4): 1–12.

Kent, M. L., and Chaoyuan, L. (2020). “Toward a Normative Social Media Theory for Public Relations.” Public Relations Review 46(1): 101857.

Muamer, T. (2019). New media and issues of identity and citizenship in the context of globalization challenges. Journal of Media Research and Studies, 10(10), 10-58.

Rao, S. K., and Prasad, R. (2018). “Impact of 5G Technologies on Industry 4.0.” Wireless personal communications 100: 145–59.

Salim, A., Abdulqader, N. (2023). Obstacles facing elementary school teachers when teaching computer science during the Corona pandemic in the Badia Al-Shamaliyah Al-Sharqiyah district of Mafraq Governorate in light of some selected variables. Journal of Education (Assiut) 39(1.2), 68-107.

Tawahir, A. A. J., Bilal, & Othman. (2022). Scientific research methods and selection techniques. Visions in Humanities and Social Sciences, 1(4), 22-32.

Tropotei, Teodor, and Ioan DEAC. (2019). “SOCIAL MEDIA IN INTELLIGENCE ANALYSIS.” Strategic Impact.

Van de Weijer, Steve, G. A., Leukfeldt, R., and Bernasco, W. (2019). “Determinants of Reporting Cybercrime: A Comparison between Identity Theft, Consumer Fraud, and Hacking.” European Journal of Criminology 16(4): 486–508.