Kurdish Studies
Sep 2023
Volume: 11, No: 3, pp. 394-402
ISSN: 2051-4883 (Print) | ISSN 2051-4891 (Online)
www.KurdishStudies.net

Received: May 2023 Accepted: June 2023
DOI: https://doi.org/10.58262/ks.v11i3.029

Social Engines of Cybercrime in Society. Sociology of Digital Crime

Enaam Youssef Mohammed[1], Al Rawashdeh, A. Z[2]*, Al Arab, A. R[3], Nasefi, Saeed. A[4]

Abstract

Objective: This study, assessed various social reasons concerning the spread of cybercrime in Ajman in the United Arab Emirates from the police officers' perspective part of the Department of Technical Crimes in Ajman. Substantial amount of resources are devoted to help overcome the criminal activities in a region. However, the prevalence of cybercrime continues to be a significant hindering block in the development. Methods: A descriptive design was used where the qualitative approach was employed. The data were collected from 10 police officers at the Department of Technical Crimes in the Emirate of Ajman. Interviews were conducted for gathering data, which were thematically analyzed. Results: The responses revealed a high prevalence of the cybercrime case. The primary causes of cybercrime were family, education, friends, and environment. The prime motive for cybercrime was wealth, followed by cyber terrorism. Also, cybersecurity concerns were high for women. Conclusion: The study suggests an offering of various awareness programs concerning the actions which can help reduce its occurrence. It also emphasizes the formation of a framework for guiding the user activities on the internet, ensuring his protection.

Keywords: *Cybercrime In Society, Emirate of Ajman, Social Engines, Wealth Accumulation Sociology of Digital Crime.*

Introduction

Digital transformation has integrated technology into every aspect of an individual's life, which helps improve efficiency in various endeavors. Even though technology has provided countless benefits, it continues to raise severe concerns related to the security, protection, and safe use of internet. Generally, the concerns related to use of technology are observed due to its misuse by the individuals (classified as criminal) who exploit their knowledge to harm others for reasons such as access to money, and extortion, generally observed in terms of moral and physical exploitation (Mali et al., 2018). This heinous exploitation is known as "cybercrime," which suggests an elevated degree of risks to society. Majorly, the issue of cybercrime has substantially increased across different political leaders, corporates, entrepreneurs, criminal justice administrators, as well as the general public (Chukwuemeka & Egbegi, 2019).

The importance of this issue is evident from the aggressive investment of enterprises for cybersecurity (Kashyap & Wetherilt, 2019). Statistics show that global spending is likely to reach $124 billion in 2019, for protection against cybercrimes. Likewise, Hiscox (2018) report estimates that 12 percent of an

[1]Department of Sociology, College of Humanities and Science, Ajman University, P.O.Box: 346 Ajman, UAE, Humanities and Social Sciences Research Center (HSSRC), Ajman University, P.O.Box: 346 Ajman, UAE.
[2]Department of Sociology, College of Humanities and Science, Ajman University, P.O.Box: 346 Ajman, UAE, Humanities and Social Sciences Research Center (HSSRC), Ajman University, P.O.Box: 346 Ajman, UAE, Department of Social Sciences, Ajloun University College , Al Balqa Applied University, P.O.Box:206 Salt, Jordan.
[3]Department of Sociology, College of Humanities and Science, Ajman University, P.O.Box: 346 Ajman, UAE, Humanities and Social Sciences Research Center (HSSRC), Ajman University, P.O.Box: 346 Ajman, UAE, Department of Social Sciences, Ajloun University College , Al Balqa Applied University, P.O.Box:206 Salt, Jordan.
[4]Department of Sociology, College of Humanities and Science, Ajman University, P.O.Box: 346 Ajman, UAE, Humanities and Social Sciences Research Center (HSSRC), Ajman University, P.O.Box: 346 Ajman, UAE.

organization's IT budget is likely to spend on cybersecurity. Ibekwe (2015) defines that global cybercrime accounts for a loss of $240 million. The issue of cybercrime is prevalence across different nations, with its noted spread in the United Arab Emirates (UAE). The increased integration of technology for social and cultural communication further makes the individual, institutions, and employees vulnerable to cybercrime attacks (Conteh, & Schmick, 2016). At present, cybercrime has significantly outperformed ordinary crimes in terms of damage caused to them. Therefore, there exists a need to address the causes of cybercrimes and their impact on society and youth. Not only this, but analysis of the impact on economic and political aspects of the state, and the relationship of sociology and social service is also integral.

UAE has initiated various efforts to combat crimes, mainly cybercrimes. It directs all its efforts to preserve human rights consistent with international agreements and conventions. However, despite these efforts, various crimes occur using modern technologies and communications technology for extortion. Recently, Grant Thorne (2019) reported that UAE is forecasted to lose about $6 trillion until 2021 due to cybercrime. Further, studies have shown that cybercrime is a challenging task for policing, where they struggle to align their efforts with digital threats.

Digital evidence from the literature suggests that crimes, in general, are facilitated due to access to technology. Accordingly, the increase in cybercrime occurs due to the shifting of social problems from the real world to the virtual. Umanailo et al. (2019) further state that the borderless nature of cybercrime makes cybercrime difficult to detect. Canter & Youngs (2016) highlights that social processes substantially affect the crime prevalence as well as its investigation, which have not been investigated previously. The scarcity of research concerning the social stimulators for cybercrime requires considerable action for highlighting the challenges posed. Thus, the study aims to identify the nature of the social reasons behind the spread of cybercrime in the UAE society from the perspective of police officers working in the section of technical crimes.

Study Objectives

The prime objective is to identify the social causes concerning the spread of cybercrime (cyber blackmail) in the United Arab Emirates from the police officers' perspective part of the Department of Technical Crimes in Ajman. It also includes the sub-objectives as followed;

1. To examine the concept of cybercrime.
2. To identify cybercrimes that occurred using various technical means.
3. To determine the causes and characteristics of cybercrime and related defamation of persons or damage to their data (electronic extortion) and how to prevent them.
4. To highlight the UAE government's efforts to combat cybercrime and identify strategies and mechanisms to deal with it.

Study Questions

The primary and sub research questions of the study include:

'What are the social causes of cybercrime in the United Arab Emirates from Ajmans' police perspective?'

While the sub-questions are as follows;

1. What are cybercrimes?
2. What are the cybercrimes that are performed using different technical means?
3. What are the reasons for the commission of these crimes and the circumstances that motivate the persons to commit them? Is it possible to justify the commission of such acts, or is it a crime whose perpetrators must be punished without regard to any of the motives for their commission?

4. What efforts have the state's taken to limit, eliminate, and punish cybercrime?

Literature Review

Evidence from literature highlights that cybercrimes affect individuals at every level and social status. Ajah (2018) shows that individuals such as young, old, rich-poor, female, and male are vicarious victims of cybercrimes (Okpa & Ukwayi, 2017; Ukwayi & Okpa, 2017). Bakhsh, Mahmood, & Awan (2016) concluded that it is necessary to introduce a legal, regulatory mechanism that punishes the one involved in the crime of destroying information and data. In case of committing information crimes, and punishing attempting such crimes. Foldes (2017) states that penal codes can help reduce all forms of cybercrime and help reduce the magnitude of the losses as an outcome of cybercrime.

Younes (2016) suggests that continuous and periodic review of the legislator should occur to deal with cybercrime. The legislative policy designed to deal with cybercrime can be amended in case of ineffectiveness or the emergence of any variables or developments. Ratten (2019) presented the requirements of raising the efficiency and effectiveness of methods to confront cybercrime in terms of advanced technologies and qualified human competencies and preparation of operational programs. It helps to reduce cybercrime by monitoring threats and risks and provide early warnings.

In addition to the legislation and the criminal justice system, a highly qualified and efficient police workforce is necessary, along with the emphasize for international regional cooperation to address cybercrime. Alshammari & Singh (2018) also emphasized the development of a unified strategy for the region. Saragih & Siahaan's (2016) study examined the crime of electronic extortion and the efforts that can be introduced for combating it. The study showed that the rapid development in the information network has contributed and facilitated the growth of cybercrimes. Riek, Bohme, & Moore (2015) showed that the increased risk of cybercrime reduces the online activities of the users. Similarly, The study (Alqahtani, N.N., et al. ,2023) recommended the necessity of developing a comprehensive national strategy aimed at limiting the ability of terrorist groups and organizations to employ digital media in general and social media in particular to attract and recruit Saudi citizens , Ilievski & Bernik (2016) and (Alqahtani, N.N., et al. ,2023) study found that the social-economic status of the country also increases the cybercrime in a region. It showed a strong association of GDP, unemployment, and education with cybercrime. The comparative analysis Saudi Arabia and UAE of Bakhsh, Mahmood, & Awan (2016) showed that although the efforts for mitigating cybercrime are high in the region, the lack of awareness makes its implementation challenging.

The analysis of the literature highlights cybercrime issues for UAE that has been explored by a few researches, particularly in the social context. The current study is significant as it monitors the cybercrime developments and the techniques employed for reducing and preventing cybercrime along with insights on the UAE legislator. It is because technical measures alone fail to suffice the need for investigating different cybercrime issues and taking relevant measures to overcome it.

Methodology

Study Design

A descriptive study design is used, which helps in the analytical analysis of the study phenomena. The rationale for the selection of this design is based on its relevance to aid in meeting the determined objectives. This also constitutes the application of case form, where the group of experts and specialists is consulted for achieving a different set of goals.

Study Population and Sample

The study population constitutes police officers representing the Department of Technical Crimes in the Emirate of Ajman. Officers were selected based on their direct exposure and relatedness for combating cybercrimes in the region. Using a purposive sampling design, ten individual policemen were included. The purposive sampling was based on the determined inclusion criteria, which required participants to belong to the Department of Technical Crimes in the Emirate of Ajman. This sampling technique was used due to its objective analysis of the data.

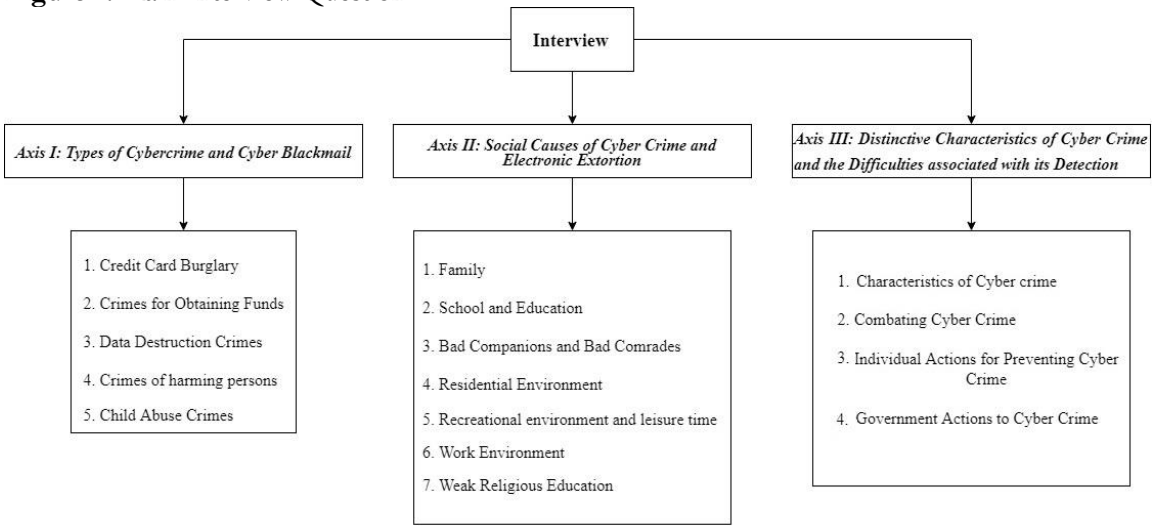
Data Collection

The data were collected through interviews, and the questions were based on three-axis, i.e.,

- Axis I: Types of cybercrime and cyber blackmail.
- Axis II: Social Causes of Cybercrime and Electronic Extortion.
- Axis III: Distinctive characteristics of cybercrime and the difficulties associated with its detection.

Every interview was based on these questions, which further division is presented in figure 1.

Figure 1: Main Interview Question.



Ethical Consideration

Prior to the study, ethical approval was achieved from the Institutional Review Board (IRB). The procedure and protocols of the study were initially communicated to the participants for gathering relevant and adequate responses. The data confidentiality and anonymity were communicated to ensure participants can easily understand and respond to the questions.

Study Procedure

A letter for conducting the study, along with its aims and objectives, was shared with the Department of Technical Crimes in the Emirate of Ajman. After participants' recruitment, the researcher communicated the study protocols. The place for the interview was determined as per the feasibility of the interview participants. The interview duration ranged from 50 to 60 minutes, where a particular number (P1 to P10), was assigned to every individual.

Data Analysis

The collected data were analyzed using a thematic analysis. The responses were categorized based on the collected data. Initially, the demographics and social characteristics of the sample were analyzed, followed by an explanation of cybercrimes and the reasons for committing them. Various technical means were used in addition to a special axis to identify some cybercrimes as well as their spread in the UAE, especially in the Emirate of Ajman. The participants were asked to clarify the characteristics associated with cybercrime and the role and efforts of the UAE in preventing cybercrime.

Results

First: Demographic Details of Participants

Understanding the social and demographic characteristics of the study sample and the extent of their differences in these characteristics is important for reflecting the difference among participants concerning the studied issues. Table 1 shows that among 10 members of Ajman Police, 6 were males, while 4 were females. Concerning the age, two individuals were aged between 32 to 36 years, while others were aged between 29 to 33 years. Two individuals had basic education, 4 had a university degree, and 4 hold a certificate. For marital status, married participants were 7 and 3 participants were single.

Table 1: Demographic Details.

Variables		Frequency
Gender		
	Male	6
	Female	4
	Age	
	29 to 33 years	8
	32 to 36 years	2
	37 to 41 years	-
	42 to 46 years	-
	47 to 51 years	-
	Education	
	Basic Education	2
	University	4
	Certification	4
	Marital Status	
	Single	3
	Married	7

For analyzing the participants understanding concerning cybercrime, the following questions were asked;

Second: What are cybercrimes?

In your view, what does cybercrime mean?

The respondents (P7, P8, P9) answered that cybercrime means an online behavior that is criminalized by law. Cybercrime refers to unlawful behaviors committed through the computer and its networks. This answer was similar to the procedural definition regarding cybercrime. The respondents (P1, P2, P3, P4, P5, P6, and P10) agreed to define them as "conduct or action that leads to the infringement of a human right" (physical or moral harm) and "through the use of electronic devices and social networking programs". This is consistent with the cybercrime definition of Shackelford (2017).

Are Material Motives the Most Important Reason for Committing This Type of Crime?

The participants (P1, P2, P3, P5, P6, P7, P9, P10) agreed on the materialistic nature as the main reason for committing cybercrime, where they explained that main objective for cybercrime is financial gain, which is consistent of what has been confirmed by several studies (Arief, Adzmi, & Gross, 2015). Unlike (P4, P8), who answered no, they stated that cybercrime is committed by individuals who are motivated by revenge for accessing and destroying certain data or hobby or spending free time without consciousness or guidance. Sabillon et al. (2016) also illustrates similar results and states that the patterns of cybercrime, according to which the reasons and motives for crimes or destruction of information vary which may require to delete or change data for some purpose concerning individuals or companies.

From Your Professional Experience, Does Anyone Who Receives Information from Other People Through Illegal Electronic Means Feel Privileged?

All participants agreed on a single answer, i.e., yes, stating that an individual's personal view and practices can substantially impact the cybercrime practices. As individuals with access to private information of a person can easily threaten people and access their secrets, which is consistent with what has been indicated by (Albadayneh, Diab, 2014), which explains that the reason behind the act of cybercrime indicating dissatisfaction with the people, as primary.

Third: Identify Some Cybercrimes that Are Carried Out by Different Technical Means

to What Extent Are Cybercrimes Prevalent in UAE Society?

The respondents (P2, P3, P4, P6, P7, P8, and P10) provided the same response concerning the spread of cybercrime stating that programs at networking sites lead to increase cybercrimes, which is consistent with findings of earlier researches (i.e., Choi & Lee, 2018) because of the rapid development of technology and lack of awareness among people concerning malware attacks. The participants (P1, P5, P9) stated that with the presence of a specialized department these attacks can be combated significantly, which is consistent with the findings of Willits & Nowacki, 2016. These specialized units, with the efforts of the Government of the United Arab Emirates, can help deal with cybercrime issues.

What Are the Most Serious Cybercrimes in The UAE Society, in Your Opinion?

The participants generally stated that the extortion of members, especially women, and defamation for material gains, followed by cyber terrorism, are the major causes of cybercrime, along with political crimes. This answer supports previous findings on electronic blackmail (Nurse, 2018), which showed different factors that increase the occurrence of the cybercrime.

Fourth: Causes And Characteristics of Cybercrime and Those Related to Defamation of Persons or Damage to Their Data (Electronic Extortion), And How to Prevent Them

What Are the Social Causes of Cybercrime from Your Experience and From Your Point of View?

The cases unanimously answered: unemployment, unhealthy or bad company, family disintegration, lack of awareness, weak religious motivation, and poor material level and inadequate thinking for committing cybercrime. This is supported by the earlier findings in the literature (Levi, 2017). It was found that family plays an important and effective role in the socialization that may be individuals and can be the result of the thinking that is inappropriate for social life, although it is the basis of standards. The Code of Ethics was also emphasized (Abdullah, Nader, 2011), who referred to education as one of the important tasks and duties in the thinking of individuals. The failure to education leads to the introduction of illegal forms committed by individuals, such as cybercrime, since school is one of the pillars of proper upbringing and if not attended can be a reason supporting the commission of crimes. Whitty & Ng (2017) also support the present findings as the understanding of the social groups can

affect the ratio of cybercrimes in a region.

In Your View, What Are the Most Important Characteristics of Cybercrime, Especially Those Related to Cyber Blackmail?

The respondents answered that they have virtual access to crimes and cybercrime. This enables its commitment remotely anywhere in the world and the difficulty of locating the criminal. Concerning blackmailing, the familiarity of the operations along with ways to access data is necessary.

What Are the General Ways of Preventing Cybercrime? Particularly the Prevention of Electronic Extortion?

The participants suggested to spread an electronic protection culture in the community and care when using electronic programs, especially that require access to images and passwords. This is consistent with the earlier research of Brown, (2015). It explains the role of protection by individuals on personal data and images and not to give personal data access to any stranger or unreliable source. It also suggests the use of protection programs to prevent the occurrence of various cybercrimes.

Fifth: To Clarify the Efforts of The UAE Government to Face Cybercrime, And Identify Strategies and Mechanisms to Deal with Them

Is There Monitoring on Social Networks and on the Internet in A Manner Commensurate with The Increasing Number of Cybercrime and Cyber Blackmail in the UAE? If Yes, What Are the Mechanisms?

The samples provided one answer, i.e., yes. It is because there is a unit for assessing the technical crimes in the Department of Cybercrime, which addresses and follows-up social networks and initiate efforts for ensuring cybersecurity. It identifies the individuals involved in cybercrime while they are committing the crime, which is consistent with what is pointed out in an earlier research (Brown, 2015). The role of security services in this field is to protect the privacy of the members of the society from spying, loss of information or attempts to steal via electronic devices carried out by a group of individuals who are indifferent to the laws set by the UAE government and the penalties for this criminal act.

Are The Police in the UAE Interested in Solving Cybercrime Problems from Your Point of View? If yes, how?

The answer of respondents is same such as these crimes can be reduced through several initiatives and programs, including the service (Secretary) and the basis of strict confidentiality. The existence of a specialized department working to reduce these crimes is created for UAE society, which is consistent with what has been indicated by Caneppele & Aebi (2017). This illustrates the efforts made by the police in the section of technical crimes that work to reduce crimes and help victims, which cause psychological impact on victimized individuals.

Conclusion

Findings revealed a strong relationship between the prevalence of cybercrime in society and the lack of regulatory framework and its commitment to overcome the cybercrime cases in the region. The responses showed that social control mechanisms in the community can help combat the prevalence of social crime. It indicated various reasons which lead to the prevalence of cybercrime among which impact of family, education, friends, and environment were significant.

Further, it is observed that for controlling cybercrime, a technical unit exists which constitutes a police officer whose primary job is to reduce the cybercrimes in the UAE. Accordingly, the current findings

showed that the motives for cybercrime vary along with the factor that promotes the cybercrime, where family and social values are the main agents. The study also supplies that the Department of Technical Crimes has established various initiatives as well as programs that assist in the reduction of cybercrimes and help strengthen confidentiality.

Inadequate understanding of the religion and its prohibition also promotes to indulge in cybercrime. The lack of a competent online network for controlling might account for easy access to data as well as its exploitation. The responses of the interviews further indicated that the increased statistics for the cybercrime might be due to inadequate family control. It also showed that sharing personal data to a stranger or an unreliable individual can contribute to cybercrime. Accordingly, it also showed that lack of awareness and knowledge of the community members provides easy access to hackers leading to compromise of the data. This study also revealed that the most common type is cyber blackmailing in the region. Overall, the study showed the widespread prevalence of cybercrime in Ajman.

It is suggested that educational intervention and awareness programs concerning cybercrime should be introduced. Furthermore, instigation of the educational interventions for the public, as well as educational ventures for the police is also recommended. A pleasant company should be maintained, where inclusion with the negative or bad company should be reduced. It is also suggested to avoid enmity with people, while eradicating actions or communication with strangers.

Acknowledgement

The author is very thankful to all the associated personnel in any reference that contributed in/for the purpose of this research. Further, this research holds no conflict of interest and is not funded through any source.

References

Alshammari, T. S., & Singh, H. P. (2018). Preparedness of Saudi Arabia to Defend Against Cyber Crimes: An Assessment with Reference to Anti-Cyber Crime Law and GCI Index. *Archives of Business Research*, *6*(12).

Arief, B., Adzmi, M. A. B., & Gross, T. (2015). Understanding cybercrime from its stakeholders' perspectives: Part 1--attackers. *IEEE Security & Privacy*, *13*(1), 71-76.

Bakhsh, M., Mahmood, A., & Awan, I. I. (2016). A comparative analysis of cybercrime and cyberlaws in Islamic Republic of Pakistan, Kingdom of Saudi Arabia, and the United Arab Emirates. *Imam Journal of Applied Sciences*, *1*(1), 9.

Brown, C. S. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology*, *9*(1), 55.

Caneppele, S., & Aebi, M. F. (2017). Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. *Policing: A Journal of Policy and Practice*, *13*(1), 66-79.

Canter, D., & Youngs, D. (2016). Crime and society. *Contemporary Social Science, 11*(4), 283-288. DOI: 10.1080/21582041.2016.1259495

Choi, K. S., & Lee, C. S. (2018). The Present and Future of Cybercrime, Cyberterrorism, and Cybersecurity. *International Journal of Cybersecurity Intelligence & Cybercrime*, *1*(1), 1-4.

Chukwuemeka, O. D., & Egbegi, F. R. (2019). An exploratory study of cybercrime in the contemporary Nigeria value system. *European Journal of Social Sciences Studies*.

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities, and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6*(23), 31.

Foldes, S. (2017). Comments on the notion of information system in the Budapest Convention on Cybercrime, the EU directive, and selected penal codes.

Grant Thorne. (2019). Cyber-crime: avoid paying the price. Available at: https://www.grantthornton.ae/globalassets/1.-member-firms/uae/may-2017-onwards/cybercrime_avoid-paying-the-price_2017.pdf

Hiscox. 2018. Cyber Readiness Report. Available at: https://www.hiscox.co.uk/cyberreadiness

Ibekwe, C. R. (2015). The Legal Aspects of Cybercrime in Nigeria: An Analysis with the UK Provisions.

Ilievski, A., & Bernik, I. (2016). Social-economic aspects of cybercrime. *Peer-reviewed academic journal Innovative Issues and Approaches in Social Sciences*.

Kashyap, A. K., & Wetherilt, A. (2019). Some Principles for Regulating Cyber Risk. In *AEA Papers and Proceedings* (Vol. 109, pp. 482-87).

Levi, M., 2017. Assessing the trends, scale and nature of economic cybercrimes: overview and issues. *Crime, Law and Social Change*, *67*(1), pp.3-20.

Mali, P., Sodhi, J. S., Singh, T., & Bansal, S. (2018). Analysing the Awareness of Cyber Crime and Designing a Relevant Framework with Respect to Cyber Warfare: An Empirical Study. *International Journal of Mechanical Engineering and Technology*, *9*(2).

Nurse, J. R. (2018). Cybercrime and you: how criminals attack and the human factors that they seek to exploit. *arXiv preprint arXiv:1811.06624*.

Alqahtani, N.N., Al Rawashdeh, A.Z., Al-Arab, A.R., Aldoy.(2023). M.I.,Methods of Protection Against the Attraction and Recruitment of Terrorist Groups Through Social Media . Information Sciences Letters, 2023, 12(5), pp. 2139–2148. , **DOI:** 10.18576/isl/120549

Okpa, J. T., & Ukwayi, J. K. (2017). Drug suspects perception of factors responsible for illicit drug trade in Cross River state, Nigeria. *IOSR journal of humanities and social science (IOSR-JHSS)*, *5*(4), 80-87.

Ratten, V. (2019). The effect of cybercrime on open innovation policies in technology firms. *Information Technology & People*.

Riek, M., Bohme, R., & Moore, T. (2015). Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), 261-273.

Sabillon, R., Cano, J., Cavaller Reyes, V., & Serra Ruiz, J. (2016). Cybercrime and cybercriminals: a comprehensive study. *International Journal of Computer Networks and Communications Security, 2016, 4 (6)*.

Saragih, Y. M., & Siahaan, A. P. U. (2016). Cyber Crime Prevention Strategy in Indonesia. *SSRG Int. J. Humanit. Soc. Sci*, *3*(6), 22-26.

Shackelford, S. (2017). Exploring the 'Shared Responsibility' of Cyber Peace: Should Cybersecurity Be a Human Right?

Ukwayi, J. K., & Okpa, J. T. (2017). The effect of electoral and economic crimes on sustainable development in Cross River State, Nigeria. *International Journal of Social Science Research*, *5*(2), 32-42.

Umanailo, M. C. B., Fachruddin, I., Mayasari, D., Kurniawan, R., Agustin, D. N., Ganefwati, R., ... & Sutomo, S. (2019). Cybercrime Case as Impact Development of Communication Technology That Troubling Society. *Int. J. Sci. Technol. Res*, *8*(9), 1224-1228.

Whitty, M. T., & Ng, M. (2017). Literature Review for UNDERWARE: UNDERstanding West African culture to pRevent cybercrimEs. Report for the National Cyber Security Centre as part of a group of studies funded in the Research Institute in Science of Cyber Security.

Willits, D., & Nowacki, J. (2016). The use of specialized cybercrime policing units: An organizational analysis. *Criminal justice studies*, *29*(2), 105-124.

Younes, M. A. B. (2016). Effects of cybercrime and ways to deal with it. *The International Journal of Engineering and Sciences*, *5*(2), 23-27.