Pakistan Journal of Criminology
Vol. 16, No. 02, April—June 2024 (263-276)

Psychological Insights into the Behavior of Cybercriminals: A Theoretical Perspective

Raed S. A. Faqir[1] & Dorsaf Arfaoui[2]

Abstract

This study explores comprehensively the complex psychosocial factors driving individuals toward illicit activities in the digital realm. The study encompasses the concept of cybercrime and psychological theories such as social learning, psychoanalytic, and cognitive behavioral theories. The application of space transition theory to cybercriminal behavior, determinants influencing cybercrime perpetration, and mechanisms for addressing cybercrimes. Employing a descriptive and legal analytical methodological approach, it combines didactic exposition and meticulous analysis to deeply explore the psychological motivations behind cybercriminal actions, including experiential trajectories, volitional tendencies, and cognitive processes. The findings reveal a nuanced array of motives underlying cybercriminal behavior, including the absence of a robust cyber-vigilance culture, financial incentives, and the attraction of unauthorized knowledge acquisition. Socio-economic elements like unemployment and intricate family dynamics exacerbate the propensity for cyber-delinquency.

Keywords: Cybercrime, psychological drivers, cybersecurity culture, mixed-methods approach, motivations, prevention Measures.

Introduction

Comprehending the incentives and mental models that drive cybercriminal conduct is a challenging undertaking with significant ramifications for psychology research (Sarkar and Shukla, 2023). The advent of the digital age has given rise to a new type of criminal behavior, which calls for a thorough investigation of the psychological elements that motivate people to engage in cybercrime (Stalans and Donner, 2018). The goal of this investigation is to disentangle the complex interactions between psychological factors that influence the intentional choices, dispositional inclinations, and behavioral expressions of cybercriminals (Vinciguerra, 2023). Through an exploration of the psychological underpinnings

[1] The author is an Associate Professor in Criminal Law, the College of Law, American University in the Emirates, United Arab Emirates. He is also an Associate Professor in Criminal Law, Faculty of Law, Al-Balqa Applied University in Jordan. He can be reached at raed.faqir@aue.ae and r.faqir@bau.edu.jo, His ORCID ID: https://orcid.org/0000-0002-6102-0983

[2] The author is Assistant Professor in Criminal Sports Law, the Director of the Master's Program in Sports Law, specializing in Criminal Sports Law, the College of Law, American University in the Emirates, United Arab Emirates. She can be reached at dorsaf.arfaoui@aue.ae, Her ORCID ID:

of cybercriminal behavior, this analysis aims to reveal the underlying forces, mental models, and affective processes that shape the dynamic terrain of cybercrime (Azouz, 2022).

Within the field of psychological characterization, investigations are important for comprehending criminal behavior as well as more general human behavior (Bonta and Andrews, 2016). Notably, Freud—the pioneering psychoanalyst—made significant contributions to psychological research, especially when it came to understanding the psychological underpinnings of criminal behavior (Hollin, 2013). Psychological research provides an explanation for many transgressions, demonstrating how psychological disorders such as anxiety and distress are major factors in motivating people to commit crimes (Klass, 1978).

According to the research of Bucy, et al., (2008), psychological characteristics can make people more likely to commit crimes, but they don't always result in criminal tendencies. Rather, they increase vulnerability to criminal behavior impacted by environmental circumstances. Psychological tendencies are prone to the effect of other elements in the intricate interaction that leads to the change of an individual into a perpetrator.

The digital environment influences criminal activity, leading to financial losses and state-sponsored cyberattacks. Research gaps in the understanding of cybercrime impede the development of cryptocurrency and artificial intelligence. Sturdy cybersecurity solutions are essential. Scholarly research is essential to comprehending the dynamics of cybercrime, preventive measures, and creative solutions. Legislative frameworks are shaped by academic institutions, but cooperation between academia, law enforcement, and business is necessary for a full framework.

This study aims to bridge the gap in understanding the psychological drivers driving cybercriminal behavior, focusing on psychological motivations rather than technical aspects. This contributes to effective prevention and intervention strategies. It investigates cybercrime and technology's role in criminal activities, incorporating the Space Transition Theory. It examines psychological factors like thrill-seeking, anonymity, cognitive biases, socio-economic conditions, and technological accessibility, emphasizing diverse psychological intervention approaches.

Methodology of the Study

The study used a descriptive approach to analyze the psychological interpretation of cybercrime, focusing on modern theories and factors. It also applies an analytical approach to identify psychological factors driving individuals to commit crimes in virtual space. This study deduces the most important principles derived from various psychological perspectives and applies them to cybercriminal behavior to reveal the psychological factors behind cybercriminality.

Literature Review

Several scholarly investigations have centered on the domain of cybercrimes, exhibiting diverse methodologies, theoretical viewpoints, and applied strategies. A critical examination of selected studies has sought to extract insights for constructing theoretical and methodological frameworks in this domain. Noteworthy among these investigations are the following:

El-Eissawi's study examining psychological theories in the context of crime elucidated that these theories predominantly hinge upon environmental influences when delineating criminal behavior. The psychoanalytic school, for instance, accentuates unconscious elements in crime genesis, notably emphasizing the role of the death instinct, destructiveness, sabotage, murder, and annihilation (El-Eissawi, 2005). Contrarily, learning theories underscore the impact of familial and peer group dynamics, with certain theories spotlighting cognitive processes and decision-making mechanisms. The multifaceted nature of criminal activities and the array of personalities involved render it challenging to unequivocally adopt one psychological theory over others to comprehensively expound diverse criminal behaviors (El-Eissawi, 2005). Nevertheless, each theory contributes to a nuanced comprehension of the intricate criminal phenomenon to a discernible extent.

The study of Al-Rashidi on "Interpreting Criminal Behavior with Situational Theories and Islamic Method," it is explores how criminal behavior imperils human security (2017). Al-Rashidi advocates an integrated approach, particularly within Islamic scholarship, to comprehensively address the causes of criminal behavior (Al-Rashidi, 2017). It assumes a span from individual traits to societal influences, aiming to clarify, assess legally, interpret via Islamic methods, outline implications, and evaluate their effectiveness in preventing and addressing crime (Al-Rashidi, 2017). Al-Musamoudi's study illuminates emerging paradigms in crime prevention and the reinvigoration of conventional methodologies in the digital era, underscoring the imperative for contemporary, proactive, and technology-driven preventive measures to address the escalating and evolving

nature of crime, advocating for a synthesis of societal, situational, and community-centered strategies (Al-Musamoudi, 2022). This study evaluates current crime prevention trends, emphasizing the significance of societal progress, community engagement, and the implementation of localized strategies at regional and city levels while recommending the prioritization of social and psychological frameworks, the establishment of an Arab crime observatory, and leveraging forensic sciences for predictive and preventive purposes (Al-Musamoudi, 2022).
The escalation in instances of digital crime victims due to shifts in individuals' daily routines, propelled by the advent of the internet, has resulted in profound disruptions across various facets of human activity, including communication patterns, interpersonal interactions, leisure pursuits, and commercial endeavors (Ajibade, 2020). Particularly noteworthy is the pervasive utilization of the Internet, social networking platforms, email services, online entertainment portals, and applications. They have not only generated opportunities but have also rendered easily accessible targets for perpetrators operating within the digital realm. A significant contributing factor to this surge in digital crime is the collective deficiency in adequate and vigilant oversight mechanisms (Hamlawi & Charatiya, 2019).

The Concept of Cybercrime

Cybercrime denotes illicit activities executed through digital and electronic mediums, often utilizing computers, networks, and the Internet (Harris, 2012). It encompasses a diverse array of unlawful actions, including hacking, identity theft, online fraud, cyberbullying, the dissemination of malware, phishing, and a spectrum of cyberattacks (Faqir and Alrousan, 2023). Exploiting weaknesses in digital systems and technology, cybercrime aims to secure unauthorized entry, pilfer confidential data, disrupt services, and inflict financial, personal, or societal detriments (Tala, 2020). With technology's ongoing evolution, cybercrime's tactics and manifestations continually morph, rendering it a multifaceted and dynamically shifting realm of criminal conduct (Attiya, 2015).

Cybercrimes involve digital execution using computers, networks, and the internet, while traditional crimes involve physical interactions and tangible assets. Anonymity and identity management play distinct roles in cybercrimes, while traditional crimes require physical evidence analysis (Baltoush, 2008). Cybercrimes can affect multiple individuals or organizations simultaneously, requiring advanced hacking skills. Both types can have immediate and delayed effects, but the consequences are more detrimental for victims due to widespread data breaches and identity theft (Azouz, 2022).

Cybercrime's digital domain and psychological dynamics set it apart from traditional crime. It attracts those who are apprehensive about conventional criminal identification and promotes anonymous participation in illicit operations (Attiya, 2015). Cybercriminals are highly skilled technicians who promote empowerment and mastery (Boudhir, 2017). The digital sphere reduces empathy and remorse by psychologically separating people from the repercussions (Ben Abdallah, 2022).

Psychological Theories on Cybercrime Phenomenon

Theory of Social Learning

The social learning theory, developed by Burgess and Akers in 1966, suggests that people learn new behaviors by watching social effects (Boudhir, 2017). Positive results from observed behaviors increase the desire to imitate and adopt them. However, the extent of this hypothesis's application to criminal skills remains unknown. Further research is needed to determine its potential application in combating cybercrime (Bayan, 2020).

The theory emphasizes the impact of social dynamics and peer associations on the feeling toward cyber-criminal activities, thereby advancing the elucidation of the cognitive course involved in the acquisition of cybercriminal skills and behaviors (Zohri, 1984). It contributes significantly to the comprehension of cyber-criminal behavior through examination of the impact stemming from the observation and limitation of actions undertaken by others (Essawi, 2017). The theoretical framework expounds on the way exposure to criminal activities informs individuals' perceptions regarding potential advantages and risks (Hamlawi, 2019). Furthermore, social learning theory systematically investigates the role played by online communities in the propagation of knowledge and methodologies pertinent to cybercriminal pursuits (Al-Musamoudi, 2022).

Psychoanalytic Theory

Psychoanalytic theory, formulated by Sigmund Freud, explores the complex interplay between unconscious desires and conflicts, influencing human behavioral patterns (El-Eissawi, 2005). It emphasizes the role of the unconscious mind and introduces conceptual constructs like the id, ego, and superego, explaining human behaviors' origins from concealed constituents and internal discrepancies (Soleimani, 2020). Psychoanalytic theory examines latent motivations and conflicts in cybercrime, examining concealed yearning, power dynamics, and suppressed affective states that influence cybercriminal behavior (Al-Musamoudi, 2022).

Cybercrime can be seen as a way for people to show their inner problems, take control of situations, or feel good about themselves (Herson and Alan, 2007). A big part of this idea is that online, it's easy to stay hidden, so people can do things without others noticing, even if they don't realize why they are doing them (Zohri, 1984).

Cognitive Behavioural Theory

Cognitive behavioral theory, created by psychiatrist Aaron T. Beck in the 1960s and 1970s, says that changing unhelpful thought patterns can improve how we act (Al-Rashidi, 2017). It illustrates that people make undesirable observations about themselves and have automated bad judgment, which amounts to conduct and sensitivity that is not supportive (Tawba, 2020). To renovate this thinking, reorganization requires exchanging those harmful thoughts with extra meaningful ones and employing practices to advance attitudes and decrease dreadful conduct (Tala, 2020).

This approach is valuable for identifying why individuals commit e-crimes. It focuses on just how they ponder and their rational bases (Moustafa et al., 2021). As per this approach, uncommon thinking, the capability to disappear in virtual space, and the undertaking of returns all impulse individuals to make cyber-offenses (Kalodner, 2011). In the current approach, activities such as modifying bad thinking and regaining constructive techniques to perform can help hinder cybercrime (Moustafa et al., 2021). Moreover, dealing with twisted ideas and what directs individuals, the theory of cognitive behavior intends to push moral virtual conduct and deter unlawful behaviors in virtual space (Al-Rashidi, 2017).

This theory looks at how both inside and outside factors affect cybercrime behavior (Ajibade, 2020). External triggers like things happening, family, and how people feel can play a part, while internal factors like feeling bad about oneself or not being in control can push someone toward cybercrime (James, 2011). The theory talks about how distorted thinking, being anonymous, and getting rewards can lead to cybercrime (Samir, 2022). Plus, things like systems that can be taken advantage of, new technology, online communities, and laws can all make cybercrime easier (Ruimel, 2012).

The Space Transition Theory

The Space Transition Theory, created in 2008, says that people who usually do not do bad things might turn to cybercrime because of their place in society and how they feel about themselves (Jaishankar, 2007). Tricks on social media and other websites can lead them to commit crimes, depending on where

the crime comes from (Ajibade, 2020). Being anonymous online, which happens when people can hide who they are or feel disconnected from themselves, often leads to doing the wrong things. This theory focuses on when and where crimes happen, paying attention to what is going on around them and how people move, to understand why they do bad things online (Schmalleger and Pittaro, 2009).

The theory says that cyberspace and real-world crime influence each other, especially organised crime or groups using the Internet for scams, hiding money, and stealing. When people feel like they do not fit in with or what society expects, it can lead to conflicts and cybercrimes (Jaishankar, 2007). This theory suggests that where people are and how they act in those places can make them more likely to commit cybercrimes (Al-Rashidi, 2017). It highlights how being able to change who you are online, feeling disconnected, and the lack of things to stop you online can lead to crimes centred around information. More research is needed to understand this theory better and how it explains cyber-criminal behavior (Ajibade, 2020).

Determinants Influencing the Perpetration of Cybercrimes

Information crimes involve many different things, like motivations, opportunities, psychological factors, society, technology, how connected the world is, online groups, laws, and conflicting thoughts (Tala, 2020). To tackle cybercrimes and stop them from happening, we need a complete plan that includes prevention and ways to step in before they happen (Faqir, 2023).

Avengers are people who do digital things without permission to get back at someone they think did them wrong. They are driven by personnel grudges, unfairness, power, and feeling satisfied emotionally (Al-Eissawi, 2005). They target specific people, groups, or organizations using cyberattacks. These actions break laws and can have serious consequences. Cybercrime happens because of both real-world and online factors. Real-world factors include where you are, the laws there, and the technology available. Online, cybercriminals exploit weak platforms (Harris, 2012). Technology, social connections, money, culture, law enforcement issues, rules, and education all play a part in cybercrime (Baltoush, 2008). Understanding these factors can help people avoid becoming victims and be careful when dealing with potential crimes (Alrousan and Faqir, 2024).

The internet has opened up new ways for criminals to make money, stay hidden, and target people all over the world. Understanding these changes is important for making plans to keep information safe and deal with cybercrimes as they change (Hamlawi & Charatiya, 2019). More people using the internet, social media, and apps means more potential targets for cybercriminals. As cyber threats keep changing, individuals and groups are at risk of being attacked online

(Soleimani, 2020). To stay safe, it is crucial to be aware of cybersecurity and take steps to protect yourself. Cybercrime is often about making money, with criminals taking advantage of online banking, payment systems, and digital money (Al-Rashidi, 2017). The "triad paradigm" shows how technology, knowledge, and motivation work together for organized crime online (Weissberg, 2022).

Cybercrime is about making money by doing illegal things online, such as hacking, stealing information, blackmail, and fraud. People do it for different reasons, like not being careful online, wanting to get rich quickly, being offered money, having personal grudges, or wanting to hurt others. Copying what others are doing, city living, not having much self-control, and how easy it is to communicate online all make cybercrimes more common (Jaishankar, 2007). Things like not having a job, being poor, and not knowing much about keeping information safe also contribute to cybercrime. Some people are drawn to learning new things and getting into places they are not allowed to, which leads to cybercrime. Laws and rules must address these reasons to make people more aware of cybersecurity and stop cybercrime. We need specific plans to protect the online world (Tala, 2020).

The Impact of Psychological Factors on Cybercriminal Behaviours

Psychological studies are important for understanding why people do bad things, but they also help us understand how people behave in general. They try to figure out why people act the way they do by looking at different parts of their minds, like things they might not even realize they are thinking (Ajibade, 2020). This includes stuff inside them that affects how they deal with the world around them, like things that happened to them or how they were raised (Soleimani, 2020). Different psychologists have specific ideas, but most agree that Sigmund Freud's ideas, which focus on mental problems and how the mind works, are helpful (Bayan, 2020).

Psychological factors can have a big impact on why people engage in cybercriminal activities. These factors can be explained as follows:

- **Motivation**: Psychological factors like the desire for money, power, or revenge can drive individuals to commit cybercrimes. For example, someone might hack into a bank's system to steal money because they are motivated by financial gain (Riley et al., 2017).
- **Risk-Taking Behaviour**: Some individuals may have a higher tolerance for risk, which can lead them to engage in cybercriminal activities without considering the potential consequences. They might feel invincible or believe they won't get caught (Rosenquist, 2015).

- **Cognitive Biases**: A Psychological basis, such as overconfidence or the illusion of control, can lead individuals to underestimate the risk of cybercriminal behavior or overestimate their ability to avoid detection (Moustafa et al., 2021).
- **Personality Traits**: Certain personality traits, such as impulsivity, sensation seeking, or a lack of empathy, may make individuals more susceptible to engaging in cybercrimes. For example, someone who is highly impulsive may act on their impulses without considering the consequences (Shappie and Debb, 2019).
- **Psychological Stressor**: External stressors, such as financial difficulties, relationship problems, or job dissatisfaction, can contribute to psychological distress and increase the likelihood of individuals turning to cybercrime to cope with or alleviate their stress (Soleimani, 2020).
- **Social Influence**: Peer pressure, social norms, and the desire for acceptance or validation within online communities can influence individuals to participate in cybercriminal activities, especially if they perceive such behavior as socially acceptable or justified within their peer group (Hamlawi, 2029).

Finally, it can be said that understanding the psychological factors underlying cybercriminal behaviors is essential for developing effective prevention and intervention strategies to address cybercrime effectively.

Mechanisms for addressing Cybercrimes.

There is a need to take action to stop deceptive emails, also called phishing or scam emails, from tricking people (Kalodner, 2017). These emails use people's trust to get them to share private information. To fight this, we should use two main strategies (Baltoush, 2008). First, we need stronger security measures, like filters for emails and using authentication protocols for emails. Second, we need to teach people how to recognize phishing emails and what to do if they get one. This way, we can better protect ourselves and our communities from these scams (Attiya, 2015).

The cultivation of a collective sense of responsibility within communities, coupled with the encouragement of individuals to report suspicious emails to relevant authorities and share insights regarding novel phishing techniques, can establish a synergistic defense against cybercriminal activities (Azouz, 2022). The amalgamation of fortified technological barriers, community-based awareness campaigns, and individual empowerment constitutes a potent strategy for

significantly diminishing the effectiveness of cybercriminal endeavors to illicitly obtain funds through deceptive electronic communications (Harris, 2012).

Educational programs aim to teach young people about the legal and ethical results of their online actions, like hacking or sharing private information without permission (Ben Abdallah, 2022). These initiatives help them understand laws, cybersecurity, and how to act responsibly online. By learning these skills, they can make smart choices and keep their reputation safe (Hersen, 2007).

The shortage of a deep protection mind among clients of monetary foundations shows why learning and consciousness are so essential (Ajibade, 2020). Numerous considerations interpose to this problem, including not being completely thoughtful about cyber dangers, expecting safety procedures too much, not having enough education about cybersecurity, language and cultural barriers, and more cybercrime happening. It is crucial to address these issues urgently (Moustafa et al., 2021).

To grasp these challenges, there is a need to converge on movements that raise awareness and teach the public about cybersecurity. This involves training customers, being sympathetic to several cultures, and working together with financial institutions. By upgrading a culture of safety awareness, people can make better choices, guard their funds, and help create a protected digital sphere (Bayan, 2020).

The growth of information offenses is a fast-growing danger online, putting groups, organizations, and societies in danger (James, 2011). To fight this threat essentially, we need powerful laws and protocols (Kalodner, 2017). These rules should clearly define different types of crimes, keep up with changes in technology, have appropriate punishments for each crime, encourage cooperation between countries, help law enforcement do their job better, protect victims' rights and privacy (Krkosh and Kothar, 2017), raise awareness about the issue, promote proactive approaches, encourage cooperation between the public and private sectors, and make sure the legal process is fair for everyone involved (Faqir, 2024). These legal frameworks are crucial for clearly defining and organizing various cybercrimes, adjusting to new threats, and making sure legal processes follow the right procedures while protecting the rights of both the accused and the harmed parties (Ruimel, 2012). By creating laws that fit the unique aspects of cybercrime, societies can better stop, prosecute, and discourage cybercriminal behavior (Samir, 2022).

Conclusion

The study explores theories explaining cybercrime behavior, focusing on social learning theory and a psychoanalytical approach. It suggests that the cyber-offense may be a means for individuals to engage in insider conflicts or persuade secret aspirations, as the secrecy and distance of virtual communications allow for the hidden motives.

Cognitive behaviors study how ideas impact conduct, highlighting how wrapped thoughts and secrecy can lead to cyber-offenses. Perspective reorganization and psychoanalytical models help understand cyber-illegal actions, enabling effective tackling and deterrence. Therefore, cyber-illegal conduct is influenced by psychosomatic, high-tech, community, fiscal, and legal factors, resulting in info-based offenses, which are influenced by enticements, digital sites, inner motives, social stimuli, and legal guidelines.

This study emphasizes the importance of a comprehensive approach to tackling information-based crimes, focusing on psychosomatic incentives like monitoring gain, good principles, and secrecy. It highlights the significant influence of cyber offense on both online and real-world environments, emphasizing the need for awareness of cyber-safety and defensive measures. Psychosomatic motives and cybercrimes are crucial, necessitating a comprehensive proactive approach that includes public education, safety procedures, and tailored legal structures to tackle cyber offenses, punishments, and the protection of victims.

Finally, the study concludes with a set of recommendations, as follows:

- Develop comprehensive educational programs targeting students, professionals, and general people to raise awareness about cyber-offense, emphasizing understanding psychometric motives and technology's role in cyber-crimes.
- Promote moral principles and values in online behaviour by encouraging the public to adopt responsible digital practices and respect discretion rights.
- Advocates for robust legal frameworks to effectively tackle cyber-crimes, including psychosomatic factors, and ensure appropriate penalties for cyber-criminals.
- Encourage the initiative collaboration among agencies, law enforcement, private sector organizations, and international partners to combat cyber offenses.

- Offer comprehensive support services to cyber offense victims, including counselling, legal assistance, and financial restitution, to aid recovery and prevent future recurrence.

References

Ajibade. A. A. (2020). Applying Space Transition Theory to Cyber Crime: A Theoretical Analysis of Revenge Pornography in the 21st Century. *International Journal of Innovative Science and Research Technology*. Vol. 5 (11), 631-637.

Ali, S. A., and Faqir, R. S. A. (2024). Criminal Protection of Digital Applications in the UAE Legislation: A Comparative Study. *Pakistan Journal of Criminology*, Vol.16 (1), 490-503.

Al-Musamoudi, S. A. (2022). Modern Trends in Crime Prevention: How Classic Approaches Renew in the Digital Age? *Arab Journal of Forensic Sciences and Forensic Medicine*, Vol. 4(2), 67-193.

Al-Rashidi, T. E.A. (2017). Interpreting Criminal Behavior in Light of Situational Theories and the Islamic Method, *Journal of the College of Islamic and Arabic Studies for Girls in Damietta*, Vol.2(9), 313-396.

Alrousan, E., and Faqir, R. S. A. (2024). Unraveling the Intricacies of Implementing Judicial Pardon within UAE Legislation, *Academic Journal of Interdisciplinary Studies*, Vol. 13 (1), Pp. 385-401.

Attiya, T. I. D. (2015). Criminal Investigation Procedures for Controlling Cybercrime in Light of The Budapest Agreement Signed on November 23, 2001, Related to Global Crime. *Journal of Security and Law*, Vol. 23 (2). 339-349.

Azouz, R. O. (2022). Cybercrime and its Response Requirements, Journal of the Faculty of Education.Vol.10, 224-247.

Baltoush, K. (2008). Crime within the Electronic Environment as a Result of Technological Development or the Beginning of a New Crime. *Academic Review of Social and Human Studies.* Vol. 1. 48 - 55.

Bayan L. (2020). Concepts and Theories in Crime. *Journal of Legal Facts*. Vol. 1 (5), 141- .179.

Ben Abdallah, N. K. (2022). Cybercrime: Sociological Reading of the most Important Explanatory Theories of Criminal Behavior. *Rawafed Journal of Studies and Scientific Research in Social and Human Sciences*. Vol.6 (2). 661-682.

Bonta, J., & Andrews, D. A. (2016). The psychology of criminal conduct. Routledge.

Boudhir, Z. S. R., and Bashiri A. (2017). Sociological Approach to Crime Study. Online Version. http://search.mandumah.com/Record/857667. (Accessed on 11 December 2023).

Bucy, P. H., Formby, E. P., Raspanti, M. S., & Rooney, K. E. (2008). Why do they do it: the motives, mores, and character of white-collar criminals. *John's L. Rev.*, 82, 401.

El-Issawi, A. M. (2005). Psychological Theories in Crime Interpretation. *Journal of Police Thought*. Vol. 13 (8), 271-298.

Faqir, R. S. A. (2023). Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview, *International Journal of Cyber Criminology*, 77-94.

Faqir, R. S. A. (2024). The Exclusionary Rule of AI-Enhanced Digital Evidence in the US and UAE: A Comparative Analysis, *Journal of Southwest Jiaotong University*, Vol. 59 (1), 76-91.

Faqir, R.S. A., and Alrousan, Ehab. (2023). Reimagining Criminology: The Transformative Power of the Postmodern Paradigm, *Pakistan Journal of Criminology*, Vol.15 (3), 151-170.

Hamlawi, H., and Charatiya, S. (2019). Do Social Networking Sites Affect the Spread of Cybercrimes among Algerian youth? Algeria: University of May 8, 1945, 1-16.

Harris, M. A. (2012). Managing Corporate Computer Crime and the Insider Threat: The Role of Cognitive Distortion Theory. *Journal of Information System Security*, Vol. 8 (2), 19-41.

Hersen, M and Gross, A.M. (2007). Handbook of Clinical Psychology. John Wiley & Sons, Inc,

Hollin, C. R. (2013). Psychology and crime: An introduction to criminological psychology. Routledge.

Issawi, N. (2017). Interpreted Theoretical Approaches to Criminal Conduct. Online Version. http://search.mandumah.com/Record/857667. (Accessed on 20 February 2024).

Jaishankar, K. (2007). Establishing a Theory of Cyber Crimes. *International Journal of Cyber Criminology*, Vol.1 (2), 7-9.

James, J. (2011). Cognitive-Behavioral Theory: An Alternative Conception. *Australian Psychologist*, Vol. 28(3), 151 - 155

Kalodner, C. R. (2011). Cognitive-behavioral theories. In D. Capuzzi & D. R. Gross (Eds.), Counseling and psychotherapy (5th ed). American Counseling Association, 193–213

Klass, E. T. (1978). Psychological effects of immoral actions: The experimental evidence. *Psychological Bulletin*, 85(4), 756.

Krkosh F. & Kothar S. The Interpretation of Criminal Conduct in the Family Context from a Systemic Perspective., 2017. Online Version. http://search.mandumah.com/Record/857667. (Accessed on 17 March 2024)

Moustafa, Ahmed A., Bello, Abubakar and Maurushat, Alana (2021). The Role of User Behavior in Improving Cyber Security Management, Frontiers in Psychology, available at https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2021.561011/full (Accessed on 10 March 2024)

Riley, Michael, Roberston, Jordan and Sharpe, Anita. (2017). The Equifax Hack Has the Hallmarks of State-Sponsored Pros, Bloomberg.

Rosenquist, Matt. (2015). Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers, Tim Dempsey.

Ruimel N. B. (2012) Modern Theoretical Trends Interpreting the Phenomenon of Crime: Towards an Analytical Reading Integration, *Journal of Communication*. Vol. 30. 27-41.

Samir, Q. D. (2022). National Cyber Security: A Reading of the most Important Security and Technical Strategies to Confront Cyber-crime in Alegria. *Riouq Journal of Social Studies*, Vol. 8 (2). 249-267.

Sarkar, G., and Shukla, S K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies, *Journal of Economic Criminology*, Vol. (2), 1-6.

Schmalleger, Frank and Pittaro, Michael. (2009). Crimes of the Internet, Prentice Hall, Upper Saddle River, N.J.

Shappie, Alexander T., and Debb, Scott M. (2019). Personality as a Predictor of Cybersecurity Behavior, *Psychology of Popular Media*, Vol. 9(4), 1-6.

Soleimani S. (2020). Cybercrime in Psych engineering. *Journal of Psychological and Educational Studies*. Vol.13. 456 – 471.

Stalans, L.J., Donner, C.M. (2018). Explaining Why Cybercrime Occurs: Criminological and Psychological Theories. In: Jahankhani, H. (eds) Cyber Criminology. Advanced Sciences and Technologies for Security Applications. Springer, Cham.

Tala L. (2020). Cybercrime: A new Dimension of the Concept of Criminality Across Website Platforms Social Communication, *Riouq Journal of Social Studies*, Vol.6 (2). 62-91.

Tawba S. (2022). Cybercrime: Activating Law Mechanisms for Justice. *Journal of Law and Humanities*. Vol.15 (3). 226-242.

Vinciguerra, T. (2023). Is ADHD Directly Related to Eventual Participation in Criminal Behavior (Doctoral dissertation, Florida Atlantic University).

Weissberg, L. (2022). Introduction: Psychoanalysis, Fatherhood, and the Work of Mourning. In: Weissberg, L. (eds) Psychoanalysis, Fatherhood, and the Modern Family. Palgrave Macmillan, Cham. Pp.1-30.

Zohri, H. T. (1984). Recent Theories in the Interpretation of Criminal Conduct, *Arab Journal of Security Studies*, Vol. 1 (1). 133 -138.