LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. S6(2025)

FINANCIAL CYBERCRIME IN THE UNITED ARAB EMIRATES: AN ANALYTICAL ASSESSMENT OF LEGAL AND REGULATORY FRAMEWORKS

Tareq Ali Salem Al Taboor Alnuaimi[1]*, Nuarrual Hilal Md Dahlan[2]

[1]*School of Law, Universiti Utara Malaysia.*
[2]School of Law, Universiti Utara Malaysia.

**Corresponding author E-mail: tareqalmu13@gmail.com[1]*

Abstract
The legal and regulatory frameworks regarding financial cybercrime in the UAE have seen significant legislative advancements, including Federal Decree-Law No. 20 of 2018, Federal Law No. 14 of 2018, and Federal Decree-Law No. 34 of 2021. These frameworks underscore the UAE's commitment to combating financial cybercrime and safeguarding its financial system. However, the evolving nature of cyber threats, jurisdictional complexities, inconsistent enforcement across financial sectors, and low public awareness present ongoing challenges. Despite the problems, this perspective, "Financial Cybercrime in the United Arab Emirates: An Analytical Assessment of Legal and Regulatory Frameworks," remains under-explored; hence, this study fills the gap. Given the above, this study by examines the effectiveness of UAE financial cybercrime laws, identifying key regulatory gaps, enforcement deficiencies, and underreporting issues. It employs a qualitative doctrinal approach, utilizing secondary sources such as law reports, academic articles, and books from high-ranking journals, with all data analyzed thematically. Additionally, general deterrence theory was applied to guide the analysis of the data explored in this study. Consequently, the findings indicate that the dynamic nature of cybercrime requires more adaptive regulatory frameworks, inconsistencies in enforcement create vulnerabilities in fintech and cryptocurrency platforms, and cyber literacy challenges hinder the full implementation of FATF recommendations. To address these gaps, the study suggests enhancing cross-border cooperation, improving enforcement mechanisms, increasing public awareness, and strengthening reporting frameworks. The study contributes valuable insights for policymakers, legal experts, and academics in law, security, and international studies, providing a basis for further research and policy enhancement.

Keywords: *Cybercrimes, Financial Cybercrimes, Legal Frameworks, United Arab Emirates*

1. Introduction

The United Arab Emirates (UAE) was established on December 2, 1971, initially comprising six emirates, with Ras Al Khaimah joining in 1972 (Kanso, 2023). The country's population is estimated as of January 25 to be 11,206,271 (Wolrdometer, 2025). Furthermore, the reliance on oil has diversified the country through initiatives like UAE Vision 2021 and Abu Dhabi Economic Vision 2030, which centers on fostering innovation and global investment, primarily through financial digital transformation (Crupi & Schilirò, 2023). However, this digital transformation has exposed the UAE to increasing financial cybercrime risks. Financial cybercrime involves illegal digital activities such as fraud, identity theft, ransomware, phishing, and cryptocurrency misuse for money laundering and terrorism financing (Tubaishat & AlAleeli, 2024); as stressed by Tubaishat and AlAleeli, the growing adoption of digital banking, fintech, and e-commerce in the UAE has made its financial system more vulnerable, as cybercriminals exploit technological advancements and the anonymity of digital transactions. As such, cryptocurrency presents regulatory challenges while offering innovation by complicating the tracking of illicit financial flows. The rise in cyber threats, including email phishing and ransomware attacks targeting financial institutions. For instance, according to the official report made by UAE Financial intelligence unit between 2021 and 2023, the UAE faced approximately AED 1.2 billion in financial losses from phishing, business email compromise, and investment scams (UAE Financial Intelligence Unit [UAEFIU 2024). Additionally, ransomware attacks rose to 34 incidents in 2024, reflecting a 65.3% increase in malware

detections (Khaleej Express, 2024). The above challenges underscore the urgent need for a robust legal framework to protect the UAE's financial system and maintain public trust.

Hussein and Mohammed (2024) stated that the UAE has implemented comprehensive legal frameworks to combat financial cybercrime. Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrimes criminalizes unauthorized financial system access, electronic fraud, identity theft, and cyber extortion, with strict penalties. Furthermore, Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) mandates financial institutions to conduct due diligence, monitor transactions, and report suspicious activities to curb illicit financial flows. Furthermore, Federal Law No. 14 of 2018 empowers the UAE Central Bank to regulate financial institutions and ensure compliance with anti-cybercrime measures. These regulations align with international standards set by the Financial Action Task Force (FATF), which provides global recommendations for combating financial crimes (Naheem, 2023).

Despite the UAE's robust regulatory efforts, financial cybercrimes persist due to several challenges, including legal framework deficiencies, jurisdictional complexities in cross-border enforcement, inconsistent regulatory application across financial sectors, and a lack of public awareness leading to underreporting. These challenges weaken preventative mechanisms and reduce the effectiveness of current laws. As a result, there has been an alarming rise in cyberattacks, with recent reports indicating that 86% of UAE businesses have experienced at least one successful cyberattack, and 44% of these resulted in financial losses, amounting to approximately 2.3 billion dirhams annually. The transnational nature of financial cybercrime presents significant enforcement difficulties, as seamless cooperation between jurisdictions and real-time intelligence sharing are crucial for an effective and timely response (Al Bloushi, 2020).

As a result of the above, this study raises the following question: What are the key challenges and gaps in the UAE's legal framework for financial cybercrime? This study examines the key challenges and gaps in the UAE's legal framework for financial cybercrime and examines proper solutions in line with the question. Also, despite the problems,

various scholars, including Hussein and Mohammed (2024), AllahRakha (2024), Naheem, (2023). Crupi and Schilirò (2023) and Al Bloushi (2020) have written many works regarding regulatory framework and digital currencies. However, the evidence reviewed from the extant literature indicates that none of the studies found to have addressed this perspective "Financial Cybercrime in the United Arab Emirates: An Analytical Assessment of Legal and Regulatory Frameworks." Hence, this study fills this gap in the body of literature and contributes to the body of knowledge.

2. Methodology

This study adopts a qualitative research methodology, specifically doctrinal legal research, to assess the impact of UAE financial cybercrime laws. Qualitative research, as outlined by Creswell (2013), involves the collection and analysis of non-numerical data, focusing on the exploration of complex legal issues. In this study, legal research is conducted by reviewing primary and secondary legal texts, including Federal Decree-Laws No. 20 of 2018, No. 14 of 2018, and No. 34 of 2021, alongside relevant scholarly articles, law reports, and books. The literature was collected through systematic searches in databases such as Westlaw, LexisNexis, Hein Online, ProQuest, Google Scholar, and Scopus; keywords used included “UAE cybercrime law,” “financial cybercrime,” “cybersecurity legislation,” “data integrity,” and “digital financial crimes.” Inclusion criteria comprised works published in English between 2015 and 2024 that focus on legal analysis, regulatory frameworks, or enforcement of financial cybercrime laws in the UAE or comparable jurisdictions. Exclusion criteria included non-peer-reviewed sources and publications unrelated to legal or policy aspects.

Given its doctrinal nature, this qualitative study does not involve empirical data such as interviews or case law analysis, and while this limits real-world enforcement verification, it provides a robust theoretical and legal foundation supported by authoritative sources. The research is underpinned by thematic analysis, allowing for the systematic identification of patterns and themes within the legal texts and existing literature. The validity and reliability of the research are ensured by using high-ranking sources from reputable legal journals and databases. Furthermore, consistency is maintained through clear inclusion and exclusion criteria during the literature selection process, as recommended by scholars like Mwita, K. (2022), who emphasises the importance of methodological rigour in legal research. The study also applies General Deterrence Theory, providing a theoretical framework for analysing the deterrent effect of the UAE's cybercrime laws. Research protocols include clear documentation of source selection, ethical considerations, and peer review to uphold the integrity of the findings.

3. Theoretical Framework

General deterrence theory, initially developed by Cesare Beccaria in the 18th century, has been further advanced by numerous scholars in the 21st century. Contemporary scholars have sought to refine the theory, incorporating new insights into how punishment systems can be **optimised** to deter crime, particularly in modern societal challenges. Recent scholars such as Nagin (2013), Piquero and Jennings (2017), and Apel (2013) have significantly contributed to the development of the theory by **emphasising** various aspects such as the certainty of punishment, the public's perception of legal consequences, and the relationship between deterrence and technological **advancements** in criminal behaviour. These modern interpretations of general deterrence theory reflect the evolving understanding of crime and punishment in an increasingly complex and interconnected world.

One recent scholar who has significantly expanded on general deterrence theory is David Nagin (2013). Nagin's work emphasises that the certainty of punishment plays a more significant role in deterrence than the severity of the punishment. He argued that people are more likely to be deterred by the perceived likelihood of being apprehended than by the severity of the legal consequences, which challenges traditional views that focus primarily on the harshness of punishment. Similarly, Piquero and Jennings (2017) focused on the role of certainty, showing that the more certain individuals perceive the legal consequences of their actions, the less likely they are to engage in criminal activities. Their findings suggest that deterrence is most effective when based on the predictability of punishment rather than its severity, aligning with the rational choice model inherent in general deterrence theory.

Additionally, Apel (2013) has made significant contributions by exploring how perceptions of punishment, both for offenders and the general public, affect deterrence. Apel's research shows that the general deterrent effect is stronger when the public believes that punishment is fair and just, further illustrating how the public's perception of legal legitimacy and the credibility of law enforcement can amplify the deterrent effect. His work has been pivotal in extending the theory's applicability to modern legal and social contexts, where individuals' perceptions of fairness and justice play a crucial role in influencing behaviour.

These contemporary scholars' contributions have helped refine general deterrence theory, making it more applicable to understanding criminal behaviour in today's society, where issues such as the certainty and immediacy of punishment, rather than its severity, have emerged as critical deterrents. In the context of financial cybercrime in the United Arab Emirates (UAE), general deterrence theory was crucial in assessing the effectiveness of the country's legal and regulatory frameworks. The perceived certainty and severity of punishment for cybercrime offences are critical factors in determining whether individuals are deterred from engaging in financial cybercrimes.

Consequently, by applying general deterrence theory, this study can assess how well the UAE's legal system prevents cybercriminal behaviour, specifically concerning financial crimes involving advanced technology. The findings of this research contribute to scientific knowledge by refining the understanding of deterrence mechanisms in the digital age, particularly in regions where financial cybercrimes are on the rise. By considering the perceptions of potential offenders and the public's trust in the legal system, this study provides valuable insights into how legal frameworks in the UAE can be strengthened to deter financial cybercrime and improve the enforcement of anti-cybercrime laws.

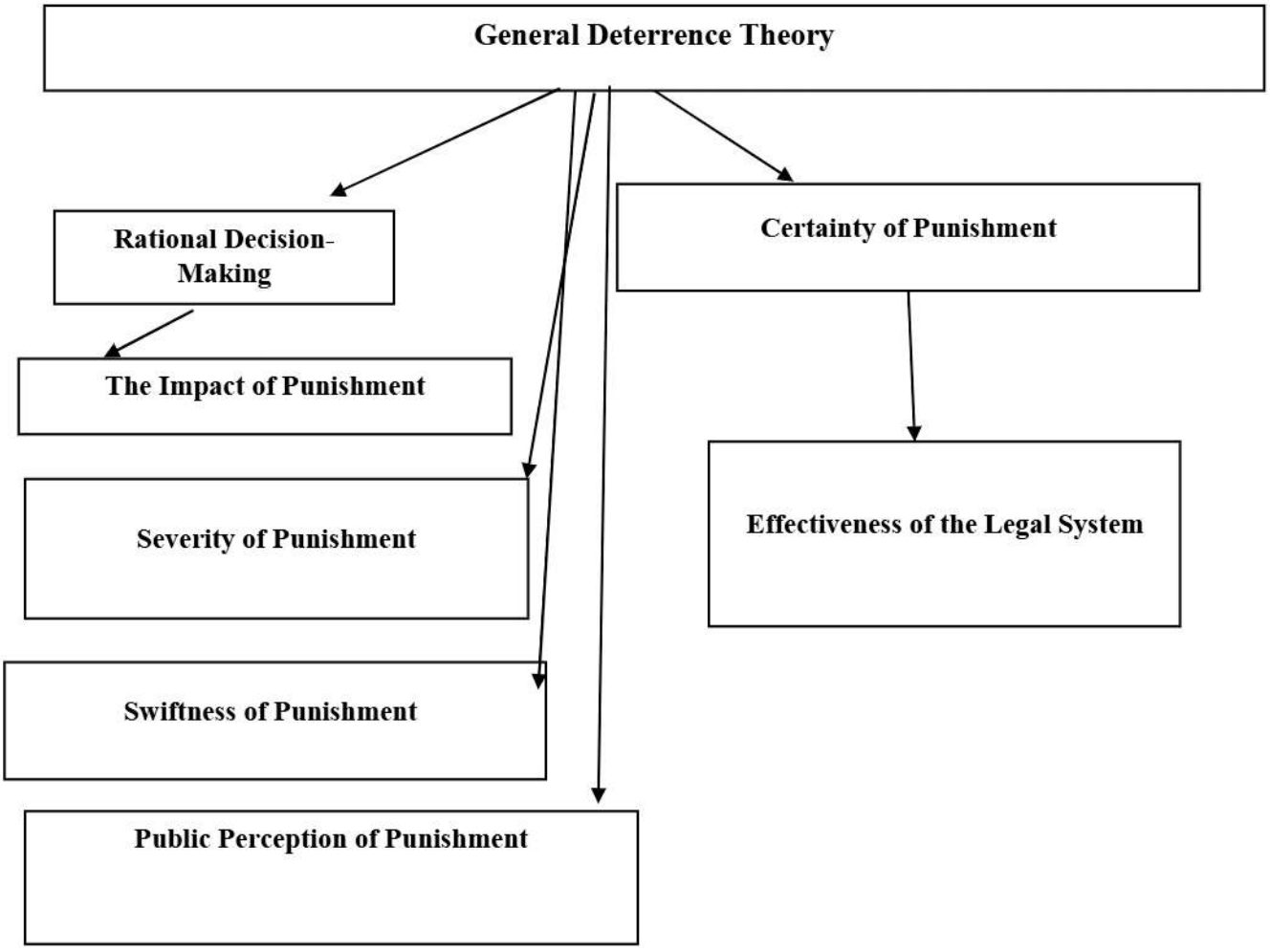

Figure 1 Research Framework

4. Literature Review

4.1 Concepts of cybercrimes

Cybercrime, as a multidimensional and evolving phenomenon, has been defined and interpreted differently by scholars over time, reflecting its complexity and challenges to legal frameworks. Scholars such as Goni et al. (2022) and AllahRakha (2024) define cybercrime broadly as illegal activities conducted through or targeting computer systems, **emphasising** its diverse forms, ranging from financial fraud to cyber terrorism. Also, some scholars build on this understanding by categorising cybercrime into crimes against systems, crimes facilitated by technology, and crimes involving illicit content. Also, AllahRakha affirms that these definitions underscore cybercrime's dynamic and borderless nature, complicating efforts to develop cohesive legal responses and **categorising** cybercrime into crimes against systems, crimes facilitated by technology, and crimes involving illicit content.

The conceptual ambiguity surrounding cybercrime has been a recurring theme in scholarly discourse. Scholars like Shukura and Jafarov (2023) argue that the lack of a universally accepted definition hampers **formulating** and enforcing adequate legal frameworks. This definitional gap is particularly problematic in cross-border contexts, where inconsistencies in national laws create significant enforcement challenges. For instance, an act considered a cybercrime in one jurisdiction might not qualify as an **offence** in another; as highlighted by Shukura and Jafarov, such discrepancies not only hinder international cooperation but also allow cybercriminals to exploit jurisdictional loopholes to evade prosecution.

Moreover, the transnational nature of cybercrime further complicates its legal regulation. Wall (2021) noted that cybercrimes often involve perpetrators, victims, and digital evidence distributed across multiple jurisdictions, creating challenges in determining which laws apply and which authorities hold jurisdiction. Scholars argue that traditional legal principles rooted in territoriality are ill-suited to address the realities of cyberspace. This has led to the adoption of Mutual Legal Assistance Treaties (MLATs) as a tool for cross-border cooperation. However, Goni notes that these treaties are often plagued by inefficiencies, such as bureaucratic delays and differing evidentiary standards, which undermine their **effectiveness** in combating cybercrime.

Besides, technological **advancements** have further exacerbated the challenges of regulating cybercrime. Emerging technologies, such as blockchain and cryptocurrencies, have revolutionised financial transactions and provided new avenues for criminal activity (Girasa, 2018). Initially, Nakamoto and Bitcoin's (2008) introduction of Bitcoin, for instance, has facilitated anonymous transactions, making it a preferred tool for money laundering and ransomware payments. Houben and Snyers (2018) argue that the decentralised nature of cryptocurrencies poses unique challenges for regulators, as these technologies often operate outside the jurisdiction of any single nation-state. Hence, they suggested that legal frameworks must adapt to address these complexities, integrating robust regulatory measures while balancing innovation and privacy concerns

Similarly, concerning the societal impact of cybercrime, some scholars, including Alghamdi (2020), highlight that the prevalence of cybercrime erodes consumer confidence in online services, with victims often reluctant to report incidents due to a lack of awareness or trust in the legal system. This underreporting distorts the understanding of cybercrime's scale and impedes the development of effective legal responses. Also, Alghamdi further **emphasises** that this issue is especially pronounced in developing countries, where weak legal and institutional frameworks leave societies more vulnerable to cyber threats.

The current literature on cybercrime in the UAE reveals several key gaps that warrant further research. While scholars, such as Graham (2023), emphasise the importance of public-private partnerships for combating cybercrime, there is insufficient analysis of how regulatory frameworks can be reformed to facilitate these collaborations, especially considering conflicting interests between public and private entities. Additionally, the effectiveness of existing cybersecurity laws, such as Federal Decree-Law No. 34 of 2021, is another area needing closer scrutiny, particularly in relation to the rapid evolution of cyber threats and real-world enforcement. Furthermore, the challenges posed by cross-border jurisdictional issues in tackling transnational cybercrime are not adequately addressed, despite the UAE's active engagement in international efforts. Lastly, the regulation of emerging sectors like fintech and cryptocurrency in relation to financial cybercrime remains under-explored, presenting another critical area for research to ensure that the UAE's legal frameworks can keep pace with evolving cyber-enabled financial crimes. Hence this study address this gap in the body of literature and add to the body of knowledge.

4.2 Concept of financial cybercrime

Financial cybercrime has become a global threat, posing significant challenges to legal frameworks worldwide. Nicholls et al. (2021) define it broadly as unlawful acts targeting financial systems via digital means; it encompasses crimes like ransomware, phishing, and fraud. These activities exploit the interconnected nature of global economic systems and point out the need for cohesive legal mechanisms to address them. The transnational nature of financial cybercrime complicates enforcement, as perpetrators often operate across jurisdictions. While foundational, the Budapest Convention on Cybercrime suffers from limited adoption in key regions like Asia and Africa, where concerns over sovereignty and data privacy deter participation (Świątkowska, 2020 & Shaffer, 2024). Also, the emergence of **cryptocurrency** further complicates the legal landscape. Its **decentralised** and anonymous nature has facilitated crimes such as money laundering, with varying regulatory responses across jurisdictions (Modi, 2023). Similarly, the Financial **Action** Task Force recommended **standardising** anti-money laundering (AML) measures, but inconsistent enforcement creates loopholes for exploitation. For instance, the European Union has advanced AML frameworks, whereas lax regulations in other regions undermine global efforts. Similarly, **decentralised** finance (DeFi) platforms present challenges due to the absence of intermediaries and accountability mechanisms, and the Poly Network hack of 2021, which saw $600 million stolen, underscores the urgency for legal systems to adapt to emerging technologies (Cong, **et al.** 2023).

As a result, Modi (2023) and Cong et al. (2023) called for global protocols that balance data sharing with privacy protection to improve detection and prevention efforts. They **emphasise** that social engineering tactics, such as phishing, also underscore the human vulnerability in financial cybercrime. They conclude that legal frameworks must extend beyond technical safeguards to mandate public education and institutional compliance. The European Union's GDPR exemplifies this by addressing data protection, though gaps remain in enforcement, particularly in developing economies.

4.3 Cybercrime Threats in the UAE

As recent data and trends indicate, cyberattacks increasingly pose a significant threat to national security. In 2021, worldwide cyberattacks surged by 50%, tripling the 2020 level and escalating sevenfold in the United Arab Emirates (UAE). The average weekly cyberattacks during Q4 2021 reached 925 globally and 408 in the UAE. The pandemic in the UAE led to a 250% increase in cyberattacks in 2020, including 1.1 million phishing attempts, a common method for launching ransomware attacks. Ransomware threat groups in the UAE rose notably, with 78% of **organisations** reporting their presence in 2020, up from 66% in 2019. Sophos estimated that 59% of UAE **organisations** were affected by ransomware in the previous year, causing more severe damage than the year before (Tubaishat & AlAleeli, 2024). Also, when a company faces a data breach, it confronts two challenging choices: paying the ransom or attempting data recovery through application restoration. Ransomware attacks can exert immense pressure on companies to resume operations quickly. Paying the ransom, however, exposes **organisations** to further interference by Transmitter Address (TA), potentially enabling backdoors and password copying for eavesdropping. Leftover toxic materials in a network may subject a company to repeated attacks (Humayun et al., 2020). Cyber Eason reported that 84% of UAE-based companies paid ransom in these attack cases, surpassing the global **average** by over 20%. Many firms that paid ransom reported experiencing a second attack, with data corruption or erasure a common outcome (Tubaishat & AlAleeli, 2024)

4.4 Legal and Regulatory Analysis of Financial Cybercrimes in the UAE

The regulation of financial cybercrimes in the UAE has undergone significant development, underscored by the enactment of pivotal laws such as Federal Decree-Law No. 20 of 2018, Federal Law No. 14 of 2018, and Federal Decree-Law No. 34 of 2021. These legal frameworks aim to combat financial crimes, reflecting the UAE's commitment to maintaining the integrity of its financial system (Maghaireh, 2024). However, the rapid evolution of digital technologies and the increasing sophistication of cybercriminal activities have introduced regulatory challenges that reveal critical challenges in these frameworks. For example, Federal Decree-Law No. 20 of 2018 exemplifies the UAE's proactive stance against money laundering and terrorism financing, establishing stringent compliance mechanisms for financial institutions. Article 2 clearly defines financial crimes under this law, and the law mandates rigorous measures for monitoring and reporting suspicious transactions. Despite these provisions, the framework's ability to address cyber-enabled laundering techniques, such as cryptocurrency abuse, remains limited (Allahrakha, 2023). As noted by Allahrakha, this law does not explicitly account for the challenges posed by decentralised financial systems and blockchain technology; an omission or technological gap underscores a broader issue: while the framework is effective against traditional money laundering methods, it struggles to adapt to the dynamic nature of digital financial crimes, allowing cybercriminals to exploit unregulated areas.

In stark contrast, Federal Law No. 14 of 2018 complements the anti-money laundering framework by strengthening the UAE Central Bank's oversight capacity. Articles 54 and 58 emphasise risk management and reporting obligations, ensuring financial institutions implement robust preventive measures to avoid financial cybercrimes (Naheem, 2023). However, Tareq has highlighted disparities in applying these mandates across financial sectors. Another issue remains the enforcement of financial cybercrime laws in the UAE, which varies significantly between traditional financial institutions and emerging fintech and cryptocurrency platforms. Established entities like banks and insurance companies are well-regulated under the supervision of the UAE Central Bank and other regulatory bodies, adhering to stringent compliance requirements.

Similarly, Watts and Wallman (2024) observed that newer entities in the fintech and cryptocurrency sectors often face inconsistent regulatory oversight. The fragmented regulatory landscape across the UAE's free zones, such as the Dubai International Financial Centre (DIFC) and the Abu Dhabi Global Market (ADGM), is a major reason for this inconsistency. These zones operate under distinct legal frameworks with separate regulatory bodies, often leading to approaches not fully aligned with federal laws. As underpinned by Al-Tawil (2023), this lack of uniformity creates regulatory loopholes, particularly in digital asset sectors. For example, cryptocurrency exchanges and virtual asset service providers (VASPs) often fall outside the **purview** of federal authorities, resulting in gaps in monitoring and reporting suspicious activities. Such discrepancies undermine the effectiveness of the UAE's financial cybersecurity framework, leaving certain sectors more vulnerable to risks such as fraud and money laundering.

In a similar vein, Decree-Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) outlines obligations for financial institutions and designated non-financial businesses and professions (DNFBPs) to implement adequate anti-money laundering measures (Morgan et al., 2020). However, inconsistent enforcement across sectors reduces public trust in financial systems, deters foreign investment, and creates vulnerabilities that cybercriminals can exploit. **Also, smaller** institutions and fintech startups face particular challenges due to limited resources and expertise, unlike larger entities that are better positioned to meet compliance requirements.

As opined emphatically by Al-Tawil (2023), these disparities exacerbate regulatory blind spots, making underregulated sectors prime targets for cybercriminals. Additionally, the absence of

real-time information-sharing mechanisms among financial entities weakens the agility needed to combat evolving cyber threats. Furthermore, Al-Tawil highlights the importance of effectively fostering collaborative defences to address these challenges. Enhanced coordination, standardised enforcement, and robust collaboration are critical to strengthening the UAE's financial cybersecurity framework.

Relatedly, the Federal Decree-Law No. 34 of 2021 represents a comprehensive effort to address broader cybercrime challenges, including electronic fraud, unauthorised access, and identity theft. Articles 4 and 5 impose severe penalties on offenders and grant authorities' significant powers to respond to cyber incidents (Hussein and Mohammed, 2024). However, the law's focus on punitive measures over preventive strategies limits its efficacy. Public awareness campaigns and reporting mechanisms remain underdeveloped, as evidenced by a 2022 survey by the UAE Cybersecurity Council, which found that a substantial portion of financial crimes go unreported (Al-Tawil, 2023). This underreporting stems from victims' fear of reputational damage or a lack of understanding about reporting procedures, a gap emphasised by Al-Tawil. **The resulting incomplete crime data** complicates efforts to understand and address the full scope of financial cybercrimes, further exposing systemic vulnerabilities within the framework (Aljassmi et al., 2024).

Besides, Al-Tawil (2023) **noted** that cross-border enforcement emerges as another critical challenge, as financial cybercrimes often transcend national boundaries. Federal Law No. 14 of 2018 incorporates provisions for international cooperation, but procedural delays and jurisdictional conflicts hinder their effectiveness. Hussein and Mohammed (2024) highlight instances where the absence of harmonised global standards for cryptocurrency regulations complicates the prosecution of offenders and the recovery of illicit assets. Moreover, the reliance on mutual legal assistance treaties (MLATs) falls short of addressing the speed and complexity of cross-border financial cybercrimes. He emphasised that these challenges underline the inadequacy of current international cooperation frameworks in combating transnational cyber threats, underscoring the need for innovative solutions that bridge jurisdictional gaps and enhance procedural efficiency.

Also, the uneven enforcement of regulations across financial sectors compounds the vulnerabilities within the UAE's legal framework. Federal Law No. 14 of 2018 tasks the UAE Central Bank with ensuring compliance across all financial entities, yet enforcement efforts often favour well-established institutions over smaller players (Naheem, 2023). Scholars Crupi and Schilirò (2023) note that resource constraints disproportionately affect fintech companies and informal financial systems, creating opportunities for cybercriminals to exploit less-regulated entities. They attribute these disparities to regulatory capacity and oversight gaps, undermining the law's objectives.

Consequently, to converge on the argument that jurisdictional conflicts and procedural delays in cross-border enforcement exacerbate vulnerabilities within the UAE's legal and regulatory framework for addressing financial cybercrimes. As noted by Sultan and Mohamed (2023), the **global standards for cryptocurrency regulation and digital financial instruments** significantly impede the ability to prosecute offenders and recover illicit proceeds effectively. These shortcomings highlight critical deficiencies in the UAE's legislative architecture, including Federal Decree-Law No. 20 of 2018 and Federal Decree-Law No. 34 of 2021, which, despite their provisions, fall short in addressing the complex and transnational nature of financial cybercrimes. Their scholarly works further indicate that fragmented enforcement mechanisms contribute to systemic weaknesses, undermining the efficacy of regulatory efforts in combating these crimes

4.5 The Financial Action Task Force (FATF) and Its Role in Regulating Financial Cybercrimes in the UAE

The Financial Action Task Force (FATF) plays a crucial role in the global fight against financial crimes, including those committed through cyber means. Its standards and recommendations are designed to combat money laundering and the financing of terrorism, which are often facilitated by financial cybercrimes (Naheem, 2023). **Scholars** Al-Tawil (2023) confirmed that the FATF, the UAE, has aligned its legal and regulatory framework with these international standards to curb financial crimes effectively. The FATF's recommendations provide a blueprint for national policies to strengthen the governance of financial sectors, including digital finance, and improve cross-border cooperation among jurisdictions in investigating and prosecuting cybercrimes.

In line with FATF's guidance, the UAE has implemented several laws and regulations addressing financial cybercrimes. The enactment of Federal Decree-Law No. 34 of 2021 was a significant step in this regard, incorporating provisions to tackle activities such as money laundering, credit card fraud, and embezzlement, often facilitated by cyber techniques. Teichmann and Wittmann (2023) opined that this law **criminalises** various offences related to financial cybercrimes, specifying severe penalties for those who misuse digital entities and commit fraud. Integrating FATF's recommendations into the UAE's legal framework ensures that these financial crimes are treated with the same severity as other forms of criminal activities, reinforcing the country's commitment to international standards of financial integrity.

Moreover, the UAE's strategy to combat financial cybercrimes is also demonstrated through its establishment of platforms such as the "go AML" digital platform (Al-Tawil, 2024). This platform aligns with FATF's recommendation to enhance transparency and traceability of financial transactions, enabling the UAE to monitor and **analyse** financial data for money laundering activities. By incorporating these technologies, the UAE meets the FATF's requirements and sets a precedent for other regional nations. **He emphasised** that the platform is designed to facilitate identifying and tracking illicit financial flows, helping financial institutions detect suspicious activities more efficiently. This proactive approach is vital in addressing the evolving threats of financial cybercrimes.

Scholars, including Al-Tawil (2024), Teichmann and Wittmann (2023), Naheem (2023), and Al-Tawil (2023), acknowledge that despite advancements, the effectiveness of the UAE's legal and regulatory framework in combating financial cybercrimes remains limited. The primary challenge lies in the rapid evolution of cybercrime tactics, which often outpace regulatory updates. For instance, Naheem (2023) noted that as FATF recommendations evolve to address emerging threats, the UAE must continuously revise its laws to remain compliant and effective. Financial cybercrimes' dynamic and transnational nature necessitate robust national regulations and enhanced international cooperation.

While the UAE aligns its financial regulations with FATF standards, a gap in cyber literacy among financial institutions persists. This deficiency hinders effective law implementation and reduces deterrent effects. As such Murrar and Barakat (2021) in respect to FATF underscores the need for financial institutions to understand cyber risks and compliance measures. Targeted training and awareness campaigns are essential to enhance cybersecurity capabilities. Additionally, the transnational nature of financial cybercrimes presents challenges in seamless cross-border cooperation (Al-Tawil, 2023; Naheem, 2023). Although the UAE has bilateral agreements, enforcement across jurisdictions remains difficult. Thus, the FATF recommends improved legal assistance and advanced technology for asset recovery.

5 Discussion and Findings

5.1 Cybercrime

This study found that cybercrime, as a multifaceted and evolving challenge, presents significant difficulties in legal regulation due to its dynamic and borderless nature. The findings of this study reveal that scholars such as Goni et al. (2022) and AllahRakha (2024) emphasise the need to categorise cybercrime into distinct types, including crimes against systems, crimes facilitated by technology, and crimes involving illicit content. This study's findings also show that the definitional ambiguity of cybercrime, as highlighted by Shukura and Jafarov (2023), complicates efforts to establish comprehensive legal frameworks, particularly in cross-border contexts. The findings further reveal that scholars highlight the issue of jurisdictional discrepancies, which hinder international cooperation and allow cybercriminals to exploit legal loopholes. Additionally, this study indicates that traditional legal principles rooted in territoriality are insufficient to address cybercrime's transnational character, leading to reliance on Mutual Legal Assistance Treaties (MLATs), which, according to Goni et al. (2022), are often undermined by inefficiencies such as bureaucratic delays and varying evidentiary standards.

Furthermore, this study reveals that technological advancements like blockchain and cryptocurrencies have exacerbated challenges in cybercrime regulation. The findings show that Girasa (2018) and Houben and Snyers (2018) highlight the decentralised nature of cryptocurrencies, which complicates regulatory efforts and facilitates cybercrimes such as money laundering and ransomware attacks. Similarly, the study found that the societal impact of cybercrime, as discussed by Alghamdi (2020), erodes consumer trust in online services, with underreporting further distorting the scale of the issue, particularly in developing countries with weak legal frameworks. This study also reveals that legal scholars like Graham (2023) emphasise the critical role of public-private partnerships in combating cyber threats. However, the findings indicate that conflicting interests between the public and private sectors, regulatory gaps, and data protection laws create obstacles to effective collaboration. These insights highlight the necessity for adaptive legal frameworks that balance innovation, privacy, and enforcement to address the complexities of cybercrime effectively.

These findings, when assessed through the lens of General Deterrence Theory (GDT), reveal several shortcomings in achieving a strong deterrent effect. Although the UAE's legal framework prescribes stringent penalties under laws such as Decree-Law No. 34 of 2021, GDT posits that the perceived *certainty* and *swiftness* of punishment are often more influential than severity alone. Underreporting of cybercrime, cross-border enforcement hurdles, and procedural delays weaken the perceived risk of apprehension and thus reduce the overall deterrent effect. Moreover, the limited visibility of successful prosecutions may contribute to a public perception that cybercriminals are unlikely to face consequences. Enhancing international legal cooperation, accelerating judicial processes, and fostering greater public awareness could therefore serve not only to improve enforcement but also to strengthen the preventative impact predicted by General Deterrence Theory.

5.2 financial cybercrime as a global threat

This study found that financial cybercrime has emerged as a global threat, presenting significant challenges to legal frameworks worldwide. The findings show that Nicholls et al. (2021) define financial cybercrime as unlawful acts targeting financial systems via digital means, such as ransomware, phishing, and fraud. The transnational nature of financial cybercrime complicates enforcement, as perpetrators often operate across jurisdictions, requiring cohesive international legal mechanisms. Świątkowska (2020) and Shaffer (2024) argue that while the Budapest Convention on Cybercrime provides a foundational framework, its limited adoption in key regions such as Asia and Africa hinders global efforts due to

sovereignty and data privacy concerns. The findings further indicate that the rise of cryptocurrency adds to the complexity, with its decentralised and anonymous nature facilitating crimes like money laundering and fraud, compounded by varying regulatory responses across jurisdictions (Modi, 2023).

The study also highlights the Financial Action Task Force's recommendations to standardise anti-money laundering (AML) measures, though inconsistent enforcement allows for exploitation of regulatory loopholes. Cong et al. (2023) underscore the urgency of addressing decentralised finance (DeFi) platforms, with examples like the Poly Network hack in 2021, where $600 million was stolen. Moreover, this study found that global protocols must balance data sharing with privacy protection to enhance detection and prevention. Scholars like Modi (2023) and Cong et al. (2023) stress the importance of extending legal frameworks beyond technical safeguards to include public education and institutional compliance. Although the European Union's GDPR sets a precedent in data protection, the findings suggest that enforcement gaps remain, particularly in developing economies.

From the perspective of **Deterrence Theory (GDT)**, the study highlights critical issues related to the certainty, severity, and swiftness of punishment in tackling financial cybercrime. While many legal frameworks impose severe penalties for cybercrime, including the theft of funds through ransomware or cryptocurrency fraud, GDT posits that the *certainty* of punishment plays a more significant role than severity alone. The study reveals that the transnational nature of financial cybercrime and jurisdictional challenges result in low certainty of punishment, as perpetrators often exploit international legal loopholes. Furthermore, inconsistent enforcement and regulatory gaps across jurisdictions, particularly in regions with underdeveloped legal frameworks, diminish the deterrent effect, as offenders may perceive a low risk of being apprehended. The issue of *celerity*—the speed at which justice is administered—also comes into play, as delays in enforcement processes or international cooperation hinder effective deterrence. While increasing penalties might seem to strengthen deterrence, GDT emphasises that without improving the certainty and swiftness of punishment, the deterrent effect will not be fully realised. To enhance deterrence, the findings suggest that a more cohesive and standardised approach to enforcement, coupled with improved public education and institutional compliance, is necessary. This would align with GDT's core principle that the deterrence effect increases when potential offenders perceive a high likelihood of punishment and swift consequences for their actions.

5.3 Financial cybercrime as a threat to UAE national security

The results of this study indicate that cyberattacks have become a critical threat to the UAE's national security, as highlighted by Tubaishat and AlAleeli (2024), who refer to recent data and trends. In 2021, global cyberattacks increased by 50%, with attacks in the UAE growing sevenfold compared to 2020. The study reveals that the pandemic triggered a 250% surge in cyberattacks in the UAE in 2020, including 1.1 million phishing attempts, a common precursor for ransomware deployment. The increase in ransomware threat groups was significant, with 78% of organisations in the UAE reporting their presence in 2020, compared to 66% in 2019. According to Sophos (2021), 59% of UAE organisations were affected by ransomware in the previous year, causing greater damage than before. The study observes that companies facing data breaches often face a difficult decision between paying the ransom or attempting data recovery, with paying the ransom exposing organisations to further risks such as backdoors and password theft. Cyber Eason (2021) reported that 84% of UAE-based firms paid ransom in these cases, exceeding the global average by more than 20%, with many experiencing repeat attacks, leading to data corruption or loss (Humayun et al., 2020).

From the perspective of **Deterrence Theory (GDT)**, these findings suggest that the threat of cyberattacks in the UAE could be more effectively managed by increasing the certainty and

swiftness of punishment for offenders. According to GDT, the deterrent effect of legal punishment is strongest when potential offenders perceive a high likelihood of being apprehended and punished swiftly. However, the study highlights the low certainty of punishment for cybercriminals due to challenges in international cooperation, the rapid evolution of cybercrime techniques, and jurisdictional issues. This results in offenders perceiving a low risk of being caught, which undermines deterrence efforts. In addition, while the penalties for cybercrime in the UAE, such as those outlined in the country's Cybersecurity Law, may be severe, GDT suggests that the effectiveness of deterrence is less about severity and more about certainty.

Consequently, the study suggests that increasing the enforcement of legal frameworks and improving international collaboration could raise the certainty of punishment, thereby enhancing the deterrent effect. Furthermore, addressing the issue of *celerity*—the speed with which punishment is meted out—would also strengthen deterrence. The delay in responding to cybercrime due to complex international jurisdictional challenges diminishes the impact of punishment, allowing offenders to continue exploiting vulnerabilities without fear of swift consequences. Therefore, in line with GDT, the findings advocate for a more integrated and responsive approach to cybercrime regulation, focusing on increasing the certainty and speed of punishment to effectively deter offenders.

5.4 legal and regulatory frameworks governing financial cybercrimes in the UAE

The findings of this research indicate that the legal and regulatory frameworks governing financial cybercrimes in the UAE have evolved significantly with the implementation of key legislative measures such as Federal Decree-Law No. 20 of 2018, Federal Law No. 14 of 2018, and Federal Decree-Law No. 34 of 2021, reflecting the UAE's proactive stance in combating financial crimes and maintaining the stability of its financial sector (Maghaireh, 2024). However, the study highlights that the rapid evolution of digital technologies and increasingly sophisticated cyber threats have introduced substantial regulatory challenges. For instance, while Federal Decree-Law No. 20 of 2018 provides stringent compliance measures for financial institutions, it falls short in addressing emerging cyber-enabled laundering methods, such as those involving cryptocurrencies, and lacks provisions for decentralised financial systems. This gap has allowed cybercriminals to exploit regulatory blind spots, thus creating vulnerabilities in the system.

Furthermore, while Federal Law No. 14 of 2018 enhances the Central Bank's oversight and bolsters risk management practices (Naheem, 2023), the study identifies enforcement disparities across different sectors. Traditional financial institutions such as banks are subject to more rigorous regulations than fintech and cryptocurrency platforms (Watts & Wallman, 2024). Regulatory inconsistencies between the UAE's financial free zones, such as the Dubai International Financial Centre (DIFC) and the Abu Dhabi Global Market (ADGM), exacerbate these challenges, as independent legal frameworks within these zones may not align fully with federal legislation (Al-Tawil, 2023). The research also reveals that despite the stringent penalties imposed by Federal Decree-Law No. 34 of 2021, the law's focus on punitive measures rather than preventive strategies limits its overall impact. Additionally, the study found a significant underreporting of financial cybercrimes, with only 30% of scam victims reporting incidents to law enforcement, primarily due to concerns over reputational harm and lack of awareness about reporting procedures (UAE Cybersecurity Council, 2024). The underreporting issue is compounded by cross-border enforcement challenges, such as procedural delays and jurisdictional conflicts, which hinder effective prosecution and asset recovery efforts (Hussein & Mohammed, 2024).

In light of **Deterrence Theory (GDT)**, the findings underscore the importance of enhancing the certainty and speed of punishment for financial cybercrime offenders in the UAE.

According to GDT, deterrence is most effective when potential offenders perceive a high likelihood of being caught and swiftly punished. However, the current regulatory and enforcement frameworks, with their inconsistencies and gaps, create an environment where cybercriminals can exploit jurisdictional issues and delays in law enforcement, thereby reducing the perceived risk of detection and punishment. GDT suggests that the effectiveness of deterrence can be improved by increasing both the certainty of detection and the speed of legal proceedings. By improving coordination among federal and local regulatory bodies, strengthening international cooperation, and implementing real-time information sharing mechanisms, the UAE could raise the perceived risks for offenders, thereby enhancing the deterrent effect. Additionally, a more balanced approach that integrates both preventive and punitive measures, alongside greater public awareness of reporting procedures, would further strengthen the overall deterrence strategy, effectively reducing the prevalence of financial cybercrime in the region.

5.5 The Role of the Financial Action Task Force (FATF) in UAE

The findings of this study underscore the pivotal role of the Financial Action Task Force (FATF) in shaping the UAE's regulatory framework to combat financial cybercrimes. The research indicates that the UAE has made significant strides in aligning its legal and regulatory systems with FATF recommendations, particularly through the enactment of Federal Decree-Law No. 34 of 2021. This legislation reflects the UAE's strong commitment to tackling financial cybercrimes, such as money laundering and fraud, and has reinforced governance in the financial sector, providing a robust framework to prevent cyber-enabled financial crimes (Teichmann & Wittmann, 2023). Additionally, the integration of FATF standards into national legal structures has bolstered the country's capacity to combat financial cybercrime. Notably, technological initiatives, such as the "go AML" digital platform highlighted by Al-Tawil (2024), have enhanced the UAE's ability to monitor and detect illicit financial activities, improving traceability and transparency in financial transactions.

However, the study also reveals significant challenges that hinder the full effectiveness of the UAE's regulatory measures. As noted by Murrar and Barakat (2021), a key barrier remains the lack of cyber literacy among financial institutions, which impedes the effective application of FATF's recommendations. Furthermore, the transnational nature of financial cybercrimes, as discussed by Al-Tawil (2023) and Naheem (2023), presents complex obstacles to seamless international cooperation. The findings suggest that jurisdictional conflicts and procedural delays limit the UAE's enforcement capabilities, even in the face of bilateral agreements. Consequently, the FATF advocates for enhanced legal assistance and the adoption of advanced technological solutions to improve cross-border asset recovery efforts.

In line with **Deterrence Theory (GDT)**, these findings highlight the importance of an effective deterrent framework, which requires not only the certainty of detection but also the severity of penalties. GDT posits that offenders are less likely to engage in criminal activity if they perceive a high likelihood of being apprehended and severely punished. The UAE's alignment with FATF guidelines and its investment in technological tools such as the "go AML" platform contribute to increasing the certainty of detection. However, the study reveals that the challenges of cyber literacy, jurisdictional complexities, and limited international cooperation reduce the deterrent effect. To strengthen deterrence, the UAE must not only refine its regulatory framework but also enhance enforcement measures, both domestically and internationally. This includes addressing the knowledge gaps within financial institutions, fostering international collaboration, and ensuring the legal system remains agile in adapting to evolving cyber threats. By improving these areas, the UAE can better align with the principles of GDT, effectively deterring financial cybercrime and protecting its financial infrastructure.

Conclusion

This study has critically examined the legal and regulatory frameworks addressing financial cybercrime in the United Arab Emirates (UAE), with a focus on key legislative measures aimed at safeguarding the financial sector. Notably, Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrimes plays a central role in criminalising unauthorised access to financial systems, electronic fraud, identity theft, and cyber extortion, all while imposing stringent penalties designed to deter offenders. Additionally, Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) further strengthens the regulatory environment by obliging financial institutions to implement rigorous due diligence, transaction monitoring, and reporting mechanisms. Together, these legal provisions are designed to protect the UAE's financial ecosystem from increasingly sophisticated cyber threats and align with global financial security standards.

Despite the robust legal framework, the study highlights the substantial challenges associated with enforcing financial cybercrime regulations, particularly in light of the complex and transnational nature of cybercrimes. While Federal Law No. 14 of 2018 empowers the UAE Central Bank to regulate financial institutions and ensure adherence to anti-cybercrime measures, cybercriminals continue to exploit technological advancements, circumventing detection and regulatory efforts. Consequently, ongoing regulatory updates and significant investments in technological infrastructure are essential. The study stresses the importance of enhanced cooperation between regulatory bodies, law enforcement agencies, and financial institutions to combat financial cybercrime effectively.

Furthermore, the research reveals that while the UAE government has made commendable strides in fostering a secure financial environment through comprehensive legal measures, significant challenges remain. Issues such as deficiencies within the legal framework, jurisdictional complexities in cross-border enforcement, inconsistent regulatory application across financial sectors, and a lack of public awareness resulting in underreporting of cybercrimes—have hindered progress. The alarming rise in cyberattacks, with reports indicating that 86% of UAE businesses have experienced at least one successful cyberattack, highlights the urgency of addressing these gaps. These attacks have resulted in substantial financial losses, amounting to approximately 2.3 billion dirhams annually.

In the context of **Deterrence Theory (GDT)**, the study's findings reinforce the importance of an effective deterrent framework, where the certainty of detection and the severity of penalties are key to preventing cybercrime. While the stringent penalties outlined in the UAE's laws are a step in the right direction, the study suggests that enhancing the overall deterrence effect requires more than just punitive measures. There must be a continuous evolution of regulatory and technological frameworks to keep pace with emerging cyber threats. Moreover, improving international cooperation, enhancing cross-border legal assistance, and fostering a culture of compliance within financial institutions will further reinforce the deterrent effect, making it more difficult for offenders to evade detection and prosecution. Thus, the UAE’s regulatory frameworks need to be adaptive, forward-thinking, and well-coordinated to effectively mitigate the growing threat of financial cybercrime, ensuring a secure financial environment for the nation.

Acknowledgement

The authors express their gratitude to their peers and colleagues for their valuable academic advice and helpful critiques throughout the course of this study. They also express gratitude to Qatari organizations and stakeholders for their continuous efforts to enhance the performance of small and medium-sized enterprises, which served as a source of knowledge and inspiration for our research. The authors also acknowledge the contributions of earlier scholars, whose

works on technological development, entrepreneurial orientation, and knowledge management served as the theoretical basis for the current investigation.

References

Al Bloushi, M. (2020). Cyber-attacks and data integrity concerns cripple large parts of the internet on banking (master's thesis, The British University in Dubai). The British University in Dubai Repository

Alghamdi, M. I. (2020). A descriptive study on the impact of cybercrime and possible measures to curtail its spread worldwide. International Journal of Engineering Research and Technology, 9(5), 731–735.

AllahRakha, N. (2024). Transformation of Crimes (Cybercrimes) in the Digital Age. International Journal of Law and Policy, 2(2).

Allahrakha, N. (2023). Balancing cyber-security and privacy: legal and ethical considerations in the Digital Age. Legal Issues in the Digital Age, (2), 78-121.

Albenjasim, S. (2024). Development of Cybersecurity Framework for FinTech: Bahrain as a Case Study (Doctoral dissertation).

Aljassmi, M., Gamal, A. A. M., Abdul Jalil, N., David, J., & Viswanathan, K. K. (2024). Estimating the magnitude of money laundering in the United Arab Emirates (UAE): evidence from the currency demand approach (CDA). Journal of Money Laundering Control, 27(2), 332-347.

Al-Tawil, T. N. E. (2024). Money laundering: effectiveness of the corporate social responsibility (CSR) law in the UAE. Journal of Financial Crime, 31(5), 1126-1139.

Al-Tawil, T. N. E. (2023). Anti-money laundering regulation of cryptocurrency: UAE and global approaches. Journal of Money Laundering Control, 26(6), 1150-1164.

Apel, R. (2013). Deterrence theory and the changing landscape of crime. Crime and Justice, 42(1), 109-178.

Cresswell, J. (2013). Qualitative inquiry & research design: Choosing among five approaches.

Crupi, A., & Schilirò, D. (2023). The UAE Economy and the Path to Diversification and Innovation. International Journal Of Business Management And Economic Research, 2286-2300.

Cong, L. W., Grauer, K., Rabetti, D., & Updegrave, H. (2023). Blockchain forensics and crypto-related cybercrimes. Available at SSRN 4358561.

Goni, O., Ali, M. H., Showrov, M. M. A., & Shameem, M. A. (2022). The basic concept of cybercrime. Journal of Technology Innovations and Energy, 1(2), 16-24.

Graham, A. (2023). Cybercrime: Traditional Problems and Modern Solutions (Doctoral dissertation, Open Access Te Herenga Waka-Victoria University of Wellington

Girasa, R. (2018). Regulation of cryptocurrencies and blockchain technologies. National and International Perspectives. Suiza: Palgrave Macmillan

Hussein, S., & Mohammed, S. (2024, February). Analyzing the Legal Framework and Implications of Federal Decree-Law No. 34/2021 in Combatting Cyber Blackmail in the UAE. In 2024 2nd International Conference on Cyber Resilience (ICCR) (pp. 1-6). IEEE.

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. Arabian Journal for Science and Engineering, 45, 3171-3189.

Kanso, H. (2023, May). The origins of UAE: From tribes to federation. ResearchGate. https://www.researchgate.net/publication/371469649

Maghaireh, A. M. (2024). Legislative Responses to Cyberbullying in the UAE: An Examination of the Effectiveness of Two Federal Decrees. Arab Law Quarterly, 1(aop), 1-24.

Morgan, G. A., Warren-Smith, C., & Kelly, R. (2020). The United Arab Emirates. Corporate Investigations, 2021, 132.

Modi, V. (2023). The Regulatory Landscape of Cryptocurrencies Comprehensive Overview. Jus Corpus LJ, 4, 781.

Murrar, F., & Barakat, K. (2021). Role of FATF in spearheading AML and CFT. Journal of Money Laundering Control, 24(1), 77-90.

Mwita, K. (2022). Factors influencing data saturation in qualitative studies. Available at SSRN 4889752.

Nagin, D. S. (2013). Deterrence in the Twenty-First Century. Crime and Justice, 42(1), 199-263.

Naheem, M. A. (2023). Presenting a legal and regulatory analysis of the United Arab Emirates' past, present, and future legislation combating money laundering (ML) and terrorist financing (TF). Journal of Money Laundering Control, 26(2), 253-267.

Nakamoto, S., & Bitcoin, A. (2008). A peer-to-peer electronic cash system. Bitcoin. –URL: https://bitcoin. Org/bitcoin. pdf, 4(2), 15

Nicholls, J., Kuppa, A., & Le-Khac, N. A. (2021). Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. Ieee Access, 9, 163965-163986.

Piquero, A. R., & Jennings, W. G. (2017). Deterrence and criminal justice: A review of the empirical literature. Criminal Justice and Behavior, 44(8), 1116-1142.

Shaffer, Y. (2024). The FATF criminalization of money laundering–much room for improvement. Journal of Money Laundering Control, 27(2), 225-227.

Shukurov, E., & Jafarov, U. U. (2023). Legal Professionals' Perspectives on the Challenges of Cybercrime Legislation Enforcement. Interdisciplinary Studies in Society, Law, and Politics, 2(4), 25-31.

Sultan, N., & Mohamed, N. (2023). The role of information sharing in combating money laundering: the importance and challenges of mutual legal assistance for developing jurisdictions like Pakistan. Journal of Money Laundering Control, 26(6), 1242-1260.

Świątkowska, J. (2020). Tackling cybercrime to unleash developing countries' digital potential. Pathways for Prosperity Commission Background Paper Series, 33, 2020-01.

Teichmann, F. M. J., & Wittmann, C. (2023). Money laundering in the United Arab Emirates: the risks and the reality. Journal of Money Laundering Control, 26(4), 709-718.

Tubaishat, A., & AlAleeli, H. (2024). A Framework to Prevent Cybercrime in the UAE. Procedia Computer Science, 238, 558-565.

Watts, G., & Wallman, M. (2024). The UAE Legal and Regulatory Landscape: A Perspective from Practice. In International Trade with the Middle East and North Africa (pp. 104-122). Routledge.

Wall, D. S. (2021). Cybercrime is a transnational organized criminal activity. In Routledge Handbook of transnational organized crime (pp. 318-336). Routledge.

Worldometer, (2025) UAE Population Retrieved from https://www.worldometers.info/world-population/united-arab-emirates-population/