Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE)

Hassan Younies
School of Management, New York Institute of Technology – Abu Dhabi Campus, Abu Dhabi, United Arab Emirates, and

Tareq Na'el Al-Tawil
College of Business, Zayed University – Abu Dhabi Campus, Abu Dhabi, United Arab Emirates

Abstract

Purpose – The purpose of this paper is to explore the extent to which cybercrime laws protect citizens and businesses in the United Arab Emirates (UAE). Pertinent questions over the lax regulatory environment and incomprehensible cybersecurity policies have influenced the discussions.

Design/methodology/approach – This paper will first offer a global outlook of cybersecurity laws and legislation. The global outlook will present the basis for examining best practices that the UAE could emulate. The paper will then examine the legislative landscape of cyber laws in the UAE, including cross-country comparisons. The comparisons are critical, as the country's cybercrime laws are in their infancy phase.

Findings – The UAE has taken decisive and proactive measures to deter the threat of cybercrimes and cyberattacks. The UAE strategy comprehensive strategy has been effective in protecting the economy and populations from the adverse effects of cybercrimes. The success lies in the enactment of comprehensive and streamlines laws and regulations with harsher penalties. The stringent legal measures, including longer jail terms, stiffer fines and deportation of foreigners, have ensured robust deterrence to cybercriminals.

Originality/value – The analysis has shown that the UAE has a higher score of preparedness against cybercrimes and cyberattacks. The UAE has specifically crafted a broader and effective legislative framework of cybercrime laws. Although the UAE has comprehensive cybercrime laws, the remarkable level of technological advances in the country makes citizens and businesses lucrative targets. The UAE now has the burden of doubling down its legal efforts to deter emerging cybersecurity risks.

Keywords UAE, Cyber-crimes law, Cyberbullying, Social media

Paper type Research paper

1. Introduction

The current pace of modern information and communication technology has had a profound effect on the lives of people. Technology has now become an integral part of human living. Businesses have also taken advantage of technology to drive innovation and competitiveness. Nonetheless, unprecedented technological advances have also paralleled growing concerns over cybercrimes (Farooqui, 2019). Despite their benefits, information and communication technologies have exposed both individuals and businesses to the increased risk of cybercrime. For example, the past decade has seen a significant increase in the number of international and reputable firms that have experienced data breaches and losses (Fiona, 2017). Increasing cases of hacking and phishing have not only led to massive

Journal of Financial Crime
Vol. 27 No. 4, 2020
pp. 1089-1105

1359-0790
DOI 10.1108/JFC-04-2020-0055

financial losses but also they have tainted the reputation of companies (Marco, 2012). On the other hand, global citizens have lost their identities and financial information to hackers and cybercriminals (Marco, 2012). The rising threat of cybercrime has influenced the enactment of stringed laws and regulations to protect both individuals and businesses.

The United Arab Emirates (UAE) is one of the countries in the Middle East and North Africa (MENA) region where financial and cybercrimes are major threats to national security. The most common crimes include fraud, identity theft, hacking, money laundering and theft of both financial assets and data. A major concern is that the UAE is a leading jurisdiction for money laundering (El-Guindy, 2020). The UAE has undergone massive economic transformations that have elevated the country into a global business center and financial hub. The remarkable evolution of the financial sector is a significant economic indicator for the country, but it has exposed the UAE to security threats [1]. For example, terrorist organizations and cybercriminals are using formal and informal channels in the UAE to launder money. Money laundering has subsequently exposed the country's financial sector to the risk of crime in the digital era (El-Guindy, 2014). A notable finding is that criminals and terror groups perpetrating money laundering conduct their activities outside the country. The latter assertion exemplifies the susceptibility of the country to cyberattacks and other forms of internet-based crimes.

The UAE is a unique case considering that it is the leading economy in the Gulf and global financial hub. The status of major world business and the financial center has attracted many multinational companies to the UAE (Farooqui, 2019). The country also has advanced insurance and real estate sectors in both the region and globally. Specifically, the rapid growth of the financial, real estate and insurance sectors in Abu Dhabi and Dubai have made the UAE a highly competitive and attractive to foreign companies and businesses [2]. Sophisticated technological innovations and offerings are the defining characteristics of the three sectors. Nonetheless, the level and scope of technological advances have coincided with increased susceptibility to cyberattacks and cybercrimes. The UAE Government has responded to the rising concerns over cyberattacks with the enactment of laws and policies. The purpose of the laws is to safeguard individuals and businesses from both overt and covert cybercrimes [3]. Nevertheless, pertinent questions have been raised over the effectiveness of the current laws and policies in protecting individuals and businesses.

The purpose of this paper is to explore the extent to which cybercrime laws protect citizens and businesses in the UAE. Pertinent questions over the lax regulatory environment and incomprehensible cybersecurity policies have influenced the discussions. Section 1 of the paper will review the prevalence of cyber threats in the UAE, regionally and globally. The country cannot address cyber threats unless the authorities understand the magnitude of the problem. Section 2 will offer a global outlook of cybersecurity laws and legislation. The global outlook will present the basis for examining best practices that the UAE could emulate. Section 3 will examine the legislative landscape of cyber laws in the UAE, including cross-country comparisons. The comparisons are critical, as the country's cybercrime laws are in their infancy phase. Section 4 will focus on the implications of the cyber security laws on both individuals and nosiness entities, with emphasis on the safety of citizens and individuals. The aim of the fourth section is to find out if the current laws and policies are effective considering that they are either poorly drafted or under-drafted. Finally, Section 5 will present recommendations for policy changes and best practices based on the findings from the second section.

2. Background and the scope of cyber threats

The era of big data, automation and internet of things (IoT) has led to the intertwining of the global society with the internet. Although technology has greater benefits for humanity, it

has also brought with in significant threats. The very nature of opportunities presented by technological advances has also paralleled with increasing cases of cybercrimes, cyberattacks and industrial espionage (El-Guindy, 2014). Cases of million passwords and usernames leaking on the internet have become too common in the modern world. Millions of people across the world are also losing private data and financial investments to hackers and cyber criminals. Both cases exemplify the lack of cybersecurity for computer systems and processes (McKinsey and Co., 2020). Cyber threats are among the leading risks in the world today. Cybercrime has now become the biggest threat to every individual and company. Specifically, the World Economic Forum's Global Risk Report ranked massive data fraud and fraud as fourth and cyberattacks as the fifth global risks in 2019 (El-Guindy, 2014). The number of cases and financial losses reflect the impact of cybercrime on society.

Furthermore, Grant Thornton UAE has projected that cybercrime will cost the global economy $6tn annually by 2021 (El-Guindy, 2014). The financial cost is double the $3tn recorded in 2015 (McKinsey and Co., 2020). Consequently, cybercrime now ranks among the top four economic crimes in the global level. A string of statistics based on current incidents in the USA shows how cyber-attacks have increased in size, cost and sophistication. For example, a major data breach that the Marriot reported in the past quarter of 2018 affected 500 million user accounts (Symantec, 2020). The USA also reported large-scale cyberattacks in 2017, which were more costly and complex than those of the past years. Notably, the Yahoo hack and the Equifax breach affected 3 million user accounts and 145.5 million customers, respectively (Symantec, 2020). The dramatic rise in financial costs related to cybercrimes paints a gloomy picture about the future. A major concern is that individuals have chosen complacency and many companies are unprepared despite the current hype in the media surrounding cybercrime. A worrying trend is that companies will be victims of a ransomware attack every 11 s by 2021 (McKinsey and Co., 2020).

Global penetration of the internet, coupled with the rising number of internet users, has led to an exponential increase in opportunities for cybercrime. Although cybercrime is a global threat, the Middle East has evolved to become a hotbed of cyberattacks. The Middle East has a remarkably complex ecosystem of cyber threats because of rapid digitization [4]. Cybercrime and incidents of data theft have traditionally been a reserve of developed nations until recently. However, countries in the Middle East are now reporting increasing cases of cyber threats as the scale of digitization in both governance and business continues to rise [5]. For example, the 2014 Microsoft Security Intelligence Report showed that the Middle East had the highest number of computers infected by malware and viruses compared to the global average [6]. The Arab Spring of 2011 offers a clear picture of the scope of digitization in the Middle East. Digital markets in the Middle East have expanded by 12%, which is the overall compound growth per annum (Symantec, 2020). The growth is expected to create 4.4 million new jobs and add as much as $820bn to the region's gross domestic product by 2020 [7].

Increased digitization and internet penetration have exposed the Middle East to cybercrime, cyberattacks, cyberterrorism, digital espionage and malware. A combination of factors has increased the vulnerability of Middle East countries to cyberthreats. First, many information communication technology (ICT) users in the region, including companies and organizations, lack awareness about cybersecurity, which has exposed them to greater risks. Second, the region has a shortage of technical skills and capabilities to defend their systems from cyberthreats. Third, inadequate or non-existent laws and regulations has exposed individuals and companies to cyberthreats [8]. The problem is pervasive in the banking sector, which has experienced the highest cases of cybercrimes in the Middle East. Banks in the Middle East trail their international counterparts in the development and

implementation of data-security measures for their ICT systems [9]. Although financial institutions are striving to ensure that their policies and procedures meet international standards, the implementation is currently weak. The wave of ransomware attacks that rocked the Middle East in 2017 exemplifies how increased digitization leads to increased vulnerability (Symantec, 2020).

The UAE is a leading country in the Middle East with large-scale digitization in both private and government operations. For example, the UAE is one of the top countries with more than 100% adoption rates for smartphones (Farooqui, 2019). Furthermore, the country has more than 70% social media us [10]. The penetration of smartphones and social media use in the UAE are higher than the rates in the USA. According to the 2016 McKinsey report, the UAE had the highest rates of digitization at the government, business and individual levels (Symantec, 2020). The UAE also ranks first among countries in the region in terms of expanded broadband access and digital adoption rates (McKinsey and Co., 2020). The newly-unified smart city enshrined in the UAE Vision 2021 illustrates how the development and adoption of advanced technologies is a national priority for the country. Conversely, increased digitization is a major worry in the UAE. The UAE experiences a wave of ransomware attacks in 2017, which epitomize the vulnerability that have come with increased digitization [11]. A key question is whether the UAE Government is well equipped to combat the growing risk of cybercrimes.

The UAE has experienced cyber threats that must be uncovered and mitigated with comprehensive laws and regulations. For example, the UAE was among the top 10 countries where 1.9% of users suffered a malware attack in the third quarter of 2018, based on Kaspersky Lab's Malware Reports. Furthermore, Dark Matter, a UAE-based technology firm, reported that the country encounters 5% of all cyberattacks recorded across the world in 2017 (McKinsey and Co., 2020). According to Dark Matter, the cyberattacks increased by 55% over the past five years [12]. The Dark Matter has also reported that the UAE was eighth globally by the percentage of individuals attacked by baking trojans in 2016 (Salama, 2016) [13]. The risk of banking Trojans is higher in the UAE because of the high number of smartphone users. On the other hand, financial costs related to cybercrimes increased from $1.3m in 2015 to $1.4m in 2016 [14]. The 4.9% in financial costs implies that the UAE has now become a key target for cybercriminals because of increased penetration of smartphones, popularity of the country internationally and increased digitization.

The scale of human attack surface highlights the link between demographics and the risk of cybercrime in the UAE. Current projection have shown that 65.9% of people in the UAE have a median age of 33.5 years [15]. Like in many other countries, millennials are the primary drivers of digitization in the UAE [16]. Although millennials have facilitated the country's digital transformation, they have also increased significantly the size of the population vulnerable to cybercrime in the UAE. For example, Symantec has shown that the total number of UAE users affected by cybercrime increased from 2.5 million people in 2016 to 3.72 million in 2017 (McKinsey and Co., 2020). The increase means that more than 50% of people in the UAE experienced cybercrime in 2017 [17]. Therefore, the large cohort of millennials may be driving digital transformation in the UAE, but it has also increased the country's cybercrime profile. For instance, the Norton Cyber Security Insights Report has shown that millennials report the highest incidents of cybercrimes than any other age group in the UAE [18]. According to the report, millennials in the UAE and across the world have a single password for all their accounts and they have shared their passwords with at least one other person (Symantec, 2020).

Phishing is the most common form of cyberattack in the UAE and the gulf region. The 2016 Symantec report ranked the UAE tenth globally by the number of emails labelled as

phishing (Sami, 2017). The report also ranked the country seventh globally by the number of malicious emails [19]. Higher penetration of broadband and fierce competition among providers are defining characteristics of the UAE's digital sector. The two features have led to a significant reduction in broadband prices, subsequently increasing adoption rates [20]. Expanded broadband coverage also has a downside for businesses and citizens. For instance, the widespread adoption of digital technologies and services, including smartphones, email communication and online banking have exposed individuals to online scams and phishing. Additionally, complacent behaviour, unfounded confidence and poor cyber hygiene also expose individuals to cyberthreats (Hudson, 2016). Noteworthy examples include using the same password for multiple accounts and sharing passwords with other people. The increasing risk of cybercrimes in the UAE has influenced government action in the form of policies and regulations.

3. Legislative landscape of cyber laws in the United Arab Emirates

The position of the UAE in the global economy offers the background for the legislative landscape in the country. The UAE has been in the race to become the leading smart nation internationally. Notably, Abu Dhabi and Dubai are among the top 10 smartest cities in the world. Vision 2021 is UAE's national agenda that exemplifies the country's commitment to becoming one of the world's innovative/smart cities (Sami, 2017; Salama, 2016). The two emirates renowned for deploying sophisticated disruptive technologies to enhance innovation and digital connectivity. The UAE has made significant strides in transforming itself into a global digital country. Conversely, the frequency and risk of cyber threats have increased drastically with the country's technological revolution (Chandra *et al.*, 2020). The problem with the rapid transformation is that many stakeholders in the UAE have inadequate cybersecurity practices. Thus, the possibility that the UAE is a strong target for cyberattacks has influenced a raft of legislative measures and strategies (Sami, 2017). The primary goal of the evolving laws is to make the UAE a cyber-resilient country in the region and internationally.

Cyberattacks on UAE's Government agencies and financial institutions in 2012, 2013 and 2014 brought cybersecurity to the forefront of the country's policy. The UAE has developed a National Cybersecurity Strategy aimed at preventing cybercrimes in the wake of expanding digitization initiatives and smart city projects. The UAE is particularly set to double spending on national security to more than $10bn by 2024 (Telecommunications Regulatory Authority (TRA), 2019). A large proportion of the spending is earmarked for strengthening the country's cybersecurity efforts. The UAE made a significant milestone in its cybersecurity preparedness when the National Electronic Security Authority (NESA) released the national cyber strategy in 2014. The national strategy has outlined policies and standards to ensure that the country is adequately prepared to counter cybercrimes and cyberthreats. The UAE Information Assurance Standards and the Critical Information Infrastructure Policy are key policies outlined in the national strategy [21]. The UAE also has a cyber incident report team or the UAE Computer Emergency Response Team (aeCERT), which is an official and nationally recognized initiative.

The UAE created aeCERT as its national Computer Emergency Response Team (CERT). The UAE Telecommunications Regulatory Authority (TRA) operates the aeCERT. The primary mandate of aeCERT is to regulate the country's telecommunications and information sector. The asCERT also plays a critical role in detecting, preventing and responding to cybersecurity incidents. The aeCERT also has a dedicated website for creating awareness; transmitting advice and information; and receive alerts from users [22]. The aeCERT is the first contact for individuals, government agencies and companies that

have experienced cyber incidents. The aeCERT employs a proactive approach to protecting the vulnerable systems (Hudson, 2016) [23]. The team also collaborates with law enforcement agencies and multiple government entities to design methodologies and policies that counter cyber threats. The UAE national aeCERT also shares data and collaboration with CERTS of other countries across the globe. Collaboration and information sharing offer the CERTS valuable opportunities to advance information and cyber security (Sami, 2017).

The UAE has acknowledged the vital role that a well-defined legal structure plays in ensuring that companies, government agencies and citizens operate in safe cyberspaces. Consequently, the federal government has developed many initiatives to enhance cybersecurity preparedness and response. For example, the UAE premier launched the Dubai Cybersecurity Strategy in 2017 to strengthen the global perception and defences of the financial capital [24]. The data wealth initiative is another strategy that Dubai has implemented to protect consumer and government data. Dubai has also adopted a multipronged innovation strategy that transforming Dubai into a smart city and expanding the penetration of IoT (McKinsey and Co., 2020). Although the innovation strategy for Dubai is unproblematic, expanded access to IoTs makes the government, businesses and citizens highly vulnerable to cybercrime. These concerns are now shaping the evolving cybersecurity legislative framework in the UAE (McKinsey and Co., 2020). A combination of the national strategy and evolving laws have put the UAE ahead in cybersecurity preparedness in the region.

Laws and regulations play an instrumental role in protecting critical national and public interests. The UAE did not have a definite regulatory framework until 2006 that the UAE federal government formulated a national law to address cybercrime. Federal Law No. (2) on the prevention of information technology crimes was enacted in 2006 at a time when the world was recognized the value of national laws to combat cybercrimes. The purpose of the 2006 law was to regulate the telecommunication sector, in addition to deterring crimes associated with information technology systems as much as possible (Chandra *et al.*, 2020). For example, article two, three and four covered violation of the rules and regulations, including the penalties that come with the legal omissions and illegal acts. Furthermore, the law also covered cybercrimes related to the distortion of medical records, diagnoses and treatment. Other critical issues incorporated in the law included cyberbullying, cyberterrorism, financial fraud, impersonification and other internet-related crimes [25]. The 2006 set the precedence for UAE's cybersecurity legal framework by setting clear boundaries for internet use.

The UAE Government bolstered its commitment to fighting cybercrimes and e-security with the introduction of two new laws. First, the federal government repealed the 2006 law in 2012 with the UAE-Law No. (5) of 2012 on combating of information technology crimes or the Cyber Crimes Law. Second, the government also enacted Law No. 3 of 2012 on Establishing the NESA (E-Security Authority Law) (O'Connell, 2013). The government repealed Law No. 2 of 2006 and introduced a new law after the remarkable increase of online financial transactions and social media use coincided with a surge in cybercrimes. The Cyber Crimes Law analyses multiple scenarios involving cybercrimes and how they will likely occur [26]. One feature of the Cyber Crime Law is that it introduced a broad range of offences than the 2006 law. Notable examples include using IT systems for phishing and hacking; forging electronic records; disabling access to an information network; and damaging or amending electronic information. The Cyber Crimes Law also criminalizes unauthorized disclosure of electronically protected information [27].

The Cyber Crimes Law has allowed the UAE to bridge the gap between online and offline offences. For example, the emergence of cyberterrorism has presented new challenges to national security. The UAE enacted the media Law No. 15 of 1980 on printed natter and publications. However, the UAE Media Law did not cover online threats to national security. Thus, the Cyber Crimes Law updated the Media Law to include online activities (Hudson, 2016). On the other hand, the Cyber Crimes Law has adopted stringent jail terms and monetary penalties. Notably, some offences now carry an imprisonment term of up to 10 years and a fine of AED 3m [28]. The law has also expanded the jurisdiction and power of the courts to apply punitive sentences, including confiscation of devices, closure of illegal websites and deportation of foreigners involved in cybercrimes (Agarib, 2018). The dynamic nature of cybercrimes and attacks underscores the essence of revising and update existing laws. The UAE has acknowledged the inadequacies of the 2012 law in dealing with new cyber threats by amending it in 2018.

The UAE Government repealed the Cyber Crimes Law into the Cybercrime New Amendment Law. The UAE President signed into law the Cybercrime New Amendment Number 2 of 2018. The new law amended sanctions under Articles 26, 28 and 42. Effectively, the Cybercrime New Amendment, which was published on 13 August 2018, has increased the range of sanctions imposed on violators. The amended law has also introduced new measures that include restrictions and probation on the use of electronic mediums, obligatory deportations and other punitive/hefty sanctions [29]. The Cybercrime New Amendment broadened the scope of incidents involving serious electronic crimes. The 2012 law included significant sanctions for cybercrimes that could potentially support or promote terrorism organizations and activities, as well as undermine public safety. The Cybercrime New Amendment has elaborated cybercrimes by emphasizing the negative effects that the misuse of social media, websites and other online platforms could have on national security, social stability and cohesion among persons from diverse backgrounds (Hudson, 2017; Debusmann, 2017).

Second, the country also developed a National E-Security Authority (the Authority) under Law No. 3 of 2012. The government created the authority to augment the Cyber Crimes Law. The expressed responsibilities and goals of the authority are as follows, "to organize protection for the communication network and information systems in the state and develop, amend and use the necessary methods in Electronic Security domain" [30]. Another stated responsibility of the Authority is to support both the federal and Emirate-level government agencies. The e-security ambit of the Authority also extends its mandate to the private sector. The authority also coordinates with relevant bodies, particularly TRA and aeCERT, to pursue its goals and responsibilities (Fiona, 2017). As such, both the Cyber Crimes Law and the authority have established a strong foundation and guidelines to manage the growing burden of cybercrimes in the UAE and across the region. The two laws have specifically strengthened the legal framework by complementing other e-security initiatives of the UAE, including aeCERT and public awareness campaigns (O'Connell, 2013).

The UAE has also shown commitment to protecting people and businesses from cybercrimes and cyberthreats by enacting diverse regulations and cybersecurity strategies. First, the TRA introduced the consumer protection regulations (The CPR) of 2017 to govern the operations of telecommunications service providers (TSPs). The law mandates the TSPs to outsource services from only vendors who have adopted the right and reasonable technical, cyber and organizational measures that protect the security and confidentiality of subscriber information. Subscriber information include the name, address, payment history, bank or credit card details and credit rating (Salama, 2016). The CPR also mandates TSPs to

"take all reasonable and appropriate measures to prevent the unauthorized disclosure or the unauthorized use of subscriber information" and "all reasonable measures to protect the privacy of subscriber information that it maintains in its files, whether electronic or paper form" (Fiona, 2017). The TSPs should also use "reliable security measures" when handling subscriber information. A combination of these provisions has created the framework for reducing the vulnerability of people and businesses to cyberattacks.

Second, the UAE Central Bank issued the Federal Regulatory Framework for Stored Values and Electronic Payment Systems of 2017 (The Framework or the Federal Regulations of 2017) to regulate how service providers using digital payments process and store the information of their users, including personal data. Service providers must store all data related to user identification and transaction records within the UAE. Service providers must also follow restrictions about when and with whom to share the stored data. The framework also requires the service providers to use cyber, technical, organizational and operational methods to ensure the confidentiality of user information and transaction data [31]. Similarly, the Federal Law on Information and Communication Technology in the Health Field of 2019 (Federal Law No. 2 of 2019) or the Health Data Law applies to healthcare providers and related services operating in the UAE and the free zones. Covered entities processing electronic health data must protect the information from unauthorized amendment, damage, alteration, addition or deletion. The failure to implement cybersecurity measures attracts sanctions and fines for noncomplying health service providers within each health authority (Salama, 2016).

4. Effects of cybercrime laws on businesses and individuals

A pertinent question is whether the comprehensive UAE legal framework is effective in protecting government agencies, businesses and citizens. Unprecedented cyberattacks on the UAE Government agencies and financial institutions were instrumental in shaping the current legislative landscape. The UAE has stringent cybersecurity laws with hefty fines and punitive jail terms. For example, the minimum jail term for offenders is five years, with a maximum fine of AED 3m. Additionally, foreigners incarcerated for engaging in cyberattacks are deported once they complete serving their sentences (Debusmann, 2017). A key argument is that the UAE has remained unscathed in the wake of massive cybercrimes and attacks across the globe. Thus, a pertinent question is whether the punitive nature of the UAE cyber laws has contributed to the low cases of cyberattacks, as the enactment of the 2012 law. The answer to the question is critical to assess the strength and vulnerability of the UAE to cyberattacks as it increasingly moves transitions to a smart city by 2021. This section will explore the effectiveness of the UAE cyber laws on both businesses and individuals.

The UAE has adopted multiple laws and regulations to combat the rising wave of cybercrimes in the Middle East. The New Cyber Crime Law of 2012 has stood out as the blueprint for UAE's cybersecurity. The 2012 law has been a landmark legislative framework because of its comprehensive approach to cybersecurity. Specifically, the law has incorporated provisions that cover up to 16 categories of cybercrimes (Debusmann, 2017). The effectiveness of the 2012 law can be understood from the perspective of the evolving nature of cybercrimes. Illegal access to electronic data through phishing and hacking constituted the primary act of cybercrime. However, many forms of cybercrimes have evolved in the era of advanced information and communication technology. Therefore, it is counterproductive to focus solely on legislating access to electronic media while ignoring other serious cybercrimes. For example, the intensity and severity of defamation, sectarianism, religious intolerance, human trafficking, terrorism and money laundering

have significantly increased in the digital era. The changing landscape of cybersecurity underscores the need of developing comprehensive laws, like in the case of the 2012 New Cyber Crime Law [32].

Moreover, the New Cyber Crime law has been effective because of the punitive fines and jail terms. The UAE Government argued that stringent legal provisions would enhance deterrence. For example, the Federal Law No. 2 of 2006 criminalized the willful act of accessing illegally an electronic site. Conversely, Article 2 of the 2012 law removed the intent requirement by prohibiting illegal access of an electronic site without permission or by exceeding the permitted boundaries. The New Cyber Crime Law of 2012 increased the penalty for copying, changing, disclosing, deleting or publishing information gained from accessing an electronic site without permission or illegally. Imprisonment for the crime has increased from not less than six months to a minimum of one year or a minimum fine of AED 250,000 (from AED 150,000) to a maximum of AED 1m (from AED 750,000). Longer sentences and stiffer financial penalties, including deportation of convicted foreigners, have attributed to the minimal cases of cybercrimes in the UAE (Aboul-Enein, 2018).

Has the enactment of stringent and harsher penalties protected individuals, government agencies and businesses from cyberthreats and cybercrimes? The answer to this question lies in assessing cybersecurity incidents and risks reported in the UAE. Data from the analysis will be instrumental in evaluating the effectiveness of the current laws in protecting citizens and businesses. The findings will also inform evidence-based policies and best practices for the future. The Fitch Solutions Group Limited publishes the UAE Crime and Security Risk Report quarterly. The report includes key statistics on security risks for both the UAE and the region. Findings from the report have shown that the UAE has the lowest rates of crime in the MENA region (Table 1), which makes it appealing to investments regionally. However, the increasing number of poor-paid immigrant workers poses some security risks to the country.

Despite the security risk, the UAE's police force has strong capabilities, with harsher punishments for violators, which offer a significant deterrent. Thus, the UAE has a high score of 86.4/100% for the vulnerability to crime risk [33]. The ranking places the UAE second after Qatar among 18 countries in the MENA region (Figure 1).

Low rates of crime in the UAE have not shielded the country from the invisible hand of cybercrime and cyberattacks. Cyberattacks and financial crimes are the leading security risks facing businesses in the UAE. Common cybercrime vulnerabilities in the UAE include money laundering, identity theft, fraud, hacking and theft of financial assets and data. High penetration of internet broadband has increased the vulnerability of the country to cybercrimes. Findings from the Fitch report have shown that the UAE has a higher risk of cybercrime despite having the best cybersecurity levels and high-capacity law enforcement agencies in the MENA region. The UAE has a business crime risk of 33/100% of which 50%

	Conflict risk	Vulnerability to crime	Business crime	Crime and security risk
UAE score	49.9	86.4	75.1	70.5
MENA average	29.4	53.3	43.6	42.1
MENA position (out of 18)	3	2	1	1
Global average	48.9	49.8	49.0	49.2
Global position (out of 201)	101	15	33	33

Notes: 100 = lowest risk; 0 = highest risk
Source: Fitch Solutions Crime and Security Risk Index

Table 1.
UAE-crime and security risk

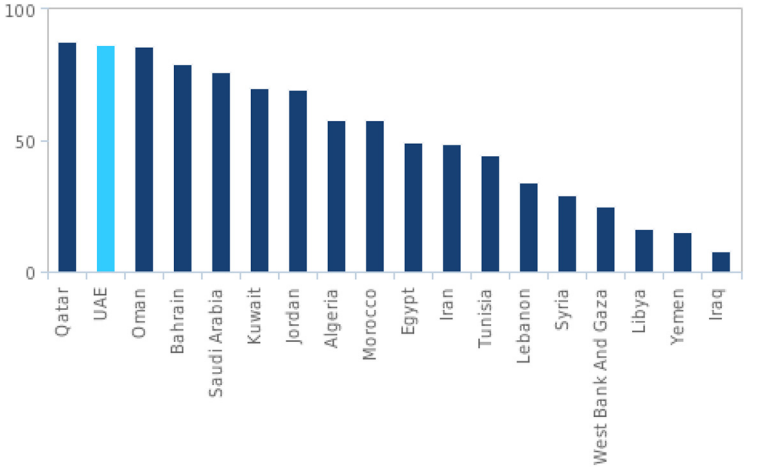

Figure 1.
MENA – vulnerability to crime scores

accounts for financial crime and cybercrime and the remaining 50% for business cost of crime [34]. The high business crime risk implies that the current cyber laws have loopholes that could expose individuals and businesses to cyberthreats. Conversely, high business risk does not necessarily mean that the current laws are ineffective. On the contrary, businesses, employees and citizens are susceptible to cyberthreats and risks because of their ambivalence attitude related to knowledge deficits [35].

A significant contribution of the 2012 New Cyber Crime Law was that it codified the broad range of cybercrimes that individuals and groups can commit, as well as the corresponding penalties. However, the ever-changing scope of cybercrimes and cyberattacks underscores the significance of having a broad combination of laws. The enactment of the Cybercrime New Amendment of 2018 illustrated the government's commitment to protecting both citizens and businesses in the era of advancing information and communication technologies (Salama, 2016). The exponential growth of social media in both the UAE and globally has created new channels for cybercrimes, especially cyberbullying. Thus, cybercrime is no longer about hacking, phishing and other related crimes. On the contrary, individuals and organizations are increasingly using the internet to slander and bully others for either personal vendetta or financial gain. The new forms of cybercrimes have challenged governments to update and develop new policies. The UAE has taken a leading role in ensuring that its legal framework covers all forms of cyberthreats to assure the safety of both businesses and citizens (Rajan *et al.*, 2017).

The effectiveness of the UAE laws can be evaluated by examining the legislative measures that the government has adopted, as the enactment of the 2012 New Cyber Crime Law. As mentioned, social media and emerging technologies have influenced the evolution of new forms of cybercrimes. As such, it is of the essence to examine how the UAE is responding to these changes. Online bullying is one of the cybercrimes with far-reaching implications on the public and businesses. The situation is worse considering the number of children being exposed to online bullying, including pornography and human trafficking (James, 2019). The UAE has assumed a leading role in addressing the emerging threats. A notable example is the enactment of multiple cyberbullying laws. The proliferation of technology and electronic devices across schools in the UAE has paralleled an increase in cyberbullying activities. In fact, the 2012 New Cyber Crime Law covered acts of

cyberbullying, but it is only recently that the Federal Supreme Court has applied the provisions in practice. The question now is whether the 2012 New Cyber Crime Law has robust provisions on cyberbullying (Fiona, 2017).

Article 20 of the 2012 New Cyber Crime Law is the foundation of cyberbullying regulations in the UAE. The law is relevant today in the wake of online trolling and abusive use of social media and the internet. The article deals with slander and defamation using technological devices in the broadest of terms. The punishment for offenders includes imprisonment and a minimum fine of AED 250,000 but not exceeding AED 500,000 (James, 2019). The standards applicable to defamation are high especially when the perpetrator harms the reputation of the victim in a way that places them in a negative light. Article 16 through 18 of the same law deals with cases related to the acquisition and distribution of pornographic content involving minors. The penalties are more of the same like in the case of defamation. The Cybercrime New Amendment of 2018 has both broadened the scope of the crimes and double the penalties. However, The Cybercrime New Amendment is inadequate to protect individuals from cases of cyberbullying and online trolling. The main concern is that the UAE does not have a specific law for cyberbullying (Fiona, 2017).

The UAE does not have enough legal protections for victims of online trolling and bullying. The Cybercrime New Amendment may have stringent penalties, but the law was neither drafted nor enacted to properly address the special circumstances of cyberbullying. For instance, cyberbullying is not a specific offence in the UAE. The current legal provisions have broad definitions that do not specifically deal with underage access to the internet and social media sites [36]. A major contestation is how to deal with children who misuse the internet and social media to bully and troll others. The Cybercrime New Amendment mandates lesser penalties for children although the sensitivity of the matter is a grey area in law. Like many other countries, the UAE has challenged Facebook and other social networks restrict children's access to adult content. Nevertheless, such restrictions have no legal basis because they lack legal consequences for the minors (James, 2019). A pressing concern for the UAE is how to deal with minors who breach the current restrictions. The UAE law is only harsher to adults and organizations that facilitate or condone access to criminalized content.

The introduction of the New Public Prosecution could allow the UAE to combat the evolving new forms of cybercrimes. Ministerial Resolution No. 220 of 2017 created a Federal Public Prosecution that specializes on crimes related to information technology. The specialized Public Prosecution means that the ordinary Public Prosecution offices no longer handles such cases. The Ministerial Resolution has ensured that the UAE Government is well-equipped to deal with new crimes arising from the fast-paced advances in information and communication technologies. A major advantage of the New Public Prosecution is that specialist prosecutors with background experience will respond effectively to the emerging new forms of cybercrimes. The New Public Prosecution does not in any way imply that the ordinary one was ineffective (Khodeir, 2017). On the contrary, the new office will augment and further enhance the effectiveness of the current practices with specialist resources and training. The assumption is that the specialized Public Prosecution will use its expertize and resources to inform the next wave of cyber laws in the UAE, particularly those aimed at combating the pervasiveness of online trolling and bullying for both children and adults (Rajan *et al.*, 2017).

Conversely, the comprehensiveness of the UAE cyber laws with the accompanying harsher penalties have raised fundamental concerns about free speech. The main contestation is that the UAE has adopted a draconian approach to the surveillance of online activities. The timing of the 2012 New Cyber Crime Law lays the basis for understanding the

relationship between cybersecurity and free speech. The Arab Spring uprisings and demonstrations, which started in 2011 and culminated in 2012, were historic events in the region [37]. The critical role that social media networks played in political activism and mobilization renewed efforts to stemming dissent voices. A critical issue is whether the UAE cyber laws are an affront to free speech. Aggrieved parties often articles that fall under defamation; sedition, sectarianism and harming national interests; state security; and promoting demonstrations without a license (James, 2019). Opponents of the cybercrime law, especially international organizations, usually cite the articles to prove that the UAE is intolerant to free speech. Nevertheless, the UAE Government has maintained that stringent laws are necessary to prevent the misuse of the internet and social media, a justification that I support.

Although the New Cyber Crime Law of 2012 deters cybercrimes, it has inadvertently created a legal caveat for misinterpretation. For example, Articles 28, 29 and 30 under state security touch on political mobilization and free speech. Notably, Article 28 has outlawed publishing of news, information and caricatures or other drawings that could pose a national security threat. Furthermore, Article 32 criminalizes the use of electronic sites or websites to plan, organize, call or promote demonstrations without a license [38]. The cited examples illustrate the intersection of cybercrimes with human liberties. An ethical dilemma is whether the quest for cybersecurity should override the freedom of speech and expression. The UAE has enacted a broad range of laws and legal prohibitions whose primary goal is to deter security threats perpetrated through the internet. The laws have significantly evolved over the years in parallel with ongoing transformation of information and communication technologies. Nonetheless, the UAE Government's efforts of protecting citizens and businesses from cybercriminals could raise questions about human liberties.

The question of human rights and free speech brings to focus the effectiveness of the UAE cyberlaws. Proponents have argued that stricter cyberlaws are necessary to address the evolving threats of cyberbullying and trolling, an argument that I support. On the other hand, dissenting voices have asserted that the UAE Government is using the stringent laws to censor online activities. Despite the divergent views, a key issue to consider is the possible legal ambiguities of the UAE cyber laws. The point of argument is that limitations on free speech are only permissible or legitimate if an unambiguous law has prescribed them [39]. Legal clarity is critical to avoid a situation where the public unknowingly break laws because of their inherent ambiguities. Another issue to consider is the conflict between human liberties and the public good. For example, it is irresponsible for people to misuse of the internet and social media because they have a right to free speech. Deterrence is the underlying principle of laws and regulations. The UAE cyber laws may be stringent, but they have been effective in ensuring widespread deterrence against cybercriminals.

5. Recommendations for policy changes and best practices

The UAE should be ready to absorb a disproportionate burden of cyberthreats considering the unprecedented levels of technological innovations in the country. Enhanced digitization and connectivity have made the UAE an allure for cybercrimes. The UAE is particularly vulnerable because of being a regional and global leader of digitization, as well as a global financial and cultural center/hub. The analysis has shown that the UAE has a higher score of preparedness against cybercrimes and cyberattacks. The UAE has specifically crafted a broader and effective legislative framework of cybercrime laws. Although the UAE has comprehensive cybercrime laws, the remarkable level of technological advances in the country makes citizens and businesses lucrative targets. The UAE now has the burden of doubling down its legal efforts to deter emerging cybersecurity risks. The greatest challenge

for the UAE is to harmonize laws between those of the UAE legislation and free zones. For example, Dubai and Abu Dhabi usually have competing and overlapping laws, which undermines their enforcement and effectiveness. Harmonization is necessary to a single, national regulatory framework.

Data protection is a key area that needs streamlined cybersecurity laws and regulations. Data protection has been a problematic issue because of fragmentation in the UAE. Specifically, the UAE lacks a specific data protection law that covers the entire country. A patchwork of laws offers some rights to privacy, in addition to criminalizing activities that lead to unauthorized disclosure of electronically-obtained data. For example, Abu Dhabi Global Market is a data protection reform unique to Abu Dhabi (Ian, 2019). The Dubai International Financial Centre has also updated its data protection law that covers its jurisdiction. Different sectors have also formulated their own data protection laws to protect the privacy and confidentiality of their clients. The fragmentation of data protection laws makes it difficult to coordinate national efforts (Rajan *et al.*, 2017). Despite the limitation, the recently launched National Cybersecurity Strategy (2020-2025) has laid the foundation for streamlining data protection laws and regulations in the UAE. The strategy is in line with Europe's General Data Protection Regulation (GDPR) (Telecommunications Regulatory Authority (TRA), 2019).

The GDPR is a mutually agreed legislation among European nations that has modernized laws that protect personal data. The modernized law has overhauled how business entities in the region process and handle data. GDPR, which was enforced on 25 May 2018, has harmonized data privacy laws on the continent. The UAE has taken the same approach through the introduction of the National Cybersecurity Strategy. The new strategy will not only streamline data protection laws but also it will allow regulatory agencies to implement easily implement the provisions across different sectors (Telecommunications Regulatory Authority (TRA), 2019). The UAE National Cybersecurity Strategy is a laudable approach because it will minimize the risk of privacy violations and data piracy. The UAE is increasingly becoming a leading digital city globally as it continues to advance its big data analytics, artificial intelligence and the Fourth Industrial Revolution. The three initiatives offer endless opportunities, but they also give hackers and phishers a gateway to cybercrime. Therefore, the National Cybersecurity Strategy implies that the UAE is well-prepared to counter the risks.

National laws and policies are insufficient to shield the UAE from cybercrimes and cyberattacks emanating from external sources. The point of argument is that cybercrimes permeates national and international boundaries. As such, it is essential for the UAE to consider regional and international cooperation. The UAE has been working closely with both the USA and other European countries to combat transnational cybersecurity threats. However, the susceptibility of the gulf region to cybersecurity risks underscores the value of regional cooperation around cyber laws. Africa and the Middle East offer convenient locations for money laundering and cybercrime because of weaker legal systems compared to those in the USA and Europe. The rationale for harmonization relates to the transnational nature of cybercrimes. For instance, criminalizing cybercrime in Country A and not doing the same in Country B makes it hard to address global cases of cybercrimes. The UAE may have sophisticated cybersecurity laws, but such regulations would be inconsequential unless countries in the region strengthen their legal frameworks. The solution lies in a regional data protection law.

TRA proposed a data protection law covering all the GCC states during the launch of the National Cybersecurity Strategy in 2018. The main issue is that developing such a law would be challenging despite being a possibility. The UAE is one of the signatory states to the Arab Convention on Combating Information Technology Offences of 2010 or the 2010 Convention. The 2010 Convention is a regional treaty that is binding for all the 22 states in the Arab League. The primary goal of the 2010 Convention is to strengthen cooperation between

the Arab League states in combating offences related to information technology. Regional cooperation is necessary considering that the Gulf region is highly vulnerable to cybercrimes and attacks. The 2010 Convention is now helping the Arab League states to protect their interests, people and property from cybercrimes. The 2010 Convention also covers unique offences that include sharing principles and ideals of terror groups; distribution of pornographic content; and diffusion of religious dissent and fanaticism. Thus, the 2010 Convention could offer the framework for developing and strengthening regional data protection laws in the wake of the new cybersecurity threats.

Formulating a regional data protection law will play an instrumental role in addressing the limitations of the 2010 Convention. Specifically, the 2010 Convention is weak, as it lacks a mechanism for direct enforcement and a dispute resolution procedure for non-implementers. Furthermore, the scope of the 2010 Convention limited to offences that are purely transnational. Furthermore, many countries have proposed a global convention that would lead to the development of an international legal instrument for combating cybercrimes under the auspice of the United Nations (UN). For example, the Russian Federation proposed a "Draft UN Convention on Cooperation in Combating Cybercrime" in 2017. Nonetheless, efforts to achieve an international consensus that would lead to the adoption of a global convention within a UN framework as still elusive (Debusmann, 2017). The absence of an internationally-binding legal framework exemplifies the urgency of either strengthening the existing regional treaties or developing new regional data protection laws. The UAE should assume a leading role in ensuring the achievement of, thus, goal because of its inherent technological capabilities and expertize.

Moreover, human rights are a valid concern for the UAE, as the country is party to both the Arab Charter on Human Rights and the UN Universal Declaration on Human Rights. The two instruments protect freedom of expression. Thus, the UAE has a legal obligation, under regional and international statues, to promote and protect the inalienable right to freedom of expression and opinion. Many GCC countries, except Bahrain and Kuwait, have not ratified the International Covenant on Civil and Political Rights (ICCPR). The core provision of the ICCPR is that countries must have a legitimate reason to justify limitations on free speech based on three aspects [40]. The first is respecting the reputation and rights of others. The second is protecting national security and public order. The third one is protecting public health or morals. However, countries should achieve the highest threshold of justification for each of the three legitimate reasons. Accordingly, efforts aimed at developing a regional data protection law should integrate provisions for ratifying the ICCPR. Domestication of the ICCPR will allow the UAE and other GCC countries to develop cybercrime laws that have legitimate limitations on free speech.

In conclusion, the UAE has taken decisive and proactive measures to deter the threat of cybercrimes and cyberattacks. The UAE strategy comprehensive strategy has been effective in protecting the economy and populations from the adverse effects of cybercrimes. The success lies in the enactment of comprehensive and streamlines laws and regulations with harsher penalties. The stringent legal measures, including longer jail terms, stiffer fines and deportation of foreigners, have ensured robust deterrence to cybercriminals. However, the structure and content of the laws undermine international cooperation. The UAE is not party to any international treaty on cybercrime. The 2010 Convention is the only regional law binding to the UAE. The problem with the 2010 Convention is that countries neither use it to fight cybercrimes nor reference it in their national laws. A combination of these issues challenges the UAE to coordinate efforts that will influence the development of effective and well-defined regulations at both the regional and international levels. Regional and international cooperation will play a fundamental role in reversing the rising trend of cyberthreats in the region.

Notes

1. Marco, Gercke. *Understanding Cybercrime*, p. 120.
2. Sameh Aboul–Enein, *Cybersecurity Challenges in the Middle East*, pp. 6-48.
3. Marco, Gercke. *Understanding Cybercrime*, p. 136.
4. Joyce, Hakmen, *Cybercrime Legislation in the GCC Countries*, p. 2.
5. Joyce, Hakmen, *Cybercrime Legislation in the GCC Countries*, p. 2.
6. Sameh Aboul-Enein, *Cybersecurity Challenges in the Middle East*, pp. 6-48.
7. Sameh Aboul-Enein, *Cybersecurity Challenges in the Middle East*, pp. 6-48.
8. Abdulla *et al.* "A Critical Analysis of the Effectiveness of Cyber Security Defenses in UAE Government Agencies" pp. 36-43.
9. Joyce, Hakmen, *Cybercrime Legislation in the GCC Countries*, p. 6.
10. Joyce, Hakmen, *Cybercrime Legislation in the GCC Countries*, p. 6.
11. Joyce, Hakmen, *Cybercrime Legislation in the GCC Countries*, p. 6.
12. Geetanjali, Chandra, Bhoopesh Kumar Sharma and Iman Ali Liaqat, "UAE's Strategy Towards Most Cyber Resilient Nation", pp. 2803-2809.
13. Geetanjali, Chandra, Bhoopesh Kumar Sharma and Iman Ali Liaqat, "UAE's Strategy Towards Most Cyber Resilient Nation", pp. 2803-2809.
14. Abdulla *et al.* "A Critical Analysis of the Effectiveness of Cyber Security Defenses in UAE Government Agencies", pp. 36-43.
15. Chandra *et al.* "UAE's Strategy Towards Most Cyber Resilient Nation", p. 2804.
16. Abdulla *et al.* "A Critical Analysis of the Effectiveness of Cyber Security Defenses in UAE Government Agencies", pp. 36-43.
17. Chandra *et al.* "UAE's Strategy Towards Most Cyber Resilient Nation", pp. 2803-2809.
18. Symantec, "Norton Cybersecurity Insights Report 2015", 20 March 2020. https://ae.norton.com/norton-cybersecurity-insights-report-uae
19. Symantec, "Norton Cybersecurity Insights Report 2015", 20 March 2020. https://ae.norton.com/norton-cybersecurity-insights-report-uae
20. Abdulla *et al.* "A Critical Analysis of the Effectiveness of Cyber Security Defenses in UAE Government Agencies", pp. 36-43.
21. Abdulla *et al.* "A Critical Analysis of the Effectiveness of Cyber Security Defenses in UAE Government Agencies", pp. 36-43.
22. Chandra *et al.* "UAE's Strategy Towards Most Cyber Resilient Nation", pp. 2803-2809.
23. Chandra *et al.* "UAE's Strategy Towards Most Cyber Resilient Nation", pp. 2803-2809.
24. Chandra *et al.* "UAE's Strategy Towards Most Cyber Resilient Nation", pp. 2803-2809.
25. Abdulla *et al.* "A Critical Analysis of the Effectiveness of Cyber Security Defenses in UAE Government Agencies", pp. 36-43.
26. Sameh Aboul-Enein, *Cybersecurity Challenges in the Middle East*, pp. 6-48.
27. Sameh Aboul-Enein, *Cybersecurity Challenges in the Middle East*, pp. 6-48.
28. Abdulla *et al.* "A Critical Analysis of the Effectiveness of Cyber Security Defenses in UAE Government Agencies", pp. 36-43.

29. Abdulla *et al.* "A Critical Analysis of the Effectiveness of Cyber Security Defenses in UAE Government Agencies", pp. 36-43; Sameh Aboul-Enein, *Cybersecurity Challenges in the Middle East*, pp. 6-48.
30. Abdulla *et al.* "A Critical Analysis of the Effectiveness of Cyber Security Defenses in UAE Government Agencies", pp. 36-43.
31. Abdulla *et al.* "A Critical Analysis of the Effectiveness of Cyber Security Defenses in UAE Government Agencies", pp. 36-43.
32. Abdulla *et al.* "A Critical Analysis of the Effectiveness of Cyber Security Defenses in UAE Government Agencies", pp. 36-43.
33. Fitch Solutions, UAE, pp. 27-33.
34. Fitch Solutions, UAE, pp. 27-33.
35. Ibid.
36. Chandra *et al.* "UAE's Strategy Towards Most Cyber Resilient Nation", pp. 2803-2809.
37. Sameh Aboul-Enein, *Cybersecurity Challenges in the Middle East*, pp. 6-48.
38. www.tamimi.com/law-update-articles/new-law-combating-information-technology-crimes
39. Sameh Aboul-Enein, *Cybersecurity Challenges in the Middle East*, pp. 6-48.
40. Joyce, Hakmen, *Cybercrime Legislation in the GCC Countries*, p. 16.

References

Aboul-Enein, S. (2018), "Deportation made optional in UAE cybercrime law", *Cybersecurity Challenges in the Middle East*, 6-48, Amira, Agarib, October 13, available at: www.khaleejtimes.com/nation/dubai/deportation-made-optional/-in-uae-cybercrimelaw

Agarib, A. (2018), "Deportation made optional in UAE cybercrime law", October 13, available at: www.khaleejtimes.com/nation/dubai/deportation-made-optional/-in-uae-cybercrimelaw

Chandra *et al.* (2020), "UAE's strategy towards most cyber resilient nation", pp. 2803-2809.

Debusmann, B. (2017), "What UAE law says about cybercrimes, penalties", *Khaleej Times*, October 1, available at: www.khaleejtimes.com/legalview/what-the-law-in-the-uaesays-about-cybercrimes-penalties

El-Guindy, M.N. (2014), "Middle East Cyber Security Threat Report 2014".

El-Guindy, M.,N. (2020), "Middle East Cyber Security Threat Report 2014," March 20, available at: www.academia.edu/5522905/Middle_East_Cyber_Security_Threat_Report_2014

Farooqui, M. (2019), "UAE to roll out new laws to combat cybercrimes", Gulf News, June 24.

Fiona, R. (2017), "Cyberbullying in the UAE: a snapshot of cyberbullying laws in the UAE", available at: www.tamimi.com/law-update-articles/cyberbullying-a-snapshotof-the-laws-in-the-uae

Hudson, A. (2016), "The fight against cybercrime", September 2016, available at: www.tamimi.com/law-update-articles/the-fight-against-cybercrime

Ian, B. (2019), "Data protection law at the heart of UAE cybersecurity strategy", September 30, available at: www.pinsentmasons.com/out-law/analysis/data-protection-law-at-the-heartof-uae-cybersecurity-strategy

James, M. (2019), "To post or not to post? The UAE, social media and the law", Arabian Business, May 2.

McKinsey and Co., (2020), "Digital middle East: transforming the region into a leading digital economy", March 2020, available at: www.mckinsey.com/~/media/mckinsey/global%20themes/middle%20east%20and%20africa/digital%20middle

Marco, G. (2012), *Understanding Cybercrime: Phenomena, Challenges, and Legal Response*, ITU Publication, London, p. 118.

O'Connell, N. (2013), "Developments in the UAE Cyber Crimes Law," May 2013, available at: www.tamimi.com/law-update-articles/developments-in-the-uae-cyber-crimes-law

Rajan, A.V., Ravikumar, R., (2017), and M.A. and Shaer, "UAE cybercrime law and Cybercrimes-Analysis", *International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, doi: 10.1109/CyberSecPODS.2017.8074858.

Salama, S. (2016), "UAE to get tough on IP address forgery", *Gulf News*, January 18, available at: https://gulfnews.com/uae/crime/uae-to-get-tough-on-ip-address-forgery-1.1655517

Sami, Z. (2017), "UAE's strategy to counter cyber terrorism can be a model for others", Gulf News, May 16.

Symantec (2020), "2017 Norton cyber security insights: the UAE", March 20, available at: www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-comparisonuae-en.pdf

Symantec (2020), "2016 Norton cyber security insights: the UAE", March 20, available at: www.symantec.com/content/dam/symantec/docs/reports/2016-norton-cyber-securityinsights-comparisons-uae-en.pdf

Symantec (2020), "Norton Cybersecurity Insights Report 2015", March 20, available at: https://ae.norton.com/norton-cybersecurity-insights-report-uae

Telecommunications Regulatory Authority (TRA) (2019), "TRA launches the UAE national cybersecurity strategy", June 24, available at: www.tra.gov.ae/en/media-hub/press-releases/2019/6/24/tra-launches-the-uae-national-cybersecurity-strategy.aspx

Further reading

Aboul-Enein, S. (2017), *Cybersecurity Challenges in the Middle East*, Geneva Centre for Security Policy, Geneva.

Al Neaimi, A., Ranginya, T., (2014), and P. and Lutaaya, "A critical analysis of the effectiveness of cyber security defenses in UAE government agencies", *Proceedings of the International Conference on Information Security and Cyber Forensics*, pp. 36-43.

Chandra, G.R., Sharma, B.K. and Liaqat, I.A. (2019), "UAE's strategy towards most cyber resilient nation", *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, October, Vol. 8 No. 12, pp. 2803-2809, doi: 10.35940/ijitee.L3022.1081219.

Fawcett, A. (2015), "Trolling the online abuse law", October 2015, available at: www.tamimi.com/law-update-articles/trolling-the-online-abuse-law

Fitch Solutions (2019), United Arab Emirates: crime and security risk report, Fitch Solutions Group Limited, London.

Hakmeh, J. (2018), "Cybercrime legislation in the GCC countries", *Fit for Purpose*?, Royal Institute of International Affairs, Chatham House, London.

Hasham, S. Joshi, S. and Mikkelsen, D. "Financial crime and fraud in the age of cybersecurity", available at: www.mckinsey.com/business-functions/risk/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity

Khodeir, O. (2017), "UAE Introduces New Public Prosecution Focusing on Cyber Crime," March 2017, available at: www.tamimi.com/law-update-articles/uae-introduces-new-public-prosecutionfocussing-on-cyber-crime

Corresponding author
Tareq Na'el Al-Tawil, Associate Professor of Business Law and Ethics can be contacted at: Tareq.AlTawil@zu.ac.ae