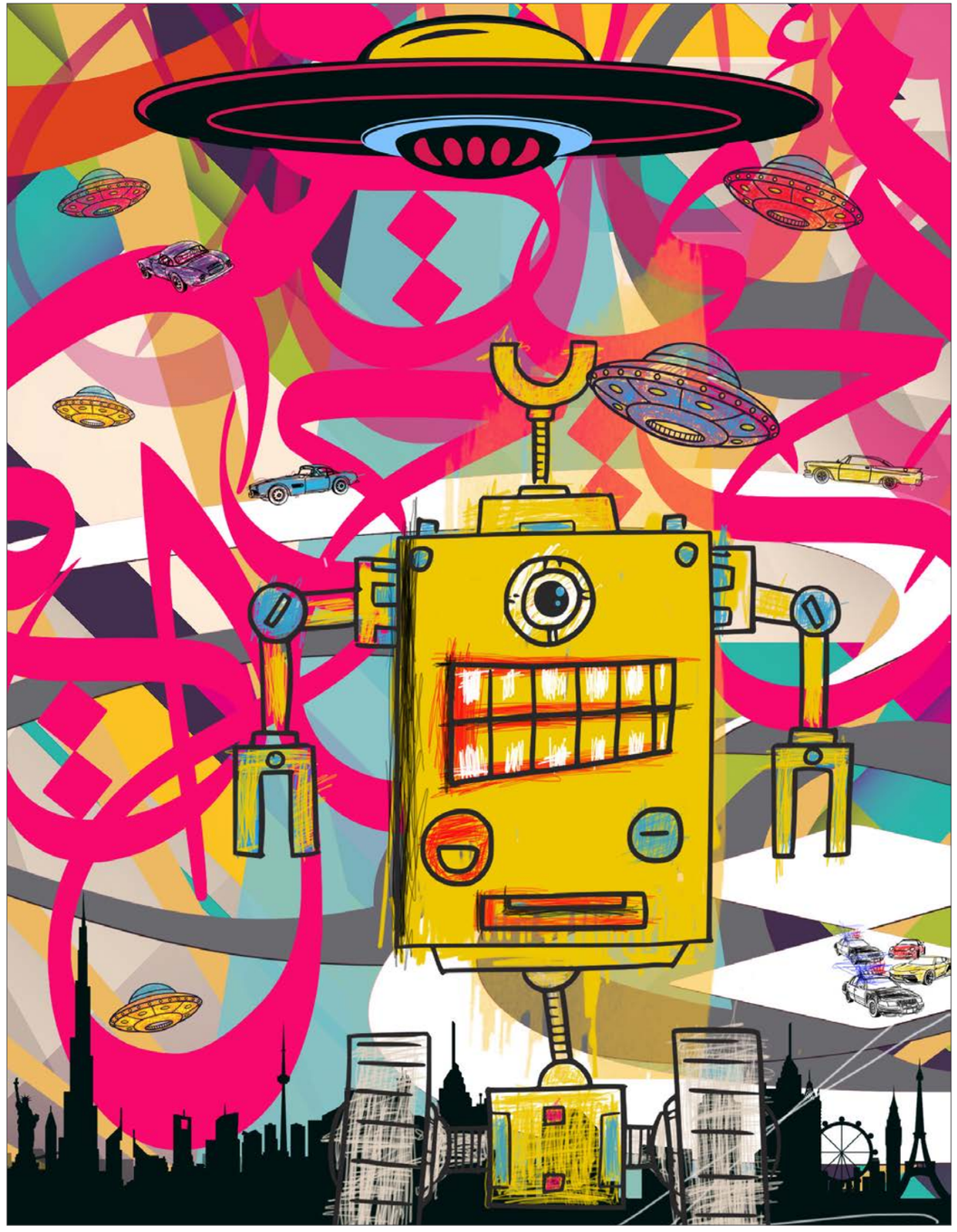


Lauris Zailaa[1]
We Are All Visitors I
Digital Creation
Variable dimensions

@lauriszailaa

The New World of Tech: Cybercrime and Cybersecurity in the UAE

Ibtissem Lassoued
Partner, Head of Advisory
Financial Crime
i.lassoued@tamimi.com

Andrew Fawcett
Senior Counsel
Technology, Media &
Telecommunications
a.fawcett@tamimi.com

It is one of the integral characteristics of technological development that the rate of digitalisation and technological adoption far outstrip the level of awareness and knowledge of how to defend against new threats. The ravenous appetite of businesses and individuals to capitalise on the opportunities and advanced capacities offered by new technology have undoubtedly yielded positive developments, but can come with a heavy price if companies leave themselves vulnerable to cyber-attacks. Naturally, although cybersecurity for businesses is maintained at an individualised level, there is an important role for the authorities to play in devising a flexible legislative framework that is capable of keeping pace with innovative technological development whilst also shielding against opportunism in criminal enterprise.

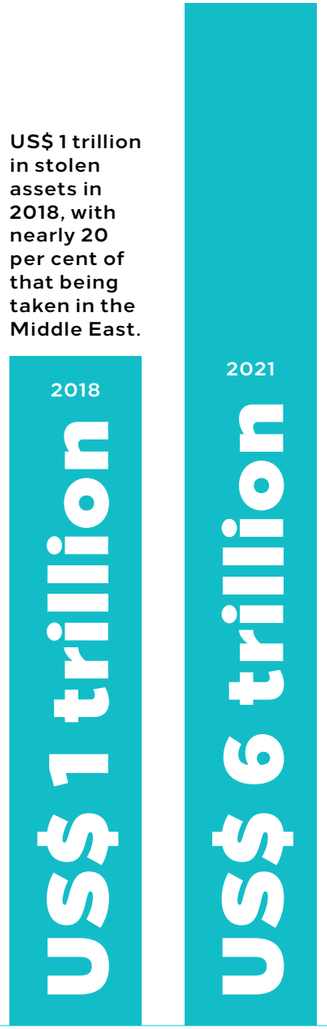
This challenge has particular significance for countries in the Gulf Co-operation Council, such as the UAE and Saudi Arabia, which are in the throes of strategic drives to transform their markets into internationally leading hotspots of commerce and growth. Part of the transitional process undertaken by both these countries has included embracing new technological and digital faculties, as sophistication in this arena is used to signify the futuristic and innovative vision guiding wider development. Social media offers a prime example of this issue; the UAE has one of the highest rates of social media penetration in the world at 98.98 per cent[1], yet this is a relatively new medium that offers almost unprecedented liberties for consumers and a plethora of new avenues for uncensored and unmonitored activities. From a criminal perspective, burgeoning platforms for clandestine or coded communication, veiled by virtual anonymity, presents an attractive new tool for activities such as co-ordinating illicit payment networks, cyberbullying, propagating disinformation streams, directing traffic to nefarious sites, spreading malware and ransomware.

[1] *Global Media Insight - UAE Social Media Statistics 2020*

Even as the world reels from the irrepressible impact of the ongoing health crisis, changes to the threat landscape of cyber-attacks serve as a potent reminder of the amorphous nature of cybercrime risks. Already, the past few months of adaptation in the commercial world have been closely shadowed by increases in malware attacks and eCommerce fraud, as well as espionage and disruption targeting the higher volume in internet communications, particularly Voice Over Internet Protocols ('VOIP'). Far from being unique to the UAE, however, these trends are pervasive at a global level and countries are grappling with finding effective means to slow their assault. Already, some estimates put organised cybercrimes as accounting for more than US$ 1 trillion in stolen assets in 2018, with nearly 20 per cent of that being taken in the Middle East. At the current rate, experts estimate that the annual cost of global cybercrime could reach US$ 6 trillion by 2021, eclipsing the value of the global drug trade[2].

US$ 1 trillion in stolen assets in 2018, with nearly 20 per cent of that being taken in the Middle East.

At the current rate, experts estimate that the annual cost of global cybercrime could reach US$ 6 trillion by 2021, eclipsing the value of the global drug trade[2].



Quantifying the cost of cybercrime is not just a rudimentary exercise in totalling the value of money actually siphoned during attacks as, subject to the methodology of the attacks, other assets may also be targeted: data is an exceptionally valuable asset for many companies which may be damaged or destroyed during an attack; intellectual property and trade secrets may also be stolen; and theft of personal or financial data may be stolen leaving the victims vulnerable to further attacks. Even once the primary attack has been committed, subsequent disruption caused to normal business operation, forensic investigation, restoration of hacked systems may further depress the bottom line of a victim, not to mention the reputational harm that may be caused if knowledge of the attack is leaked to the wider market. In some situations, the reputational damage caused to a company by failing to prevent a cyberattack could constitute an extinction level-event; in other words, even relatively routine cyberattacks can pose an existential threat to a business.

Part of the problem in defending against cybercrime is raising awareness and ensuring that people are cognisant of the type and level of protection that is needed in modern business practices to protect commerce. Simultaneously, this awareness needs to be reinforced by an effective legislative framework, involving not only criminal provisions but also supporting standards and policies that are capable of acting as guidance for companies in protecting themselves against contemporary cyber threats.

Typical Methodologies for Cyber Attacks

The UAE has had a dedicated cybercrimes law since 2005. The current law is Federal Law No. 5 of 2012 on Combating Cybercrimes (amended by Law No. 2 of 2016), however, in its current format, the law is largely limited to criminal law articles that criminalise the offences considered as constituting cybercrimes. Whilst criminal laws are a proven and vital measure for deterring undesirable and damaging activity, they are insufficient as a solitary means for creating a secure cyber ecosystem.

"In the UAE, the TRA is undertaking the challenge of designing a comprehensive cybersecurity legal and regulatory framework as a pillar of its National Cybersecurity Strategy to better safeguard UAE's digital future.

On 24 June 2020, the Dubai Financial Services Authority ('DFSA') published a thematic review report on cyber risks and highlighted that "cyberattacks targeting the financial services sector are becoming more frequent and sophisticated", indicating that the UAE still needs to treat the development of an effective cybersecurity system and cyber risk management framework as a strategic priority.

Capitalising on the nascence of cybersecurity awareness within many companies, many of the cyber-attacks perpetrated against companies in the UAE deploy relatively simplistic methodologies involving phishing emails, or fraud schemes whereby criminals assume false identities online to solicit transfer of funds. These methodologies are particularly vicious as they exploit the human weaknesses in cybersecurity systems, bypassing controls by deceiving unassuming human operators instead. This is a commonly recognised ploy in cyberattack methodologies, as compromising people is an easier feat than introducing sophisticated hacking techniques. The GCC is a particularly amenable market for such schemes, as criminals often pose as representatives of wealthy local families or high-net worth individuals and government institutions, targeting international businesses and claiming to offer investment services in line with the entrepreneurial reputation of emerging markets in the region.

One of the main challenges associated with cybercrime is the anonymity that is afforded by the internet. Often it is very difficult to trace the individuals behind online activities and new technologies are providing new ways to further inflame this issue; cryptocurrencies, for example, have added an additional element to ransomware and blackmail crimes and make recovery of funds almost impossible. This in turn increases their appeal to criminal actors.

The international element of cybercrimes is omnipresent, so legislation that facilitates co-ordination between national authorities is paramount. As offenders often are not necessarily physically present in the UAE, principles of jurisdiction and international co-operation need to be considered in order to properly equip the authorities to effectively enforce the laws. Not only do countries need to implement effective mechanisms to report and take action locally, but authorities also need to be able to amplify their capacity regarding cross border measures, in co-ordination with other jurisdictions. Seeming

[2] *Cybersecurity Ventures 2019 Official Annual Cybercrime Report*

inefficacy of this option can be a major deterrent to companies taking measures to pursue or report cyber incidents, and where cyber criminals feel they can act with impunity, the risk of further incident is exacerbated.

UAE's Path to Cyber Resilience

In the UAE, the Telecommunications Regulatory Authority ('TRA') launched an updated National Cybersecurity Strategy ('Strategy') in June 2019. The vision for the Strategy is to create a safe and resilient cyber infrastructure in the UAE that enables citizens to fulfil their aspirations and empowers businesses to thrive. To achieve these objectives, the TRA is mobilising the whole cybersecurity ecosystem to deliver initiatives across five strategic pillars: developing a comprehensive legal and regulatory framework; fostering a vibrant cybersecurity ecosystem; establishing a standardised National Cyber Incident Response Plan; protecting critical assets of the UAE in key sectors; and cultivating local and international partnerships to mobilise the entire cyber ecosystem.

As the primary pillar, the plan to implement a comprehensive legal and regulatory framework includes devising legislation that both addresses all types of cybercrimes and secures existing and emerging technologies. Whilst, in principle, these dual goals may seem simplistic, there are multifarious considerations that would underpin their execution. What would such laws and regulations potentially cover? How could they be structured to account for future development and unforeseen applications of technology? Lessons learnt from cybersecurity laws that have been enacted in other jurisdictions may prove invaluable in assisting the UAE's efforts to design a cybersecurity legal and regulatory framework that meets its long-term needs.

Possible Provisions to Assist with Investigations and Prosecutions

One area of potential legislative development is the application of technology to cybercrime investigations and prosecutions. Concurrent with strict criminal provisions, additional laws will likely be needed in order to elaborate on important procedural aspects that are now found in some of the main international laws. Such supplementary laws could cover specific powers for search and seizure of computer hardware or data, for example, access to stored computer data, as well as orders requiring preservation of computer data.

Licensing of Cyber Security Professionals?

Singapore's Cybersecurity Act 2018 creates a framework for the licensing and regulation of certain types of cybersecurity services and their providers. The rationale is that cybersecurity service providers are given broad access to customer systems and networks and could amass an in depth knowledge of system vulnerabilities in the course of providing their services. Consequently, there should be some assurance concerning the fitness and ethical code of conduct of such service providers.

Important considerations around this possibility include questions such as whether licensing would negatively impact the development of a cybersecurity ecosystem, and who should be licensed. Singaporean legislation allows only licensed penetration testing and managed security operations monitoring service providers, as they are already mainstream and widely adopted. Any significant expansion of such provisions would be a foray into unchartered waters for the UAE.

Licensing costs should not be significantly high so that companies are not dissuaded from obtaining the licence and instead deal with the cybersecurity consequences. The legislation would need to strike a balance between mitigating upfront costs and ensuring that the profession is duly formalised and legitimised.

Legalising 'White Hat' Hacking?

White hat hackers, also known as 'ethical hackers', are either employed by companies or contractors who specialise in finding weaknesses in a security system via 'authorised' hacking. The existing UAE legal framework does not explicitly address the permissibility of white hat hacking, and regulating such activity would be a significant development to the UAE's cybersecurity ecosystem, potentially adding an aggressive capability to existing defence measures.

Hacking Back?

'Hacking Back' allows victims of cyber-attacks to try to track down their attackers by entering the systems of organisations they suspect have been used by the hackers to mount their assault. The potential consequences of allowing such activity, however, would seem to suggest that hacking back is best left to government security authorities.

This is because it can be very hard to determine who is behind a cyber-attack. A computer that appears to be behind an attack, could itself have been hacked. Consequently, harm could easily be caused to innocent parties' computers.

Security by Design?

Applications of emerging technologies tend to be developed with functionality as a priority, and security is often an afterthought. Security by design is an approach to cybersecurity that focuses on preventing a cybersecurity breach at the outset of a project, by building in a way to minimise flaws rather than repairing the issue after a breach. Whilst the TRA's existing Regulatory Policy on the Internet of Things ('IoT') dated March 2018 already requires security by design to be incorporated into IoT devices to provide protection against unauthorised usage, this approach to cybersecurity could be expanded into the regulation of Artificial Intelligence and cloud services.

Brave New World for Cyber in the UAE

Cybercrime and hacking have a material impact on society that needs to be comprehensively addressed by a bespoke and responsive legal framework. All too often, a reactive approach to cybersecurity is applied, taking measures only after a security breach or a vulnerability has been found. The UAE has announced grandiose plans to reform its cybersecurity and cybercrime ecosystem, in recognition of the accelerating effect new technology can have on development, and the counterweighted restraints that need to be imposed to prevent cyber-attacks. In the meantime, the onus is on individual businesses to understand the risks posed to their operations through their cyber infrastructure and the ways in which they can fortify their defences against cyber-attacks. Human error plays an indubitable role in facilitating cyber-attacks, so training and awareness initiatives are an effective means by which companies can reduce their susceptibility to attacks that deploy common techniques such as phishing.

The UAE has one of the highest rates of social media penetration in the world at **98.98** per cent.

Source: Global Media Insight - UAE Social Media Statistics 2020