International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-12, October 2019

UAE's Strategy Towards Most Cyber Resilient Nation

Geetanjali Ramesh Chandra, Bhoopesh Kumar Sharma, Iman Ali Liaqat

Abstract: ***With the fast-paced industrial and Techni revolution, smart nations are emerging with the idea of integrating the developing technologies, like IoT and CPS, to make communications and networks easier and closely interconnected. With increasing technology usage globally, the UAE envisions transitioning into a global smart nation by innovating and deploying world class disruptive technologies for the better connectivity digitally.***
However, the frequency of cyber threats has also increased drastically with this ever-evolving technology. For a nation like UAE that is transforming into a digital nation at a rapid speed, while still having stakeholders with poor cybersecurity practices, UAE stands as a strong target for attacks by malicious hackers. With cyber-attacks becoming the top most concern globally, especially in the Middle East, UAE has built certain strategies to combat the evolving issue of cybersecurity.
In this paper, the authors suggest that just as the collaboration of the key stakeholders – government, academics, industry and society – depicted under the Quadruple Model is needed to develop an innovative and creative nation, so is their coordination required to protect that nation from the potential cyber threats. In light of this theory, the four key stakeholders of the UAE are analyzed for their cybersecurity practices, initiatives and coordination to prove UAE's commitment towards becoming the most cyber resilient nation in the world.

Keywords: UAE, Cyber Resilient Nation, Fourth Industrial Revolution, Quadruple Model, Cybersecurity

I. INTRODUCTION

The population of the UAE is rapidly increasing from 9.5 million in 2018, to a predicted rise to 9.8 million by 2021[1]. Most of the population are tech-savvy millennials, where about 70-80% of the population carry smart phones, setting the nation in the top positions of worldwide technology infiltration [2]. This increasing trend has prompted UAE government to take smart initiatives to manage the growing population effectively which involve the use of IoT technologies embedded in the "smart cities" of the UAE. It aims to provide its people with the best facilitates and produce a happy nation. The UN World Happiness Report 2019 ranks UAE 21st among other nations of the world [3].

Revised Manuscript Received on October 30, 2019.
***** Correspondence Author
Geetanjali Ramesh Chandra*, Department of Law, Amity University Dubai, Dubai (UAE). Email: gchandra@amityuniversity.ae
Bhoopesh Kumar Sharma, Deapartment of Forensic Sciences, Amity University Dubai, Dubai (UAE). Email: bsharma@amityuniversity.ae
Iman Ali Liaqat, Department of Commerce, Amity University Dubai, Dubai (UAE). Email: imanali6@hotmail.com

UAE is also among the top ten most positive nations in the world [4], housing two of the world's smartest cities - Abu Dhabi and Dubai. The UAE Vision 2021 emphasizes on innovation and transitioning towards a knowledge-based economy by increasing research and development three-fold by 2021 [5]. As per the Global Innovation Index 2018, UAE ranks 38th but demonstrates high commitments through its National Agenda to become one of the top ten most innovative countries by 2021 [6].
But where technology exists, accompanies it are its risks and threats, and with a city undergoing digital transformation, there are higher threats to a country which must be identified and mitigated. As per Kaspersky Lab's Malware Reports, UAE was one of the top ten countries with 1.9% users attacked by a malware in Q3 2018 [7]. Dark Matter, a cybersecurity firm in UAE, reported that the country is subject to 5% of all the global cyber-attacks and such attacks have increased nearly by 55% over the past five years [8]. There are many such statistics that portray the cybersecurity vulnerabilities of UAE. Yet the country is determined to strengthen its cybersecurity through collaboration of various key stakeholders – government, national and international industry players, academicians and the society at large - and the aim of this paper is to understand the importance of these players and the extent to which they contribute in the UAE to the build a smart and secure nation.

II. LITERATURE REVIEW

A. Smart Nation

Smart City has been a concept widely sought out by many countries worldwide including those in the GCC like Oman, Kuwait, Bahrain, Saudi Arabia, Qatar, and UAE. The most prominent smart city projects in UAE are the Masdar City in Abu Dhabi and Smart Dubai in Dubai. There are several definitions of a Smart City. The smart city is a concept of compelling mix of physical, advanced and human frameworks into a misleadingly made condition so as to guarantee maintainable, fruitful and far reaching future for natives [9]. Smart cities are emerging to improve quality of life and create a competitive and interconnected economy through Internet of Things (IoT) and Cyber Physical Systems (CPS) [10]. Other technologies that support smart city transformation include artificial intelligence, machine learning, blockchain technologies, drones, autonomous vehicles, robotics, and cloud technologies. UAE has several specific smart technology strategies like the UAE Artificial Intelligence Strategy 2031, UAE Blockchain Strategy 2021 and the Hyperloop project.

Moreover, a leading Dubai project is known as the Dubai 10X initiative, a concept of disruptive innovation that positions Dubai 10 years ahead of other global cities. Dubai's Smart City initiative aims to make its citizen happy by using Internet of Things (IoT) and Internet of Everything (IoE) to enhance safety, waste management, educational platform, financial services, e-government and much more [11].

UAE has built its National Innovation Strategy (NIS) to become the leading innovative nation. It defines innovation as the desire of individuals, private institutions, and government to generate creative ideas and innovative products and services that improves quality of life, promotes economic growth and increases competitiveness. It aims to do this by providing the right platform and infrastructure and by primarily focusing on priority sectors that will drive innovation including technology, education, transportation, renewable and clean energy [12]. Including UAE Vision 2021, the National Strategy for Innovation recognized digital technology among the top domestic main sections. The strategy mainly focuses on the development of smart cities, updated software, and applications using disruptive methodology such as the artificial intelligence, nanotechnology, semiconductors, and 3D printing, as well as ensure a swift implementation of technology across various industries.

Transformation into a Smart Nation is a "Whole of Nation Approach" that requires commitment and cooperation of various stakeholders and deployment of the right set of skills and infrastructure [12].

B. Quadruple Helix Model

UAE has constantly been distinguishing itself in terms of innovation and creativity by enhancing its social and economic status. Believing on innovation being the future of human investment, the UAE Vision 2021 emphasizes innovation, research, science and technology to be the pillars of a knowledge-based economy, led by ambitious entrepreneurs in a business-friendly environment where effective public-private partnership exists [12].

A successful innovative and creative economy requires the combined synergy between key innovative players - academicians, industry, government and the society at large [13]. This is well depicted under the creativity knowledge-based model "Quadruple Helix Model" (Figure 1), that suggests a strategic approach to economic development through interaction between the four key stakeholders for decision making, policies and practices [13]. The Quadruple Helix Model is a further development of the Triple-Helix Model, which previously involved interaction between three players – academicians, industry and government. The triple-helix model enables economic development towards a smart city by synergizing government policies, academic leadership and other major corporate strategies [14]. This model consists of only institutionalized domains, missing the public domain, whose contribution would complete the entire knowledge-based, innovative economy paradigm [15-16]. Every stakeholder in the Quadruple Helix model has a key role to play – academicians from universities act as researchers (science), the government acts as the policy maker (policy), and the industry plays the role of producers (economy), while the society acts to fill the gap between these three parties and complete the paradigm (connector).

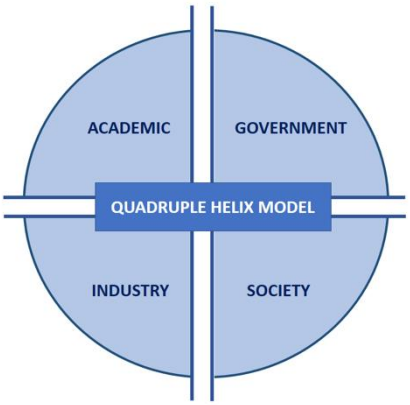

Figure1: The Quadruple Helix Model (Compiled by Authors)

C. "The Challenge" For Smart Nations

Smart nations are built on emerging technologies with support of Internet of Things (IoT) devices, Cyber-physical Systems (CPS or sensor networks), cloud technologies and their likes and result in several dimensions such as Smart Governance, Smart Energy, Smart Technology and Smart Infrastructure. As acknowledged earlier, with every technology accompanies its risks. And just like the four key players of a smart nation – academics, government, industry and society – play an important role in the development of a knowledge-based, innovative economy, so is their collaboration vital to identify the risks associated with the technological innovation and find ways to mitigate them (summarized in Figure 2).

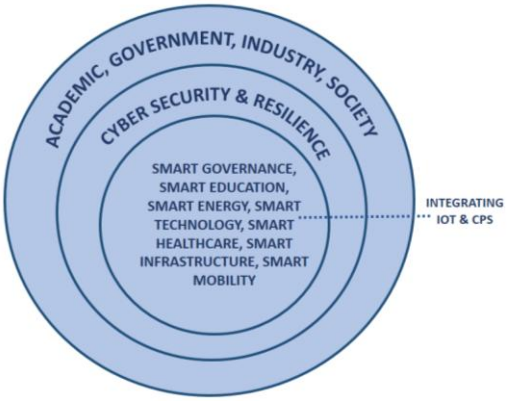

Figure 2: Role of the Innovative Economy's key players to identify and mitigate risks associated with innovative technology (Complied by Authors).

With increasingly interconnected cities and large amount of data distribution, the main challenge will arise in cybersecurity and privacy. There will be a great need to mitigate security risks associated with new data and that collected for future use and manage privacy concerns and personal data control. With cities using technologies like autonomous vehicle, smart apps and smart traffic lights to interconnect, hackers look for loopholes in the entire network to target critical infrastructure and private data [11].

Table 1 lists some of the likely cyber-attacks and their consequences on the autonomous vehicles for instance.

Table 1: Potential cybersecurity risks to an autonomous vehicle

Risk	*Consequence*
Network Attack	Loss of communication between various IoT and CPS devices connected, causing network interruption.
Sensor Attack	Loss of data transmission to the network, hence requiring vehicles to be trained to make uninformed decisions.
Vehicle Attack	Vehicle may be used for maleficent activity, causing car crash or harming passengers by any means.
Data Theft	Data privacy and security threat, exposing sensitive data (including user information)

Hence, we understand that with coordination of key stakeholders of a creative economy, traditional security infrastructures need to be upgraded and robust cyber policies must be in place to address the challenges associated with the emerging technologies and successfully transform to an innovative and cyber resilient nation.

III. CYBER SECURITY

Cyber security is a combination of the policies, best practices, tool and devices designed and used to maintain the CIA triad – i.e. Confidentiality, Integrity and Availability. The flourishing digital economy, however, is attached with cyber threats, and risks for nations in context of malware, organized cybercrime and cyber terrorism, personal information and data breach, and Advanced Persistent Threat (APT) [17]. In this section, we will analyze the extent of the various cyber-attacks globally and those specific to GCC and UAE.

Cyber Threats Worldwide

The Global Risks Report 2019 is the 14th Edition published by World Economic Forum that provides an overview of the potential global risk landscape in the year 2019 which extend from increasing environmental degradation to the disruptions of the Fourth Industrial Revolution. The report presents results of Global Risks Perception Survey (GRPS), wherein about 1,000 decision-makers from public sector, private sector, academia and the civil society have assessed the global risks. In over ten years span, extreme weather and climate-change policy failures are foreseen as the deadliest threats. Technology instability is seen as another substantial risk in the coming decade, where massive data fraud and theft ranks four and cyber-attacks rank five globally [18]. It is predicted that cybercrime would cost $6 trillion globally by 2021[19].

Malware attacks generally tripled the total amount of cyber-attacks in 2017 in the first half of 2018, though 2017 faced the most drastic of ransomware attacks called WannaCry and Petya/NotPetya. The serious assessment of cryptocurrencies has drawn illegal trade on the Dark Web and payments through infections with ransomware, Distributed Denial of Service (DDoS) and tons of others. Just as technology is advancing, the malware threats are getting more sophisticated since criminals and terrorists employ experienced hackers. These threats are growing regionally and globally, and the worst threat to a nation is cyber-attack on energy in the form of power plants and grids that if disturbed would shut the country down.

Data fraud is also associated with identity theft, where two-third of the GRPS respondents expected the risks with fake news and identity theft to magnify in 2019 and about three-fifth held the similar opinion on loss of privacy to companies and governments, a consequence of mainly the loopholes in cybersecurity national policies. Like the Yahoo accounts breach in 2016 which reported around 3 billion accounts' data stolen. In India, government ID database, Aadhaar, suffered several breaches compromising the records of about 1.1 billion registered citizens [19].

Many other massive data breaches were reported in 2018, especially with new hardware weaknesses revealed, posing great risk to critical infrastructure and the national security at large. Meltdown and Specter were threats to the hardware that affected almost every Intel processor in the last decade. The Global Risk report stresses on the potential use of Artificial Intelligence (AI) and Machine Learning (ML) to engineer more sophisticated cyber-attacks with high use of IoT to connect billions of devices together. Some of these AI and ML threats include exploiting fake video and audio generated mostly by AI, hacking smart contracts, breaking encryption using quantum computers, and cloud computing assaults [20]. Likewise, malicious attacks on critical infrastructure may negatively affect people's lives, for instance an attack on a hospital's system could cause casualties if the data is tempered by changing prescriptions or turning off life-support or other critical systems.

Cyber Threats in the GCC & UAE

Over the previous few years, cyber-attacks have increased in the GCC region, posing an increasing threat to business operations. Both government and private websites have frequently been targeted by malicious attacks such as ransomware, virus attacks and crypto jacking, and have also been hit by the biggest worldwide WannaCry attack in 2017. For example, at the end of 2017, malicious software assaulted the websites of Kuwait's Ministry of the Interior and Saudi Aramco (state-owned oil corporation). UAE's Telecommunications Regulations Authority (TRA) has also reported at least 86 cyber-attacks faced by the country in the beginning of 2018, like the UAE ride-sharing service Careem data breach that exposed data of around 14 million people. Since the Middle East is more dependent on the oil and gas sectors, attacks on such sectors could be devastating for the economy. Ever since, the GCC countries are actively seeking to mitigate these risks by enhancing cybersecurity strategies and implementation [21].

According to Dubai Police, around one in five residents in the UAE were victims of cyber-crime in 2015, and reports of cyber-crime increased by 23% later in 2015. According to Kaspersky Lab, UAE ranked 8th worldwide in 2016 in terms of the percentage of users attacked by banking trojans, where five of the top ten trojans targeted smartphones running Android OS holding the largest market share (about 40 percent) in the UAE.

In 2017, credit / debit card fraud was the most expensive cybercrime technique in the UAE with a loss of more than $1,000 per customer.

Besides individual consumers, financial institutions and government agencies have also been struck hard by cybercrime, particularly by targeted attacks such as DDoS and malware infections.

While a handful of GCC countries are better ready to deal with the increasing risk of cyber-attacks, others still need to upgrade their policies for cyber security. According to the Risk Briefing of the Economist Intelligence Unit, which measures operational risk in 180 nations, the analysis of the cybersecurity preparedness in GCC region 2018-19 (Table 2) showed that Oman and Qatar rank the highest. As per UN Global Cybersecurity Index (GCI) 2017, Oman is a proactive country in the cybersecurity field and is also ranked fourth globally for best preparedness for cyber-attacks. It has taken a number of measures to combat cybercrime including strong legislations, active and continuous audit checks and the launch of Oman's National Computer Emergency Readiness Team (CERT) in 2010 to promote cybersecurity awareness.

Table 2: Preparedness on Cyber Security in GCC countries (2018-19)

(0 = High preparedness; 4 = Low preparedness)

Country	*Score*
Qatar	0
Oman	0
UAE	1
Bahrain	2
Saudi Arabia	2
Kuwait	3

Source: (The Economist Intelligence Unit, 2018)

The UAE scored 1, it is comparatively well prepared to deal with cyber-attacks in the region, and ranks 47th in the global cybersecurity index (as compared to 4th position of Oman). Several national and international strategies have been put in place to address the growing issue of cybersecurity which shall be discussed in depth in the following sections. Saudi Arabia and Bahrain both score badly on cyber preparedness, while Kuwait is the most vulnerable of the six GCC countries evaluated for cyber-attacks.

IV. UAE CYBERSECURITY PREPAREDNESS

In light with the Quadruple Helix Model, we have analyzed the extent to which the key stakeholders in the UAE – government, industry, academics and society - have contributed to the nation's drive to become the leading Smart and Cyber Resilient Nation.

Government

The UAE government, including the Smart Government, ranks number one in Middle Eastern digital adoption and has the largest digital facilities, such as digital signatures and smart cards, as well as numerous digitization initiatives, such as increasing broadband coverage and smart city projects [2]. The National Cyber Security Strategy (NCSS) of the UAE aims to secure the national information and communication across the country primarily by preventing and addressing cyber threats, educating public and the workforce, encouraging research in cybersecurity, international collaboration and by developing initiatives to guide the implementation of the NCSS. Moreover, UAE has also set a national cyber incident report team (CIRT) known as "aeCERT" [22]. As part of national and international collaboration strategy, The UAE has signed a Memorandum of Understanding (MoU) with several international organizations such as the British Standards Institution (BIS) and the SENAAT General Holding Corporation.

In 2014, the Dubai Electronic Security Center (DESC) was launched to develop and implement best practices in city-wide information and cyber security. The center introduced the Dubai Cyber-security Strategy in 2017 with domains for cyber smart society, innovation, cyber security, cyber resilience and collaboration. Though the strategy is well in place, the estimated time frame for the implementation of the Cyber Security Strategy is five years [23]. The DESC also initiated 'Cyber Security Standard' for Autonomous Vehicles in line with the Dubai Autonomous Transportation Strategy which aims to transform 25% per cent of the total transportation in Dubai to autonomous mode by 2030.

UAE has several cyber laws in place governing the cybersecurity and data privacy some of which include Federal Law 5 of 2012 on Combatting Cybercrimes and Federal Law No. 1 of 2006 on Electronic Commerce and Transactions. Speaking of data protection legislations in UAE, there is also no general federal data protection law in the UAE, like the GDPR in the Europe, though there is a general right to privacy for citizens under the UAE Constitution, limited to citizens of UAE that are 8% to 12% of the total population of the UAE [24]. There is also no particular national regulatory authority for data protection in the UAE, and criminal sanctions can be enforced against an offender by the police for violation of the Penal Code or the Cybercrime Law. However, there are some sectoral regulators placed that include:

- *Telecommunications Regulatory Authority:* The Telecommunications Regulatory Authority (TRA) regulates and enforces the Telecommunications Law.
- *DIFC Commissioner of Data Protection:* The Commissioner of Data Protection is responsible for enforcing the Data Protection Law in the Dubai International Financial Centre (DIFC).
- *Centre for Healthcare Planning and Quality (CPQ) in Dubai Healthcare City:* The Centre was established as an independent regulatory body to set and maintain best international practices in healthcare, that include data security and privacy, in Dubai Healthcare City (DHCC).

Worth considering are some conflict of interest arising from different set of cyber related laws and principles between the sectoral regulators and the UAE legislation at large. For instance, the free zone UAE-Dubai International Financial Centre (UAE-DIFC),

that has an independent Commissioner of Data Protection serving as a national data protection authority, prohibits data transfer to jurisdictions with less stringent requirements, including areas of the UAE outside the DIFC free zone. On the contrary, there are no specific provisions governing data transfer under UAE law and, pursuant to Article 378 of the Penal Code, data subjects should give their consent to the transfer of personal data to third parties, either within or outside the UAE.

This entails that the inconsistency between UAE data protection legislation and those of the sectoral regulators, like the DIFC, reflect different priorities and responsibilities towards citizens which creates a conflict of interest worth considering and mitigating [24].

Industry

As highlighted previously, the Middle Eastern region has been prone to many cyber-attacks, including advanced malware attacks primarily on large organizations, oil and gas utilities and the financial sector, and so many initiatives are put in place to protect the nation's critical information infrastructure [25]. Only investing in highly secure and robust technology to mitigate these risks will do no good if the persons handling the systems are not well educated on how to safely deploy the technology. Hence personnel's awareness, training and education on cybersecurity is very crucial for a successful and competitive enterprise and economy at large.

There is a significant danger recognized among UAE organizations as per Dark Matter's Q3 2018 study that should be resolved to enhance cyber resilience. The research demonstrates that UAE organizations can enhance their IT security and make attacks difficult merely by addressing some essential vulnerabilities that include obsolete and unsupported software, weak passwords, unpatched systems, and weaknesses in configuration management. It has been revealed that approximately 45% of the top 20 recognized vulnerabilities have been categorized as extremely serious. 93% of the assessments reported were obsolete software, 83% were unsupported software, 77% had poor credentials and 34% had misconfigurations [26].

In UAE, the Dubai Future Academy, the Dubai Future Foundation's initiative, holds numerous workshops and crash classes to demystify the recent techniques by disseminating expertise and leveraging individuals ' abilities to assist them better prepare for the ever-changing future. Dark Matter Group, the region's first and only fully-integrated digital transformation, defense and provider of cybersecurity alternatives, "Cyber Education" has been launched, offering a broad variety of lessons and programs to increase cyber talent – from fundamental safety awareness programs to training for particular sectors and professions.

One of the pillars of the National Cyber Security Strategy (NCSS) of the UAE and the Dubai Cybersecurity Strategy is to leverage international and national collaboration, hence the Government entities actively plan to collaborate with private entities and startups. The Dubai Future Foundation (DFF) was founded to play a crucial role in shaping the future and enabling effective government and private sector entity cooperation, allowing international technology companies to test their future solutions in Dubai and setting it as the leading industry of the future.

Academics

Academic institutions play a critical role in educating the future cybersecurity workforce and preparing them to take forward a safe, innovative nation. Collaboration with the industry players will enable academic institutions to stay updated and mend their curriculums according to the recent technological trends to equip the students for the jobs of tomorrow. To attract a large number of people to this growing field, it is important to acknowledge that cybersecurity is an interdisciplinary field and should not just be confined to engineering students, but also to other fields of management and science so that they are all well prepared to contribute to a smart and secure nation. Universities can also offer great up skilling programs and opportunities for executive-level training courses.

Evolving technologies like IoT and CPS interconnected in smart nations require innovative and robust cybersecurity techniques, which can be well supported by research and development and closer cooperation between the government, academia, industry and society. R&D will help fill the technology gaps in IT security by constantly preparing for the next generation security threats and producing solutions to mitigate the same [27]. Open innovation involves different approaches to attain and manage intellectual property rights, which helps resolve ownership issues and enables the IP owner to commercialize their innovation. The Takamul program in Abu Dhabi provides legal and financial support, to IP owners in the UAE, for international patent filings at the USPTO and the PCT. Financial support extends to as much as 90% for individuals, 60-75% for academic institutions and about 50% for commercial organizations. UAE has also planned to double its spending on national security to more than $10 billion by 2024 with a majority of the funding aimed at strengthening cyber-security.

UAE has established research centers like the Information Security Research Center (ISRC) at the Khalifa University, which offers MSc and PhD degrees in cyber-security, and the Center for Cyber Security (CCS) at New York University Abu Dhabi, which focus on partnering with key local universities, industry and government agencies to facilitate cybersecurity research and enhance the country's cyber resilience.

Society

As emphasized earlier, cybersecurity for a smart nation is not just an institutional approach, but the responsibility equally lies on the public to ensure safe use of the technological solutions provided. And it is the responsibility of the other key stakeholders – government, industry and academicians – to make the public aware of the cyber risks they are prone to and ways to guard against them [27].

Though UAE has one of the highest mobile penetration worldwide, and a large portion of its population are millennials, it is this very segment of tech-savvy youth that is the most vulnerable to cybercrimes around the world. Millennials globally own at least four devices on average and have the least amount of cyber hygienic practice, one in four millennials, for example, uses the same password for all accounts and 63% shared at least one of their passwords with another. While in the UAE, about 45% of cybercrime victims share their password with another individual for at least one account and 20% use the same password across various accounts [28].

Phishing is one of the most common cyber-attacks in the GCC region, including in UAE. UAE ranked 10th in the globe in terms of the percentage of email traffic recognized as phishing and 7th for the percentage of email traffic recognized as malicious, according to a study. Dubizzle — the UAE's largest classifieds website— carried a survey to assess the cyber hygienic practices of the public [29]. The results showed that 36% of the respondents had never heard of the term "phishing" while 16% had heard the term but did not know its meaning. The outcomes explain why Dubizzle is a lucrative platform for phishing scammers, where 30.8% suspected scams where on Dubizzle Jobs and 27.6% on Dubizzle Motors [30].

Therefore, education, awareness and safe surfing of the users is essential in combating cyber threats that arise from emerging technologies. In early 2018, the initiative "Cybersecurity Ambassador" was launched to build a secure e-culture, empowering Emirati students as ambassadors for cybersecurity, in line with UAE Vision 2021 to promote a secure electronic lifestyle in the UAE. Recently, the 'Child Digital Safety' initiative was launched in UAE to enhance child safety and the quality of digital life in the country. The initiative was launched on the Emirati Children's Day on 15th March 2019, consisting of several activities like an interactive children's camp, training workshops, digital wellbeing portal and a platform to address queries from parents.

V. CONCLUSION

The main objective of this paper was to analyze the cyber resilience of UAE, a smart nation with strong visions of becoming a knowledge-based creative economy and leading other countries in terms of innovation and cybersecurity. Leading two successful smart city projects – in Abu Dhabi and Dubai – UAE is in the frontiers in deploying advanced IoT, CPS and cloud technologies. Yet in terms of cyber-attack preparedness, UAE demonstrates a relatively well score on preparedness for cyber-attacks among the GCC countries, and 47th globally. High digitization, interconnected communications and inadequate cybersecurity measures make countries like the UAE a strong target for cyber attackers, especially with an increase in the extent of cybercrimes worldwide and in the Middle East.

Introducing the Quadruple Helix Model for an innovative economy, we connect the same model to the importance of establishing a cyber resilient nation. The collaboration between the key stakeholders namely the government, industry, academics and society are essential to build a cyber secure nation. Having said that, we analyzed to what extent has the UAE's four key players actively contributed to the cyber resilience of the country.

UAE has legislations for cybercrimes in place, but what is required is a single national regulatory to harmonize laws between free zones and those of the UAE legislation at large. A constructive national cybersecurity strategy is also in place, including the Dubai Cyber Security Strategy, however the implementation time frame of these strategies is quite long compared to the rapid changing cyber environment and need for quick actions for cybersecurity.

Public-private sector collaborations and investment in advanced cyber security technologies are a great stepping stone, however, the most significant factor in the successful deployment of these investments is the development of an ecosystem for qualified individuals, technocrats and researchers from the national and global talent pools. Moreover, businesses must be aware that cyber-attacks are evolving in their methods and techniques and so to keep pace with the evolving cyber climate, timely personnel awareness and training is crucial to minimize its impact. And so, the academics and R&D play a major role by equipping the future talent with skills of tomorrow and by up skilling employees and executives. The UAE has several initiatives on technical workshops, but it also needs to integrate cybersecurity in schools and universities as part of their curriculum. R&D is required to prepare cybersecurity techniques for the future, unexpected cyber threats and UAE has established research centers and actively planned to invest a great deal in R&D.

Lastly, yet most importantly, the public plays a very important role in the whole paradigm of transforming into a smart and secure nation. With rapidly increasing population and high digital penetration, UAE comprises a population of mostly the tech-savvy youth with poor cyber hygiene practices, make the country vulnerable to cyber-attacks. Hence a lot of effort from the UAE Government, aeCERT, academics and national and international collaboration of the industry is required to make the society well aware on the threats of the cyber world and enable them to make more informed decisions.

The UAE government, national and international industries, academicians and R&D and the society at large, together these key players can lead the country to become a leading Smart, Secure and Cyber Resilient Nation.

REFERENCES

1. World Population Prospects - Population Division - United Nations. (2019). Retrieved from https://population.un.org/wpp/
2. McKinsey & Company. (2016). *Digital Middle East: Transforming the region into a leading digital economy.* Digital McKinsey.
3. Helliwell, J. F., Layard, R., & Sachs, J. D. (2019). *World Happiness Report* . United Nations.
4. The National. (2019, Mar 18). *UAE ranks among top 10 'most positive countries'.* Retrieved Mar 22, 2019, from The National UAE: https://www.thenational.ae/uae/uae-ranks-among-top-10-most-positive-countries-1.838601
5. Government, UAE. (2015). *Science, Technology and Innovation Policy in the UAE.* UAE.
6. (n.d.). *Global Innovation Index 2018.* WIPO; INSEAD; Cornell SC Johnson College of Business.
7. Chebyshev, V., Sinitsyn, F., & Parinov, D. (2018, Nov). *IT threat evolution Q3 2018. Statistics*. Retrieved Mar 22, 2019, from Kaspersky Lab: https://securelist.com/it-threat-evolution-q3-2018-statistics/88689/
8. Ibish, H. (2017). *The UAE's Evolving National Security Strategy.* The Arab Gulf States Institute in Washington .
9. Smart Cities | BSI Group. (2019). Retrieved from https://www.bsigroup.com/en-GB/smart-cities/
10. Chia, E. S. (2016). Singapore's smart nation program — Enablers and challenges. *11th System of Systems Engineering Conference (SoSE).* IEEE.
11. Bloomberg New Energy Finance. (2018). *The Masdar Report on Technologies for Future Smart City Transit.* Abu Dhabi: Masdar.
12. UAE Minstry of Cabinet Affairs. (2015). *UAE National Innovation Strategy.*

13. Wahyu, S. (2017). The Quadruple Helix Model: Enhancing Innovative Performance Of Indonesian Creative Industry. *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH* , 90-94.
14. Carayannis, E., & Campbell, D. (2012). *Mode 3 Knowledge Production in Quadruple Helix innovation Systems.* Springer.
15. Leydesdorff, L., & Deakin, M. (2011). The triple-helix model of smart cities: A neo-evolutionary perspective. *Journal of Urban Technology 18*, 55-63.
16. Leydesdorff, L., & Etzkowitz, H. (2003). Can 'the public' be considered as a fourth helix in university-industrygovernment relations? Report on the Fourth Triple Helix Conference, 2002. *Science and Public Policy 30*, 55-61.
17. Teih, C. S., & Kamil, A. (2017). NATIONAL CYBER SECURITY STRATEGIES FOR DIGITAL ECONOMY . *Journal of Theoretical and Applied Information Technology* , 6510-6522.
18. WEF. (2019). *The Global Risks Report 2019.* Switzerland: World Economic Forum. Retrieved from http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
19. Grant Thornton. (2017). *Cyber-crime: avoid paying the price.* Grant Thornton UAE.
20. Giles, M. (2019, Jan). *Five emerging cyber-threats to worry about in 2019*. Retrieved Feb 2019, from MIT Technology Review: https://www.technologyreview.com/s/612713/five-emerging-cyber-threats-2019/amp/
21. The Economist Intelligence Unit. (2018, April 03). *Cyber attacks: is the GCC prepared?* Retrieved Mar 21, 2019, from Telecommunications: http://www.eiu.com/industry/article/806588464/cyber-attacks-is-the-gcc-prepared/2018-04-03
22. Government.ae. (2018, Dec 16). *National Cyber Security Strategy of the UAE*. Retrieved Mar 23, 2019, from https://www.government.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/national-cyber-security-strategy-of-the-uae
23. Dubai Electronic Security Centre. (2017). *Dubai Cyber Security Strategy*. Dubai: Government of Dubai
24. Dowle, C., & Fox, E. (2018, Dec 01). *Data protection in United Arab Emirates: overview*. (Rouse & Co International) Retrieved Mar 21, 2019, from Thomson Reuters Practical Law: https://uk.practicallaw.thomsonreuters.com/0-518-8836?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1#co_anchor_a883251
25. Aboul-Enein, S. (2017). *Cybersecurity Challenges in the Middle East.* Switzerland: Geneva Centre for Security Policy .
26. DarkMatter. (2018). *Cyber Security Report (Nov 2018).* UAE.
27. European Commission. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Brussels.
28. Symantec. (2017). *2017 Norton Cyber Security Insights Report - Global Comparison*. Retrieved Mar 23, 2019, from https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-comparison-uae-en.pdf
29. Symantec. (2016). *Internet Security Threat Report-Government.* USA: Symantec Corporation World Headquaters.
30. Guven, H. (2018). *The State of Cyber (In)security in the United Arab Emirates.*

AUTHORS PROFILE

Dr. Geetanjali Chandra, has completed a successful stint of more than 16 years of teaching in Higher education sector in India and abroad along with NGO, Court Practice for almost 8 years. In 2011 re-located to offshore campus Amity University Dubai. She has worked in diverse roles ranging from Head of Law Program, Faculty of Corporate Laws and Management Sciences, Curriculum Developer and Mentoring. She is actively involved in research and associated member of University Board of studies active member of representing team among Accreditation agency like WASC, IACBE, BCI.
Presented papers in International & National forums like; Inpalms, AALCO, (ICRC) International committee of red cross, Indian society of International Law, Indian Law Institute New Delhi, Indian Social Institute New Delhi, Conducting workshop on legal literacy, advocacy, on Intellectual property and Consumer Rights. she started an "Amity Law Journal" as Editor in Chief with International Indexing Serial Number for Amity University Dubai. Her research encompasses Sustainability Women rights social and ethical responsibility of Business, Islamic Economy.She authored Book on "Public Interest Litigation And Environmental Protection" 2005 (ISBN : 8176297046.), contributed chapters in Book., Published Research papers, Case study like Halal tourism , Halal cosmetics, free zones in UAE in case Centre(ECCH) Entrepreneur like "Filli Café" with Ivey Publication which is featured in Harvard Business Review in 2019.

Dr. Bhoopesh Kumar Sharma, is an Assistant Professor and Programme Head, Forensic Science at Amity University Dubai with 14+ years of experience in Teaching, Research and project supervision in various areas of Forensic Science including fingerprints, questioned document analysis, ballistics, and crime scene investigation. He has solved a large number of civil and criminal cases and given Forensic opinion in Indian and abroad court cases in various areas like Handwriting, signature, Bank Frauds Investigation, thefts, murder mysteries, etc. Have presented and published many Research Papers in National and International Conferences / Seminars/ Workshop/Journals of repute.

Iman Ali Liaqat, student at Department of Commerce at Amity University Dubai. She has presented and published many papers in national and international conferences. Her major research area is blockchain, artificial intelligence and halal economy.