

إشارات Esharat

Dedicated to a safer cyberspace

THE FUTURE OF CYBERSECURITY



DESC POLICIES ENSURE
PROTECTION

5G PROMISES UNPRECEDENTED
SPEED

TIPS FOR HEALTHIER TECH
HABITS



IS YOUR TWO-FACTOR AUTHENTICATION (2FA) ENABLED?

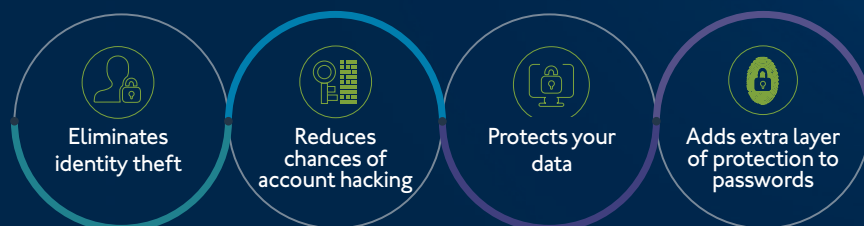
2FA adds an extra layer of security to your online accounts. It eliminates the risk of having your account hacked, even if your password has been discovered. You can activate 2FA for all your online accounts quickly and easily in the SETTINGS function. The next time you want to access your account or make important transactions, you will be asked for confirmation in two steps:

Step 1 – You will be asked to enter your password

Step 2 – You will be asked for the unique one-time confirmation code or pin (OTP) sent to your mobile phone number or email address

You will need both these factors to access your account details online. Quite simply, that makes you twice as secure!

Benefits of 2FA:



#Awareness_is_security



A magazine specialised in cyber security and technology, issued by Dubai Electronic Security Center

Director General

Yousuf Hamad Al Shaibani

Managing Editor

Amer Sharaf

Editorial Secretary

Shaikha Essa

Maitha Khalid



www.desc.dubai.ae

Editorial and Design



7G MEDIA

Editorial Board

Amani Abuseedo

Mary Jane Botha

Ahmed Mersal

Nicole Rehbane

Design and Production

Sree E S

Yasmeen Almonayyar

Illustrator

Akhila Sekhar

To contact the magazine:

DESC: +971 4 251 2538

7G Media: +971 4 449 5427

info@desc.gov.ae

info@7gmedia.com

All content provided by Esharat magazine is for informational purposes only. Although every reasonable effort is made to present current and accurate information, Esharat makes no guarantees of any kind and cannot be held liable for any outdated or incorrect information.

Copyright 2019. All Rights Reserved

DESC leads strategic collaborations to secure our robust cyber future



INSIDE

- 2 DESC SUPPORTS SHEIKH MOHAMMED'S 8 STRATEGIC PRINCIPLES
- 4 DESC ENSURES GOVERNMENT WEBSITES ARE SECURE BY DESIGN
- 6 CYBER RESEARCH AND INNOVATION IN DUBAI POWERED BY DESC SUPPORT
- 9 SMART TIPS FOR SAFE MOBILE PHONE PAYMENTS
- 10 DESC NEWS
- 12 DESC PROMOTES AI ADVANCEMENTS TO MAKE CYBERSECURITY SMARTER
- 15 HACKING FOR GOOD CYBER HEALTH
- 18 5G IS THE LATEST GENERATION OF CONNECTION TECHNOLOGIES - GET SET FOR SPEED!
- 22 DESC HOLDS AN UMBRELLA OVER GOVERNMENT DATA IN THE CLOUD
- 24 CYBERSECURITY WORLDWIDE NEWS
- 26 DIGITAL IMMUNITY ECOSYSTEM & DNA DIGITAL STORAGE COMING SOON TO DUBAI!
- 28 ENCOURAGING THE YOUTH TO CARVE A CAREER IN CYBERSECURITY
- 32 HEALTHIER TECH HABITS

This has been a year of great strides and significant achievements in the rollout of the Dubai Electronic Security Center (DESC) Cyber Security Strategy. In our journey towards the vision of His Highness Sheikh Mohammed bin Rashid Al Maktoum to make this the safest city in cyberspace, the continuously accelerating pace of technological development in 2019 has driven DESC's initiatives forward at speed!

Through its strategic partnerships, DESC facilitates world-leading opportunities for the cutting-edge research, development and launch of future-oriented innovations that will ensure a secure cyberspace. Our mandate is to support government, and semi-government entities and entrepreneurial talents so that they can safely accelerate their work in realizing Dubai's vision for the economic, social and scientific achievements of tomorrow.

DESC's recently launched 'Cyber Think Tank' is the first of its kind in the Middle East. The initiative is built upon the Center's core strategy, which includes high-level collaboration to brainstorm solutions for electronic security challenges. Among DESC's other significant partnerships, the IEEE UAE Cyber Intelligence Summit, the HITB+ CyberWeek, and the launch of academic cyber-research labs at leading national universities are just some of the initiatives that reflect our open-minded embrace of innovative technological progress in the development of cybersecurity solutions.

The Center is highly tuned to the futuristic cybersecurity opportunities presented by technologies like artificial intelligence, in which deep learning and natural language processing is being used to greatly enhance the capabilities of humans. Penetration testing conducted by the DESC Crisis Response Department simulates approaches that could potentially be used by hackers to breach government public domains, and these are further protected by DESC's cybersecurity policies, some of which are the Web Security Policy and the Cloud Service Provider Security Standard.

Raising awareness of cybersecurity is essential to the success of the Cyber Security Strategy. An informed society is a secure society, equipped to be alert for cyber risks. Esharat magazine supports DESC's goals by sharing knowledge with you, our reader, about the latest in information technology and the ever-shifting virtual landscape that the Center patrols.

This new era of technology is not simply about sophisticated gadgets or the latest virtual experiences. It is about our human story and about how we can use these high-tech innovations, safely and securely, to carve a progressive, stable and prosperous future – not just in Dubai and the UAE but contributing to the journey of all humanity.

Yousuf Hamad Al Shaibani
Director General
 Dubai Electronic Security Center



DESC SUPPORTS SHEIKH MOHAMMED'S 8 STRATEGIC PRINCIPLES

The strategic planning and focused activities of Dubai Electronic Security Center (DESC) are in accordance with the eight defining principles of governance in Dubai, as laid out in January this year by His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice-President and Prime Minister of the UAE and Ruler of Dubai.

The significant declaration marked 50 years of Sheikh Mohammed's wise and visionary leadership in service to the country. His Highness said that the eight principles were the ones upon which Dubai was founded and has always been governed.

"These principles ensure the well-being of our people, the sustained progress of our nation and the welfare of future generations," Sheikh Mohammed said. He called on future generations to preserve these principles and also called on all those in a position of responsibility in the Emirate to abide by the principles and ensure their implementation.

DESC's Cyber Security Strategy is built upon the foundations of Sheikh Mohammed's vision and protects Dubai from risks, thereby supporting the growth of the city and its economy.

Through its commitment to securing the cyberspace in Dubai, DESC abides by the directives of Sheikh Mohammed and his strategic principles. An open and trusted cyberspace provides value for all individuals, public and private sectors. It reduces barriers to trade as well as between countries, communities and citizens, and allows secure information sharing across the globe.





Sheikh Mohammed's 8 STRATEGIC PRINCIPLES

1. THE UNION IS THE FOUNDATION

Dubai is an integral part of the UAE and a pillar of the federation. The Emirate's destiny is entwined with the UAE's destiny, its well-being is vital to the UAE, and its people are ever-willing to sacrifice for the greater good of the country.

The Union's interest is above local interest, the Union's laws transcend our laws and legislations, the Union's policy is our policy, and the Union's government priorities are our government's priorities.

2. NO ONE IS ABOVE THE LAW

Justice is the basis of a strong and proud nation and it guarantees prosperity and stability. No one is above the law in Dubai, starting with the ruling family. The law does not discriminate between citizens and residents, rich and poor, male and female, Muslims and non-Muslims. Justice delayed is justice denied. Injustice anywhere is a threat to justice everywhere.

3. WE ARE A BUSINESS CAPITAL

The Government of Dubai aims to improve the lives of its people by strengthening its economy. Dubai does not invest or involve itself in politics and does not rely on politics to ensure its competitiveness. We extend a hand of friendship to all those who hold good intentions towards Dubai and the UAE. Dubai is a politically neutral, business-friendly global hub that focuses on creating economic opportunities.

4. THREE FACTORS DRIVE GROWTH

Dubai's growth is driven by three factors: a credible, resilient and excellent government; an active, fair and open private sector; and public and government-owned flagship companies that compete globally and generate income for the government, jobs for its citizens and assets for future generations.

5. OUR SOCIETY HAS A UNIQUE PERSONALITY

Our society is a respectful and coherent one, bound by tolerance and openness.

It distances itself from all forms of discrimination and bias. It is a disciplined society, committed to its promises, timelines and covenants. We are modest about our successes, perseverant in dealing with challenges, charitable and generous in achieving the greater good, and open to everyone.

6. WE BELIEVE IN ECONOMIC DIVERSIFICATION

Economic diversification has been the foundation of our unwritten constitution in Dubai since 1833. The changing times and the rapid developments make our commitment to this principle everlasting. Our new goal is to create at least a new economic sector every three years that will be productive, contribute to our GDP and generate jobs.

7. A LAND FOR TALENT

Dubai has always relied on talented tradesmen, administrators, engineers, creatives and dreamers for its success. The Emirate's prominence, sustainability and competitiveness depend on its capacity to continue attracting skilled and talented people, and nurturing the brightest minds to generate innovative ideas. We have to continually review and renew our policies and procedures to ensure our appeal to talented individuals. We must build the best environment in Dubai for the world's leading minds.

8. WE CARE ABOUT FUTURE GENERATIONS

The destiny of our future generations must not be affected by the fluctuations of regional politics and global economic cycles. We invest in and create valuable assets for them. Our fundamental rule in this regard is that the government should, under all circumstances, own economic assets that are worth at least 20 times the value of its annual budget.

We work towards maintaining a secure future, and we are focused today on ensuring the prosperity of our future generations. 🇦🇪



DESC ENSURES GOVERNMENT WEBSITES ARE **SECURE BY DESIGN**

Esharat interviewed Dr Bushra Al Blooshi, Head of Research and Innovation Department at DESC to find out about the Dubai Electronic Security Center's (DESC) Web Security Policy. Introduced in 2019, it ensures

that government websites are shielded from cyber risks by providing them with controls they can apply right from the start, and with which developers can establish secure foundations to their digital architectural designs.

Dr Al Blooshi explained that in today's always-on digital world, it is especially critical for government entities to take a proactive approach to securing their website-based data and cyber assets. The latest websites can equip digital developments and other plugins, so it is critical for web security to place a protective net over a much wider range of internet-related products and services. Mobile applications, web applications, application programming interfaces (APIs), coding standards, security testing and public information domains now accompany websites in requiring increased resilience against cyber hostilities.

Dr Al Blooshi said that the Web Security Policy was developed specifically to assist and support Dubai governments in achieving peak levels of holistic cybersecurity. However, the Policy also serves as a guideline to highlight the principles of web



Dr Bushra Al Blooshi, Head of Research and Innovation Department at DESC

security that any organisation or developer should responsibly follow.

“The essential aim of the Web Security Policy is to reduce the number of cyber vulnerabilities in the public-facing digital communication channels of government entities,” Dr Al Blooshi said.

“Rather than discovering vulnerabilities in a web-based product once it has already been developed, DESC has provided a set of controls that developers (whether internal or outsourced) can apply from the beginning.”

Within the realm of the Web Security Policy, various web security principles apply, depending on whether the product is being developed in-house or by an external provider, is being procured or is based on an existing solution (in which case a risk assessment will be conducted and mitigating controls applied).

WORKING TOGETHER TO SECURE DUBAI

While the Web Security Policy is not compulsory for now, compliance is included in DESC's evaluation systems. Dr Al Blooshi explained: “Government bodies have been given a year in which to implement the policy, as most already had existing or legacy websites. DESC always prefers to offer its clients incentives to utilize its best practice guidelines and policies, rather than to coerce them.”

Adoption of the policies provided by DESC are among the Key Performance Indicators (KPIs) included in the Dubai Government Excellence Programme. The annual DGEP Awards acknowledge and reward exceptional government employees, departments and initiatives, and are a highly prized level of recognition.

DESC's overarching Cyber Security Strategy aims to provide integrated protection from the challenges and risks that accompany technological progress and the smart transformation of Dubai. Holistic support for innovation in the field of cyberspace also supports sustainable development and economic prosperity.

MAIN STRATEGY DOMAINS

The Strategy encompasses five main domains in which DESC works to achieve its mandate of a cybersecure Dubai:

-  **CYBER SMART SOCIETY** – Achieving awareness, skills and capabilities for public and private sectors and individuals
-  **CYBERSECURITY** – Putting controls in place to protect confidentiality, integrity, availability and data privacy
-  **INNOVATION** – Promoting research and development for cybersecurity, and establishing a free, fair and secure cyberspace
-  **CYBER RESILIENCE** – Ensuring the continuity and availability of IT systems
-  **COLLABORATION** – Establishing national and international cooperative relationships to manage cyber risks


Implementation of the Web Security Policy and its supporting guidelines forms an important part of DESC's Cyber Security Strategy and, thus, contributes substantially to the overall vision of Sheikh Mohammed bin Rashid Al Maktoum, Ruler of Dubai,

positioning the emirate as a world leader in innovation, safety and security.

APPLICATIONS AND REQUIREMENTS

The Web Security Policy is applied to the following four fundamental elements of cybersecurity:

- Website security
- Security of web applications
- Security of mobile applications
- API security

Among the other requirements outlined in the Web Security Policy are those that oversee authentication and identity management, authorisation/access control, site configuration, data storage, encryption, logging, error handling, the hosting server, client storage and third party libraries, among other aspects of complete web security. 

 The essential aim of the Web Security Policy is to reduce the number of cyber vulnerabilities in the public-facing digital communication channels of government entities 





DESC cyber research laboratories

CYBER RESEARCH AND INNOVATION IN DUBAI POWERED BY DESC SUPPORT

The most impactful discoveries and innovative inventions have emerged from intensely focused minds collaborating together in close quarters... such as the DESC-funded cyber research laboratories at leading UAE universities.

Innovation and the promotion of cybersecurity research and development is one of the main domains of Dubai Electronic Security Center's (DESC's) Cyber Security Strategy. The Center supports the UAE's scientific community through research grants and other funding in their pursuit of technologically advanced ways to ensure that the emirate's cyberspace is amongst the safest in the world. Two 'Cyber Labs' – one at the University of Dubai and another at the University of Sharjah – were launched early this year and are hard at work, with a third – at Khalifa University – already in the pipeline.

Dr Bushra Al Blooshi, Head of Research and Innovation Department, said that DESC is a front runner among UAE public

organisations in its approach to research and scientific collaboration, which is also one of its chief strategic principles to cybersecurity.

"Many other government and federal entities visit us to learn from our research journey and how we develop our relationship with academic bodies. Initially, we launched a competition in which we called for ideation. The response, from both inside and outside the UAE, was excellent and the research ideas were of such a high international quality that it was decided the initiative could be expanded and formalised.

"The initiative is open to research proposals from universities, industry or other entities, with the criteria that the outcome needs to be applied, not just theoretical, and is intended to have a positive impact on cybersecurity in Dubai. This, in turn, will have an impact on the future economy of the UAE.

"DESC cannot give researchers the opportunity to work here due to the



DESC CYBER
INTELLIGENCE
LAB



DESC/UNIVERSITY OF DUBAI LAB - Prof Sameera Al Mulla, co-leader of the DESC Cyber Intelligence Lab, strategises with research assistant Carl Biron, and researchers Mohammad Wael and Ammar Ahmad



extreme sensitivity of our data, so instead we are providing opportunities at university research level,” she explained.

Dr Al Blooshi said DESC held regular meetings with the Cyber Lab teams, following up on their outputs and ensuring their further development with stable results. Outputs and findings are tested on a minimum of two government entities before they are considered for implementation.

DESC/UNIVERSITY OF SHARJAH: BYTE LAB

In January this year, the University of Sharjah and DESC launched the 'Byte Lab' to investigate security screening for the rapidly increasing number of Internet of Things (IoT) devices, along with research into blockchain, artificial intelligence and other cyber-related fields.

The research laboratory was inaugurated by His Excellency Yousuf Al Shaibani, Director General of DESC, together with His Excellency Prof Hamid Al Naimiy, Chancellor of the University of Sharjah. Speaking at the ceremony, HE Al Shaibani expressed DESC's support for the laboratory and said its scientific research outcomes would reflect Dubai's goal of being a leader in the field of secure digital development and the implementation of secure IoT initiatives.

The Byte Lab team is led by Prof Qassem Naser, Dr Manar Abu Talib and Dr Bushra Al Blooshi, with teams of researchers at Master's and PhD levels from scientific and engineering programmes. Dr Al Blooshi also stressed the significance of DESC's support for the scientific community and its funding of applied research projects that served government organisations and aid in the development of scientific innovations.

One of the Byte Lab's chief projects is the IoT Testbed, which Prof Naser and Dr Talib have been working on since 2016. Their research summary explains that authentication of smart devices and establishing trust for critical infrastructure plays a vital role in the realisation of



HE Yousuf Al Shaibani, Director General of the Dubai Electronic Security Center (DESC) and HE Prof Hamid Al Naimiy, Chancellor of the University of Sharjah, together inaugurated the cyber research-related Byte Lab in January 2019.

the IoT. Using the testbed, the team can investigate security and privacy issues in sets of IoT devices through experiments such as penetration testing and vulnerability scanning.

The work of the Byte Lab will contribute substantially to DESC's holistic welfare of Dubai's IoT network, which is set to grow rapidly and be increasingly enabled through the implementation of 5G technology in the near future.

DESC/UNIVERSITY OF DUBAI: CYBER INTELLIGENCE LAB

The University of Dubai, in collaboration with DESC, officially opened the Cyber Intelligence Lab in October 2018. The chief research focus of the lab is on securing Dubai's Industrial Control Systems. These are all the smart systems controlling devices around the city, which are, at times, connected to the internet.

Talking about the Lab, Prof Sameera Al Mulla, one of the Cyber Intelligence Lab leaders, said the team analysed all online traffic to their networks, generating

DESC is a front runner among UAE public organisations in its approach to research and scientific collaboration



beneficial data that includes reports of suspicious Internet Protocol (IP) addresses. .

"We analyse all malware, such as viruses, and identify those that are trying to target critical infrastructure in the city. We are now working on integrating artificial intelligence (AI) into our processes through machine learning, which can immediately identify threats in network traffic," Prof Al Mulla added.

The DESC Lab is considered to be a leader in this field, pioneering the development of AI with increased capabilities to recognise and assess suspicious internet activity, helping to protect Dubai from infrastructure attack. The challenging project is divided into several

fields that involve the dark net, big data and machine learning.

Prof Al Mulla also praised DESC for enabling postgraduate student internships at the Lab, the benefits of which are twofold: they provide helping hands for the research work plus they give students the opportunity to join, learn, assist and support the work.

"DESC is always on the lookout for skilled national graduates. The Cyber Lab internship programme is a good way to discover the potential of students, to develop their knowledge and enhance their learning process.

"Students are excited and encouraged to join UD because of the labs. What DESC is doing is rare; having a government entity invest in research is an important step towards the UAE's development," she said. ■

Students are excited and encouraged to join UD because of the labs. What DESC is doing is rare; having a government entity invest in research is an important step towards the UAE's development ■



DESC CYBER
INTELLIGENCE
LAB





SMART TIPS FOR SAFE MOBILE PHONE PAYMENTS

Banking has come a long way since people paid their way with wads of cash. These days, just a click or a tap of a smartphone can cover the grocery trolley at the till, pay the monthly accounts, shop online, transfer investments and much more. Fintech is super convenient – so let's make sure your smartphone payments are super secure too.



USE ONLY SAFE PAYMENT PLATFORMS

Trustworthy mobile payment platforms do not store your credit card details after the transaction. Fraudulent payment apps are usually designed especially to gather and use your financial information, so be extra cautious about using third-party or downloaded apps.

NEVER FOLLOW LINKS TO YOUR BANKING SITE

It is not safe to click on email or SMS links. 'Phishing' communications are designed to look like they come from your bank, but their click connections will take you to a phony site that grabs the login information you innocently provide. Also, never provide numbers or passwords in response to an email or SMS. Your real bank will never request that of you.

STRONG PASSWORD PROTECTION IS YOUR SHIELD

Set your phone to lock automatically and

create a strong password to protect your mobile and the information stored within. Use any technologically advanced security features your smartphone may offer, like fingerprint or face recognition.

LOCK YOUR LOST OR STOLEN PHONE REMOTELY

Be sure to activate Find My iPhone or Find My Device for iPhone or android phones, respectively, to locate or remotely wipe your devices if they get lost or stolen. Even if you never get your phone back, at least your information will stay safe.

PUBLIC WI-FI IS NO PLACE FOR SECRETS

Never send sensitive information through public wi-fi. Open internet connections, in places like malls and coffee shops, are accessible to everyone else who logs in. Your data is at greater risk of being exploited when making online purchases or transfers on public wi-fi networks.

DOWNLOAD YOUR BANK APP

Actually, it is even safer to download your bank's specially developed mobile application for use on your phone than it is to use the browser. Be sure to say yes to regular software updates – these will keep your system safe from any new malware or software glitches.

ENABLE ONE-TIME PINS

All of your banking transactions should provide double protection by requiring that you enter an OTP (one-time pin or password) sent to your registered phone number in addition to your login details. Even if your password is cracked, payments cannot be authorized without the OTP.

LOOK AFTER YOUR PHONE!

Not that anyone is careless on purpose, but, really, now that our phones have become so much more than just clever walkie-talkies, it is essential that we all take extra care with them. Keep yours locked, keep it with you and do not lend it to anyone you don't know and trust. 📱

DESC AWARDS 'INNOVATION IN CYBERSECURITY RESEARCH' GRANT

In February this year, Dubai Electronic Security Center (DESC) named the two winners of its sought after 'Innovation in Cybersecurity Research' Award: Khalifa University and University of Sharjah. The total AED700 000 research grant supports the UAE's drive to build a knowledge- and innovation-based economy.

At the prestigious award ceremony, attended by university directors, cybersecurity researchers and industry experts, Dr Marwan Al Zarouni, DESC Director of Information Services, emphasized the importance of innovation as a cornerstone of the country's social and economic development and the execution of DESC's strategies and frameworks.

In May 2017, His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE and Ruler of Dubai, launched the Dubai Cyber Security Strategy with innovation at its heart and the vision of establishing Dubai as a global leader in innovation, safety and security.

"We believe in the vital role of research and development in advancing innovation and hope that this honour will be a strong motivation for all researchers and innovators to widen their perspectives and strengthen their interest in the vast world of cybersecurity research," Dr Al Zarouni told the audience.

More than 70 researchers and students from over 20 national and international universities competed for the grant, with 14 high quality research proposals ultimately shortlisted.



Dr Al Zarouni said: "DESC highly appreciates the tremendous efforts invested by the researchers into the competition. We are pleased to congratulate the winning teams and confident that this award, as DESC's primary initiative, will contribute in safeguarding the digital wealth of Dubai. This, in turn, enhances the vision of our wise leadership by making Dubai the safest city in the world."

Groundbreaking Research Proposals

The grant was open to proposals from researchers in accredited higher education institutes within the UAE as well as internationally, with a particular focus on cybersecurity.

The winning research team from Khalifa University investigates "Energy efficient, secure IoT (Internet of Things) hardware for smart cities". The proposed research from the other winning team, Sharjah University, aims to design a "High-speed microplasma-based true random bit generator for real-time encryption."

Moreover, other proposals encompassed diverse cybersecurity-related areas such as digital forensics, threat intelligence, mobile security, big data, blockchain, and autonomous vehicle security.

FOSTERING DISRUPTIVE CYBERSECURITY AT OPCDE CONFERENCE



As part of its mission to curb cybersecurity threats, Dubai Electronic Security Center (DESC) co-hosted OPCDE, a high-end technical conference attended by some of the world's foremost cybersecurity specialists.

Top speakers at the April 2019 event included experts who shared insights on the latest research, threats and trends in securing the digital world. The name 'OPCDE' reflects the industry term 'operation code', the binary words used to instruct computers.

In his keynote address at the event, Dr Marwan Al Zarouni, Director of Information Services at DESC, said the event helped to raise public awareness about risks and the important role of security in the digital age, as well as the growing demand in the market for cyber education and training.

"It is important to empower the next generation of digital talent and equip them with the necessary technical skills. Events like these help us to realize the Dubai government's efforts in building a secure and resilient cyber space," Dr Al Zarouni emphasized.

Matt Suiche, founder of OPCDE, said the event was another successful milestone for Dubai's local ecosystem, nurturing a strong local talent pool in order to become a global hub of cybersecurity innovations.

DESC HIGHLIGHTS LATEST DEVELOPMENTS IN CYBERSECURITY AT GISEC 2019

For the second consecutive year, Dubai Electronic Security Center (DESC) participated in the Gulf Information Security Expo and Conference (GISEC), held at the Dubai World Trade Center in April.

GISEC is the largest annual information security event in the Middle East, attracting international cybersecurity experts, 170 exhibiting companies from 86 countries, and more than 12,000 visitors. This year, DESC highlighted the latest developments and practices in cybersecurity, as well as initiatives geared at making Dubai's cyberspace the most secure in the world.

Among other contributions to the event, DESC exhibited a password interactive screen that tested the strength of individuals' online

security by indicating the estimated time it would take the computer programme to exploit the password, ranging from only seconds to a couple of thousand years.

"Cyberattacks are getting more sophisticated and disruptive, posing a great risk to the growth of the digital economy and smart infrastructures. Each year at GISEC, we outline the latest cybersecurity practices, correlating these with emerging technologies to scale up safety and, in turn, establish trust in our cyberspace. Our main priority is to protect Dubai against cyberthreats by securing privacy and data,



and safeguarding Dubai's digital wealth," noted Amer Sharaf, Director of Compliance Support and Alliances at DESC.

DUBAI 'CYBER THINK TANK' LAUNCHED

Dubai Electronic Security Center (DESC) has launched an innovative 'Cyber Think Tank', the first of its kind in the Middle East, to brainstorm ideas, conduct research and design solutions to assist in the fight against current and future cyberthreats.

The pioneering initiative was launched in October 2019 and will include regular meetings and interactive, high-level focus groups with participating public and private sector entities. Jassim Mohammed, Security Operations Manager at DESC, said: "The priorities of the platform include confronting and resolving the current and future cyber challenges and risks, as well as contributing to the development of proactive policies and frameworks for the cybersecurity of Dubai".

At the end of every edition, the platform will develop a detailed report including the results of all scientific research and studies, which will help to develop future cybersecurity strategies, policies and methodologies for public and private organisations. These will be based on recommendations culminating from the research findings.



Jassim Mohammed highlighted that the Dubai Cyber Think Tank initiative is driven by DESC's core strategy, which includes strategic partnerships with government entities and organisations in Dubai to define and confront cyberthreats and challenges.

"These initiatives help us to make remarkable progress in realising Dubai government's vision for developing and carrying out initiatives and policies that aim to solve electronic security challenges and build a secure and resilient cyberspace for the city and the United Arab Emirates," he added.



AI TECHNOLOGY REDEFINES CYBERSECURITY

Artificial intelligence (AI) is boosting the capabilities and controls of cybersecurity professionals in powerful and exciting ways.

Dubai Electronic Security Center (DESC) places innovative technologies and development at the forefront in its mission to establish the city as a global leader in digital security, thereby achieving the vision of His Highness Sheikh Mohammed bin Rashid Al Maktoum and ensuring a free and secure cyber world that fosters the best of new age innovation.

In the words of H.E. Yousuf Al Shaibani, Director General of DESC: "The vision of our leadership is not only planning and readiness for the near future, but also focuses on the importance of developing strategic plans and solutions that meet the needs of Dubai and the position it occupies among the cities of the world for decades to come".

Al Shaibani explained that AI technologies are developing in quantum leaps as this century advances. Machine learning, cognitive computing and other AI innovations are increasingly being put to use in the cybersecurity sector, supporting the capacity of human security operations and enabling them to respond to threats faster and more efficiently than ever before.

LEARNING - AI 'feeds' off trillions of bits of data, coming from a vast range of sources, growing more effective with each new experience. It is through machine learning and deep learning techniques that AI gains immense knowledge about cyberthreats and can quickly process effective responses.

REASONING - Using the insights and knowledge it has accumulated, AI is able to analyse and recognise threats such as malware, malicious files or other suspicious activity within seconds. This speed and precision is vital in a world where criminals are also employing modern technologies to launch their cyber attacks.

ENHANCING - Cognitive machines provide significant support to cybersecurity teams, augmenting their roles by ceaselessly performing time-consuming research and analysis of billions of logs of data. By continuously classifying, detecting patterns, predicting attacks before they occur, and providing humans with relevant, accurate information, cybersecurity AI speeds up the time it takes for security specialists to make critical decisions and respond to threat conditions.

STRENGTHENING HUMAN CAPACITY

Machine learning enables computer systems to create algorithms based on the data it receives, so it can quickly recognise patterns and also irregularities that could signal a problem. Cognitive computing describes machine learning that applies data to build systems that simulate human thought processes. Instead of being specifically programmed, this AI gains better 'understanding' from every new interaction with its environment.

Cognitive security is a leap ahead because it combines the best of artificial intelligence and human intelligence. Using deep learning, machines build on their vast body of knowledge, getting smarter and better at proactively detecting and analysing cyberthreats, and making it easier for security analysts to take decisions and action. So, AI can be employed to perform extremely time consuming and monotonous tasks with more speed and accuracy than humans.

In fact, these are the type of jobs in which AI is well suited. Computers don't get tired or bored. Their excellent large-scale data analysis and anomaly detection skills are scalable ways to strengthen human efforts and enhance the cybersecurity of an organisation.

AI APPLICATIONS

Threat hunting is one example of a cybersecurity area in which AI is valuable, because it involves trawling through massive amounts of data to spot any vulnerabilities, risks or threats to an organisation's IT infrastructure. It would be almost impossible for a human to perform this preventative



H.E. Yousuf Al Shaibani, Director General of DESC and Honorary Chair of the IEEE Cyber Intelligence Summit

cybersecurity service with the same consistent focus, speed and accuracy as a cognitive machine.

AI and machine learning is being implemented to make a positive impact on cybersecurity in numerous other innovative ways too, such as the following:

BIOMETRIC PROTECTION

Biometric authentication, such as facial or fingerprint recognition, has been introduced as an alternative to password security, since these are vulnerable to hacking. The system is not always perfectly secure or convenient, however, as cited in Forbes magazine and by industry experts, AI is now being developed to enhance biometric software for login access, making it safer and more accurate. The technology processes facial features by identifying key correlations and patterns, so it's near impossible to trick. It also works in different lighting conditions.

PHISHING PREVENTION

Phishing emails are a common method

of cyber attacks, with almost one in every hundred emails coming from hackers (zdnet.com). AI can scan networks, detect and react to thousands of active phishing campaigns within minutes. The machine learning system can also quickly differentiate between fake and genuine websites, providing fast protection at all levels. Some anti-phishing systems perform 'deep link inspections' by simulating clicks on all links in an email and examining the resulting pages for malicious activity.

BEHAVIOURAL ANALYTICS

Machine learning algorithms can study patterns in user behaviour by analysing how you usually use your device, your typical login times, the online platforms you visit, and even your typing and scrolling movements. Any behaviour that is different to your standard patterns will alert suspicion from the AI security system – like unusually fast typing or a sudden spike in document downloads. The AI will raise attention to its suspicions or even block the user if the

behaviour clearly points to hacking.

NATURAL LANGUAGE LEARNING

One of the most valuable AI-powered advances is that of 'natural language processing', through which systems can collect data by scanning articles, dark web conversations and news to build knowledge and predict and prevent cyber attacks. This helps cybersecurity operations to calculate risks, stay updated on the latest cybercrime techniques and prepare effective security strategies. Natural language processing is also used in email protection with machines that check if the word choice, grammar and spelling are cause for suspicion.

AUTOMATED NETWORK ANALYSIS

The amount of data constantly flowing through networks is massive – too much for efficient human capabilities. However, most malware and cyberattacks are launched over networks, so it is vital that these are kept secure via ongoing, rapid and careful analysis. AI systems use algorithms to match keywords,



monitor statistics and detect data that is even slightly different from the norm. This frees up human cybersecurity analysts to quickly respond when the AI signals threat alerts.

LIMITATIONS AND PROGRESS

Highly advanced AI-driven machines are sophisticated developments that require huge resources, such as computing power and precise datasets. Building and maintaining such systems and integrating them into mainstream applications will take some time and there are various challenges and limitations that cybersecurity engineers are working to solve. It will be a while before AI can become a standalone cybersecurity solution.

Al Shaibani explained, however, that AI is already supporting and enhancing the work of traditional professionals and, through continuous research and development, the technology is accelerating at speed. AI is also being integrated with other advanced technologies, such as blockchain, to ensure superior security protocols that will soon become essential in the cybersecurity arena.

DESC SUPPORTS AI RESEARCH AND COLLABORATION

Dubai Electronic Security Center (DESC) places innovative technologies and development at the forefront in its mission to establish the city as a global leader in

digital security. Al Shaibani said the Center contributes to research and development in the field through international and local engagement with leading academic and scientific institutions, thereby strengthening the Dubai Cyber Security Strategy and other pillars of technological leadership.



This year, 'AI and the Future of Cybersecurity' was the theme of the 2019 IEEE UAE Cyber Intelligence Summit, which DESC presented in partnership with TRA and IEEE for third consecutive time. The event was held on 14 November in Dubai.

The IEEE is the world's largest technical professional organisation for the advancement of technology. IEEE (pronounced Eye-Triple-E) is an acronym for the Institute of Electrical and Electronics Engineers. The non-profit group comprises engineers, scientists, software developers, information technology and other professionals. The IEEE UAE Section, established in 1987, is the organisation's official representation in the United Arab Emirates.

As well as being Director General of DESC, H.E. Yousuf Al Shaibani, is also Honorary Chair of the IEEE Cyber Intelligence Summit. He said the event was an important step towards achieving the Dubai Cyber Security

Strategy, which aims to promote cybersecurity research and development and establish free, fair and secure cyberspace in Dubai as well as influencing it on a global scale.

"We, at DESC, extend our great pleasure to partner with IEEE, one of the world's largest technical professional organisations. Our aim is to offer a forum where leading cybersecurity experts and researchers can engage in fruitful discussion, exchange ideas, and reflect upon the important possibilities of AI technology in the field of cybersecurity," Al Shaibani said. 

 Our aim is to offer a forum where leading cybersecurity experts and researchers can engage in fruitful discussion, exchange ideas, and reflect upon the important possibilities of AI technology in the field of cybersecurity 

PENETRATION TESTING: CYBER GUARDIANS OF DUBAI GOVERNMENT

The Crisis Response Department at Dubai Electronic Security Center (DESC) takes a skilled strategic approach to averting potential cybercriminal attacks on the government's computer systems – by simulating attacks on the system!

Penetration testing is a mandated service that enables the Crisis Response team at DESC to take on the role of white hat hackers to find and fix any vulnerabilities.

Imagine exposing yourself to germs on purpose – just to check whether your body is resilient enough to withstand the disease (and, if you do get sick, the quickest way to get healthy again)! This, very simply put, is what the work of penetration testing involves, except that the germs in this story

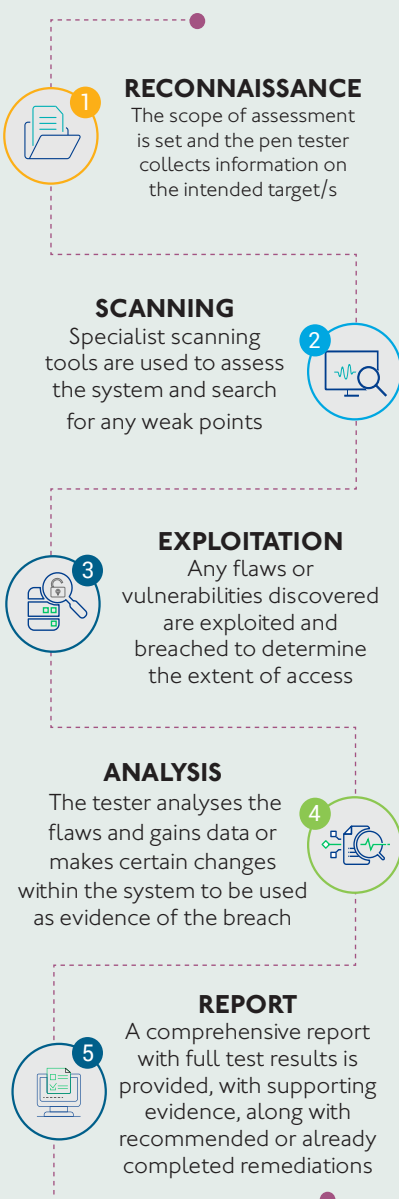
are digital and they are being launched against computer systems and networks.

Penetration testing (known in the cybersecurity field as 'pen testing') is an intentional simulated attack on a computer system that is designed to evaluate its level of security. By performing the test, cybersecurity experts can provide a full risk assessment that identifies any potential weaknesses in the system as well as its strengths.





A PENETRATION TEST COMPRISES A STEP-BY-STEP PROCESS OF RECONNAISSANCE, SCANNING, EXPLOITATION, ANALYSIS AND REPORTING:



Ahmed Al Hussain, Deputy Manager of DESC's Crisis Response Department

EXPERTLY GUARDING GOVERNMENT CYBER INFRASTRUCTURE

Ahmed Al Hussain, Deputy Manager of DESC's Crisis Response Department, explained that the team was formed specifically to assess and ensure the continuous security of all government entity systems linked to the interconnected digital technology of cyberspace.

"The service DESC provides, through the work of the Crisis Response team, includes penetration testing for mobile applications, web applications and internal network infrastructures."

Al Hussain explained: "As the number of digital systems within the government grew, so, too, did the need for a penetration testing service that would measure the effectiveness of the security measures implemented in these systems. DESC

established the Crisis Response Department to provide this vital service to all government entities as a way of ensuring that their computer systems, networks, web applications and mobile applications are properly secured. We assist these entities by securing their critical infrastructure – thereby achieving the vision of making Dubai the digitally safest city in the world."

"The penetration testing process involves the evaluation of security measures and mechanisms in scoped systems. The Crisis Response team is expertly trained and equipped with deep knowledge on how to assess any vulnerabilities they discover, reverse-engineer software applications and review the source code of an application."

WHITE HAT HACKING

What is the process involved in penetration testing? This security approach is sometimes referred to as white hat hacking, because it

is authorized and for productive purposes. The penetration tester takes on the role of a hacker and simulates a real attack. They will look for ways to break through the layers of security and invade the network, website or application – if they are successful, it means that a real hacker might be too!

In this way, penetration testing can provide a clear picture of where any cybersecurity flaws or weaknesses are in the system at the time of the test. With this knowledge, these vulnerabilities can be reinforced to enhance the security of the system.

Faisal Abdulaziz, Deputy Manager of DESC Security Systems Operations Department, explained that hackers are continually finding new ways to maliciously compromise the cyberconnected systems of governments, business and individuals, so penetration tests need to be performed on a regular basis. Cybersecurity experts, like those at DESC, are specially trained to be on the alert for any new techniques and technologies exploited by criminals, so that they can quickly step in to upgrade network defences where necessary.



Faisal Abdulaziz, Deputy Manager of DESC Security Systems Operations Department

MULTI-PRONGED APPROACH

There are various types and approaches to penetration testing that can be applied to ensure a full risk assessment:

WHITE BOX TESTING

In this approach the pen tester has full knowledge of the IT infrastructure, including IP addresses, system configurations and other credentials. Extensive white box testing involves in-depth analysis of processes and systems to assess the security of all underlying technology.

BLACK BOX TESTING

This form of pen testing involves taking on the role of a real hacker and the tester approaches IT infrastructure with minimal prior knowledge. All means of the latest hacking techniques are used to try to gain access into the network and systems, so that the tester can provide a full security evaluation and take steps to rectify vulnerabilities and block the possibility of criminal breaches.

GREY BOX TESTING

Grey penetration testing is a combination of the above two approaches, in that certain limited knowledge of the infrastructure and systems is shared with the tester.

SOCIAL ENGINEERING

Many of us can recall at least one type of social engineering hacking attempt – hopefully without falling victim to this type of exploitation. This approach involves direct fraudulent communications to try to compromise a system. Phishing is a common approach to such trickery, using emails or SMSes with phony messages that encourage people to click on malicious links. By doing so, users unintentionally download malware or expose their credentials (or those of their company), opening the digital door for exploitation. Penetration testers will take exactly such approaches, communicating directly with unwitting employees in an

attempt to breach an organisation's IT infrastructure. This will help the IT team to devise cross-checks and processes that can avoid any human vulnerabilities.

NETWORK PENETRATION TESTING

Network assessments are the most sought after and most complex form of pen testing. The tester will attempt to breach the organisation's network by launching attacks on infrastructure. These include firewall configurations and bypass possibilities, intrusion prevention system (IPS) evasion, domain name system (DNS) attacks, as well as attacks on the software running within the network, such as the Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP) and email login pages.

WEB APPLICATION TESTING

Where sensitive personal data, such as financial or health-related details, are located within a website or web-based application, penetration testing must address vulnerabilities on these systems. Depending on the design of the website or app and what it is used for, the tester will examine its components, software and coding.

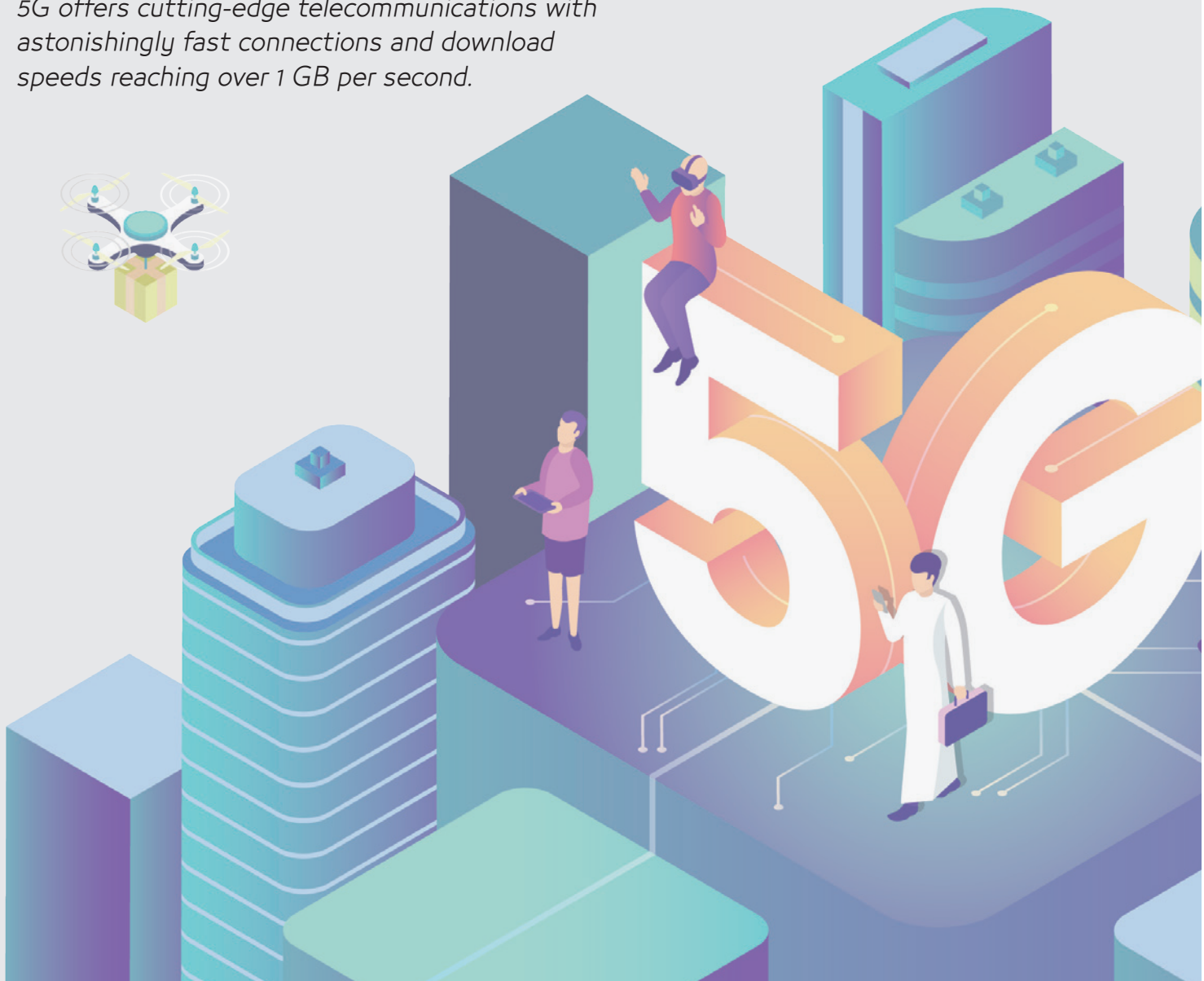
PROACTIVE PREVENTION OF CYBERCRIME

Depending on the scope of the audit, the size of the infrastructure and the number of devices and servers that are communicating with each other and the greater cyberspace, penetration testing can vary greatly in terms of time, cost and resources. However, with cybercrime taking a terrible toll on the world's economy, this targeted approach to cybersecurity is fighting back effectively and proactively protecting the integrity of government and private digital assets. 🇦🇪



5G IS THE LATEST GENERATION OF CONNECTION TECHNOLOGIES - *GET SET FOR SPEED!*

5G technology is here and it promises to make almost everything in our lives even faster. The next generation of mobile internet connectivity, 5G offers cutting-edge telecommunications with astonishingly fast connections and download speeds reaching over 1 GB per second.





How will 5G improve the quality of life, governance and business in Dubai? And what impact will it have on cybersecurity? Esharat explored this game-changing technology.

WHAT IS 5G?

5G is simply the latest way in which we connect to the internet. The 'G' refers to each 'generation' of wireless mobile telecommunications technology. A new G is launched approximately every ten years so, while 2G took us out of the age of dial-up in 1991, 3G connected mobile directly to the internet when it appeared in 1998, enabling apps like GPS. Then, in 2008, 4G arrived to give us greater bandwidth and even faster connections for easy streaming and social sharing.

5G, the next generation of mobile internet connectivity, is set to be around 20 times quicker than 4G. To put this into perspective, a full-HD movie that now takes hours to download will be seamlessly accessible with 5G in a matter of seconds.

HOW DOES IT WORK?

5G networks are anticipated to launch across the world by 2020, providing always-on, super quick connections wherever we are. Unlike 4G, however, which drastically improved connectivity without asking much of consumers, 5G technology will not simply upgrade our existing smartphones or other devices. It will require the purchase and installation of entirely new systems, including hardware and software. Until we

are all connected, 5G will work alongside existing 3G and 4G technologies.

5G technology will actually affect the way the internet works, by shifting to 'fixed wireless access'. Instead of connecting through a router, as wireless architecture does now, your home or office Wi-Fi will connect wirelessly to a larger network of connectivity.

Data that is required by always-on devices, such as those in a self-driving vehicle, will be stored near the edge of these networks to ensure quick connections.

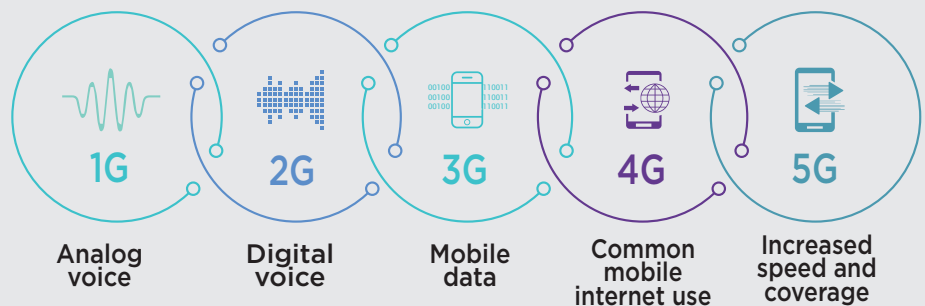
All wireless communication sends and receives data via signals carried on the radio (electromagnetic) spectrum, but 5G uses radio higher frequencies (millimetre waves) to achieve their speed and capacity. The high frequencies are shorter and experience more interference, so a great number of strategically positioned transmitter towers will be required.

WHAT ARE THE BENEFITS?

One word: speed! Essentially, 5G will connect like lightning and this development is what is going to impact so much more than just our movie downloads. 5G will be an important enabler for nearly all emerging technologies, such as the Internet of Things (IoT), autonomous vehicles and machine learning.

5G can also support LOTS of devices – a minimum of one million devices for every square kilometre! This sounds like overkill but, remember, these could

THE MOBILE EVOLUTION:





include everything from mobile phones to smartwatches, any vehicles in the area, all IoT machines and more, simultaneously demanding connectivity.

Some of these 5G uses are truly remarkable. Medical advancements include remote surgery, where a specialist surgeon in a hospital might be able to save the life of a child in a rural African clinic by live streaming and carefully instructing the work of the on-site doctor.

Traffic jams, even accidents, may become a thing of the past, as autonomous vehicles communicate with each other and synergize their speeds or routes to keep the flow moving smoothly.

Saleem AlBlooshi, chief infrastructure officer at Emirates Integrated Telecommunications Company (EITC), which also owns du, says that one of the main drivers of 5G has been the proliferation of video.

"5G will cater to high-definition viewing, such as 4K and HD viewing. This correlates with another driver for 5G: virtual reality and augmented reality," AlBlooshi said. These devices require vast bandwidth and connection speeds to help them achieve the 'real' experience for users.

Here are some of the general benefits we can expect from 5G:

- Almost instant access to online data
- Hardly any lag (low latency) when streaming (which is also great news for gamers)
- An explosion of innovative products that need ultrafast speeds
- Always on, always reliable internet everywhere
- Smart, cybersecure cities, transport, factories and infrastructure
- Cyberconnected vehicles and traffic controls
- Smarter AI-integrated healthcare
- Smarter farming with efficient

The launch of fifth generation mobile broadband services is in line with the UAE's Vision 2021 and will establish the country as a leader in 5G deployment

equipment producing better crops at lower cost

- Augmented reality communications, like 3D hologram conference calls, emails or documents that project into the space in a room, and floating TV monitors

WHEN WILL 5G BE AVAILABLE IN DUBAI?

We have become so accustomed to the incredible rate at which technological progress enters our lives that 5G's benefits will, no doubt, soon feel ordinary.

5G implementation is extremely costly and must be done securely. Regulatory approvals, network construction (including hardware like antennas, towers and wiring), as well as the availability of actual devices, all affect rollout.

There are currently very few locations in the world where 5G service is available

and it will probably appear in pockets, with the UAE likely to be one of the first areas in the world to benefit and certainly the first in the region. The Telecommunications Regulatory Authority (TRA) says the launch of fifth generation mobile broadband services is in line with the UAE's Vision 2021, and will establish the country as a leader in 5G deployment.

Both of the country's big telecom service providers, du and Etisalat, report that their infrastructure is ready for the new technology, but the wait is on for consumers as many manufacturers have yet to unveil their 5G-enabled products in the market.

Saleem AlBlooshi confirmed that du's "ongoing network revolution" was in full readiness to offer 5G, saying the technology would bring wireless communication speeds never before experienced, very low latency and massive capacity.

Ericsson's 2019 Mobility Report suggests that the growth of 5G traffic will be more rapid in the Middle East - around eightfold by 2024 compared to fivefold globally. This is largely due to the region's high video consumption, as well as the evolution of industries seeking to maximise efficiencies along with economic diversification strategies.

WHAT IMPACT WILL 5G HAVE ON CYBERSECURITY?

As with all technological progress, the tools that improve life also



help cybercriminals become more sophisticated, so security experts must continue to stay a step ahead. The number of 'attack surfaces' is constantly increasing, making us all more vulnerable.

Armin Wasicek, a 5G expert from AVG Internet Security, says the biggest 5G security concern will come with the growth of the IoT. A totally connected world is especially susceptible to cyberattacks. Even before 5G, hackers sabotaged appliances, but the potential is greater now for them to breach networks with disruptive actions that can do extreme harm. The threats are unprecedented, which is why cybersecurity experts conduct extensive research and employ white hats to find holes in the system.

5G technology also has the potential to spur entirely new industries and services, all of which will demand new levels of security. Automotive cyberattacks, for example, may rise as autonomous vehicles become more commonplace. Dubai Electronic Security Center (DESC) has foreseen this possibility and ensured multi-layered cyberprotection through its pioneering Cyber Security Standard for Autonomous Vehicles in Dubai in the near future, in cooperation with the Roads and Transport Authority (RTA).


Healthcare risks, including medical identity theft or data sabotage, will also require ever tougher cybersecurity

measures. Fortunately, DESC has foreseen these unprecedented challenges and developed targeted IoT and Biomedical Standards to provide greater levels of control. Generally, IoT devices and sensors, such as those used in smart homes, public and private organisation, will need increasingly complex authentication to prevent unauthorised access. Biometric identification, using voice, iris or fingerprint locking, may become standard and companies will need to continually monitor their security strategies.

WHAT'S NEXT FOR MOBILE TECHNOLOGY?

A slowdown in internet connections is highly unlikely and, as billions more devices connect to the web, infrastructure will need to keep developing to handle the traffic quickly and reliably. The natural progression is towards ever faster and more enhanced wireless connectivity.

Now, even before 5G has had its day in the sun, engineers are already working on its successor, 6G, which is likely to

launch around 2030. Connectivity – and interconnectedness – will be instant and almost permanent throughout the planet, creating a meeting of biology and artificial intelligence which Marcus Weldon of Nokia Bell Labs has described as “a sixth sense experience for humans and machines.” 





DESC HOLDS AN UMBRELLA OVER GOVERNMENT DATA IN THE CLOUD

The term 'cloud' computing had many people mystified when first it was introduced to the general public, but now most of us have grasped that 'cloud' is simply a metaphor for the internet... the virtual space that connects users all over the globe.



As much as this technology provides an innovative network for storing and sharing digital resources, the cloud also opens users to potential cybercriminal risks. Dubai Electronic Security Center (DESC) protects the cloud data of all Dubai government and semi-government entities through its Cloud Service Provider (CSP) Security Standard. The Standard lays out specific requirements, as well as guidance for organisations using cloud services, and compliance is mandatory for CSPs that provide cloud-related services to Dubai government clients.

First, let's clear the air by explaining how cloud works:

Did you know that you are probably already using the cloud? If you are on social media, if you ever watch music videos online or use

a webmail account... you use the cloud! Already, more data resides in the cloud than in all the world's data endpoints (like your PC or smartphone). By 2025, market intelligence company IDC forecasts, digital data generated worldwide will grow from 2018's 33 zettabytes to 175 zettabytes, half of which will reside in public cloud environments. How much?! Well, one zettabyte is equal to a trillion gigabytes – that's a LOT of data and it's growing daily!

Information in the cloud is stored on physical or virtual servers, which are maintained and controlled by cloud computing service providers responsible for ensuring that data is accessible and protected. As a personal or business user, you access data stored in the cloud via an internet connection.

There are three main strategies to deploying cloud computing, particularly for organisations:

- **PUBLIC CLOUD** – all data is kept in the service provider's infrastructure and resources are shared with other clients
- **PRIVATE CLOUD** – a private network with dedicated resources for a single customer; high levels of security and control
- **HYBRID CLOUD** – uses a mix of public and private cloud, depending on client needs

Cloud computing in the UAE

The UAE has taken the cloud adoption lead in the Middle East, fuelled by its vision of a digitally driven economy and non-oil diversification. This has created a technologically advanced ecosystem for government entities and businesses in diverse sectors, from finance to retail.

Dr Bushra Al Blooshi, Head of Research and Innovation Department at DESC, said the Center encourages emerging innovation and the implementation of new technologies, which contribute significantly to economic growth. However, its chief responsibility is to safeguard the integrity of Dubai's cyberspace and, most particularly, the data of the government.

"Our recommended approach to the cloud really depends on the sensitivity of the data," she explained. "If the data is intended to be readily available and open to anyone, then any public cloud service would be suitable. However, we advise government entities that, if they want to utilise cloud services, they need to do their research first. Data that is confidential or sensitive should remain in a safe, certified cloud environment in the UAE."

Cloud Security Provider (CSP) Security Standard

The CSP Security Standard produced by DESC sets out criteria against which suppliers can achieve certification to demonstrate their compliance. Dr Al Blooshi said



Amer Sharafuddin Sharaf, DESC Senior Director – Compliance Support and Alliances and Theuns Kotzé, Managing Director – BSI Middle East and Africa, signed an MOU at DESC headquarters, Dubai

DESC was the first UAE government entity to have implemented this kind of best practice for the internet. The Standard was developed on the basis of the internationally accepted certification scheme that is used for ISO/IEC 27001.

DESC aims to make the process as smooth as possible and applies global best practice standards so that only a few localised controls and minor audits are sufficient for leading providers to achieve certification.

Once certified, suppliers are considered compliant and free to conduct their business with government entities. Compliance audits are conducted annually by accredited certification bodies and a re-certification audit is required every three years.

DESC has partnered with the British Standards Institution (BSI), a global leader in the establishment of IoT and cybersecurity practices, to conduct audits against the CSP Security Standard, manage the certification process and issue certificates to suppliers. Amer Sharaf, Senior Director of Compliance Support and Alliances at DESC, said: "This collaboration with BSI advances our efforts towards preserving the digital future of

Dubai as well as implementing the best practices in the field of cybersecurity across the Emirate."

Theuns Kotzé, managing director of BSI Middle East and Africa, said the company recognised DESC's critical role in establishing Dubai as a global leader in innovation, safety and security. "We are delighted to collaborate closely with DESC," Kotzé remarked.

Microsoft makes the first move

Microsoft was the first provider to achieve DESC's stamp of approval through CSP Security Standard certification in June 2019 for selected cloud services. The US tech giant has also established the Middle East's first cloud regions in the UAE, selecting both Dubai and Abu Dhabi to provide local organisations, individuals and developers with optimally secured, resilient cloud services while maintaining data residency, security and compliance. The number of international tech corporations launching data centers in the region is fast growing. 

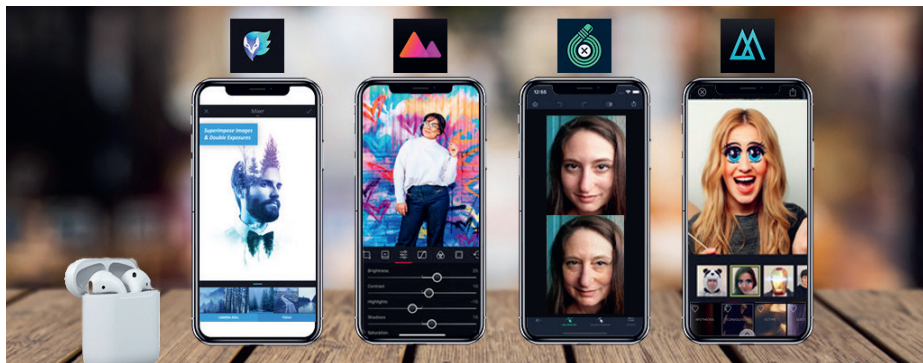


PHOTO EDITING APPS ARE FUN AND USEFUL... BUT ARE THEY DANGEROUS?

Although FaceApp was launched in 2017, it wasn't until recently that this mobile application caused a social media flurry, with celebrities around the world posting manipulated images of their older selves. However, it has also come under fire for privacy concerns.

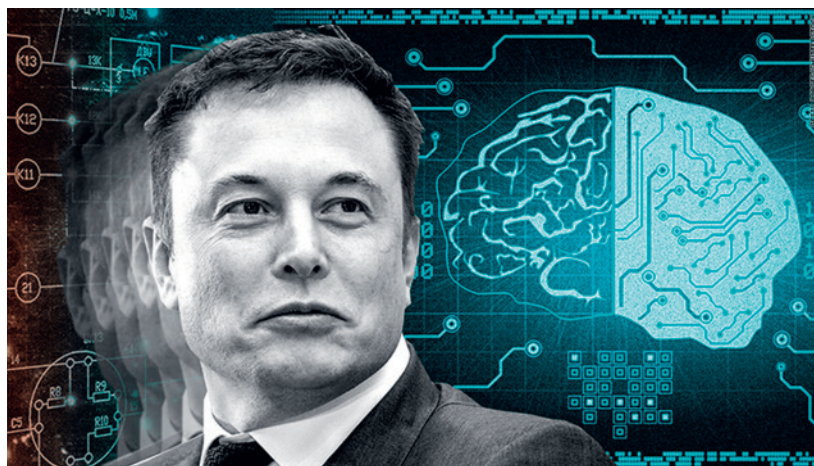
The app is a state-of-the-art photo editor powered by AI. It already has more than 150 million active users and has won numerous awards including Best of 2017 from both the AppStore and Google Play. 20-plus filters allow people to create digital photographs of themselves looking realistically older, younger or more attractive.

FaceApp and others like it have, however, been the focus of security scrutiny, primarily because – like many apps and social media platforms – they collect data from users that could make them vulnerable to criminals should they be exposed.

FaceApp only takes photographs specifically provided by users to see a face change – it uploads nothing more – but these photo files are sent to the cloud for processing, where stringent controls are constantly required to secure the data. Social media companies are urging that people protect their digital data and use the app with caution.

Like many technologies, the innovation has both pros and cons. A similar AI system, created by Chinese tech giant Tencent, recently helped to reunite a family in which the toddler went missing 18 years ago. Police managed to track him down using a similar face-ageing app to predict what the child would look like today. Although the now-21 year old initially found it hard to believe that he'd been kidnapped as a toddler, DNA tests confirmed a match with his overjoyed biological parents.

ELON MUSK REVEALS PLANS TO CONNECT HUMAN BRAINS TO COMPUTERS



High-tech business leader Elon Musk is developing implantable brain-machine interfaces (BMIs) – devices to connect the human brain to computers. The focus of this work is finding ways to stimulate the brains of patients with severe neurological challenges, enabling them to control computers and so improve their quality of life.

One of Musk's companies, Neuralink, is spearheading the research, while other technology firms are also investigating similar ways to augment human brain capabilities in association with AI machine learning. One of its systems has already been tested on a monkey, making it possible for the animal to control

a computer with its brain. Now Musk wants to start testing the device on humans.

The system includes a tiny probe containing over 3,000 electrodes attached to flexible threads thinner than a human hair. This allows it to monitor specific areas of the brain, analyzing recordings using artificial intelligence (AI) that would then establish what type of stimulation a patient requires.

Years of scientific, technical and ethical development are still needed for the system, but it has so far been applauded for its potential to alleviate serious medical conditions, like strokes, epilepsy and Parkinson's disease.

MOZILLA FIREFOX TO WARN USERS OF PASSWORD BREACH



Free web browser Mozilla Firefox will soon introduce a security update to warn users if their login credentials have been compromised.

The company is collaborating with a data breach tracker to develop the initiative. It will utilize a database of over 8 billion accounts that have been exposed to data breaches to alert users, scanning saved

logins for any matches and issuing a password warning to alert those it finds and prompt users to change their codes.

The new security feature will be fully integrated into Firefox version 70 and will benefit more than 800 million active desktop browsers who have saved their login details before the breach. The alert will be issued automatically, reading: "Passwords were leaked or stolen from this website since you last updated your login details."

More detailed information may be provided in future, such as the impact of the breach on the user's account and the number of email addresses affected. Mozilla warned that users should still implement basic password security measures, such as ensuring unique passwords and enabling two-factor authentication.

THE SKY IS NO LIMIT FOR SATELLITE HACKERS

The thousands of satellites orbiting the Earth offer a new hunting ground for cybercriminals and experts are concerned that satellite engineers worldwide are not sufficiently considering such dangers in their designs.

At the 2019 RSA IT security conference in San Francisco, researchers reported that, while satellite communication structures have focused on safety, information security has become equally important. Thousands of people attend the RSA conferences which take place in the UAE, United States, Europe and Asia each year.

The first satellite to be deployed was Sputnik 1, in 1957. Since then, over 8,900 satellites have been deployed and the majority are still active. These highly sophisticated machines provide essential information in an array of applications, from

GPS to weather and disaster tracking, and space exploration.

In recent decades, several malicious attacks have disrupted or destroyed satellites.

As far back as 1998, a satellite X-ray telescope built by the US and Germany was reportedly hacked via cyber-intrusion and manipulated toward the sun so that it was destroyed by the heat.



However, they are set to become increasingly vulnerable as the cost of antennas plummet and the field of satellites and space capabilities grow. Hackers could also jam GPS signals, intercept or falsify vital data or potentially hijack a satellite for ransom, among other underworld activities.

Cybersecurity experts advise that several layers of security are required, including technological and policy measures.

AI IS DRIVING THE DANGER OF DEEPPAKES



Where there are innovative technologies, there will be darker elements of society using them for exploitation and menace. Malicious Artificial Intelligence (AI) is leading the development of 'deepfakes' – in which a combination of real-world video and audio are manipulated by an imposter to create highly convincing but totally fake footage of someone doing or saying things they never did at all.

Deepfake material goes beyond even the digital trickery of photomanipulation. AI is being used illegally to fool people into believing they're watching real clips of celebrities, politicians, even state leaders caught in compromising positions or making shocking comments. Machine learning (AI) software can easily clone anyone's voice to generate new speech and algorithms have been developed to create deepfake faces from large data sets.

Criminals and terrorists can create deepfakes for ransom attacks, to destabilise a financial market, even to incite panic, if that suits their dark agendas. Once they're deployed on social media, deepfakes can go viral in a matter of minutes. While experienced analysts are still able to detect fakes using specialist computer programmes, the rest of us need to trust our instincts and think twice when we hear or see something that probably isn't real.



DIGITAL IMMUNITY ECOSYSTEM & DNA DIGITAL STORAGE... COMING SOON TO DUBAI!

Digital immunity? Storing data within DNA coding? If these sound to you like something out of a sci-fi movie... welcome to the future!

Dubai Electronic Security Center (DESC), represented by Dr Bushra Al Blooshi, Head of Research and Innovation Department at DESC, together with Dr Eesa Bastaki, President of the University of Dubai, is currently collaborating with global expert Dr Rocky Termanini, CEO of MERIT Cyber Security Consulting, to develop a prototype Digital Immunity Ecosystem as well as a DNA laboratory for data archiving, which will be presented at Expo 2020.

Here, Dr Termanini explains these technologically sophisticated concepts and how they can protect Dubai against future cyber challenges.

We are living in the age of innovation. With his ingenious strategic vision, Sheikh Mohammed, Vice President and Prime Minister of the United Arab Emirates and Ruler of Dubai, is building the smart future of Dubai - and of the country - in a brilliant synthesis of futuristic technology, human intelligence and natural resources that delivers a high quality of life and sustainable economic prosperity.

Two strategic initiatives that could embrace this vision are currently being researched in collaboration with the Dubai Electronic Security Center, under the direction of the Director General H.E. Yousuf Al Shaibani and DESC's Research and Innovation department:

1. Digital Immunity Ecosystem (DIE) - which will offer the new generation of autonomic cybersecurity defense for the next 20 years. The combined artificial intelligence (AI) and



Dr Rocky Termanini

nanotechnology-centric platform of the DIE is designed as a replica of the human immune system. It is the techno-solution capable of exterminating a whole range of malware if launched against a smart city system.

2. DNA Digital Storage - a mind-boggling expedition to the land of the blueprint of life: the deoxyribonucleic acid (DNA). Dubai will be one of the foremost cities to adopt DNA data storage, which will also be an integral element in the DIE.

Here is how these two cutting-edge technologies could be successfully deployed to put Dubai ahead in the domain of smart city cyber security:

DIGITAL IMMUNITY ECOSYSTEM (DIE)

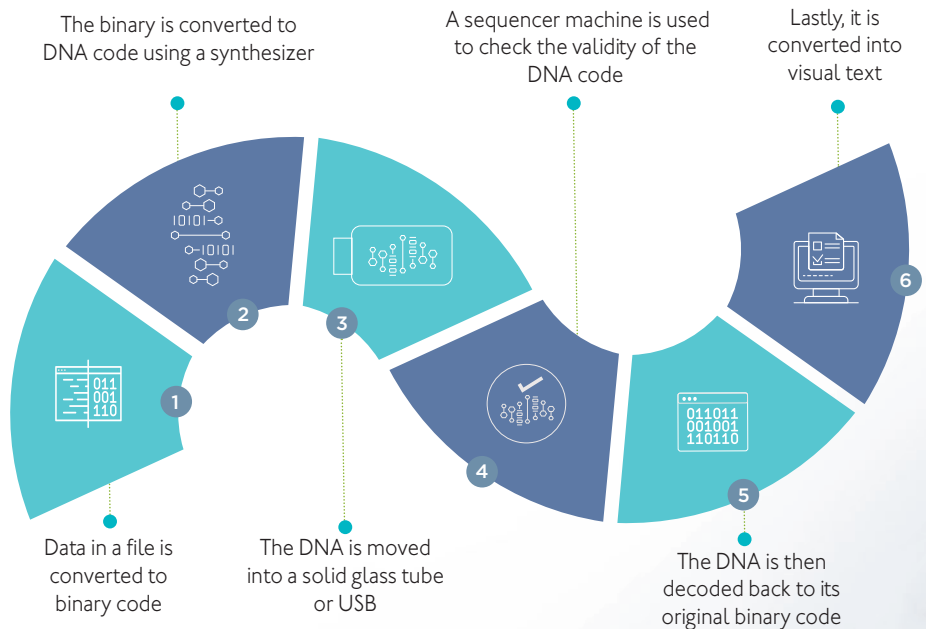
Technology has always been a double-edged sword. Cybercrime and terrorism have been making black holes in our societal fabric, thriving on profound immorality and political poisoning, but the DIE is designed to provide a complex network that protects the smart city from cyberattacks.

The concept of technology to replicate human intelligence (artificial intelligence or AI) is as challenging as it is attractive. The DIE is a hybrid of human intelligence and expertise, empowered by AI and nanotechnology expert components.

The AI components allow the system to programme and operate itself, learn from past actions and even repair itself. To replicate the human immune system, however, we need another vital component at the atom level, which is where nanotechnology comes in. Nanotechnology will give the DIE better control, more resilience, higher efficiency, speed and precise predictability of cyberattacks.

- **Early Warning Prediction System** - provides intelligent alert capability to catch attacks before they hit the city and its critical infrastructure systems
- **Cognitive Attack Memory** - an attack-learning engine to remember prior attacks, and forecast future attacks
- **Nano Smart Vaccine Defense** - strengthens the immunity of all systems against surprise attacks
- **Autonomic Grid** - offers hyper responsive AI and nanotechnology engineering to keep all city devices and critical systems protected

DNA DIGITAL ENCODING PROCESS



The genetic molecule is extremely small yet, through this digital encoding technique, it is possible to store 2.15 Pb (or 2.15 million Gb) of digital data in a single gram of DNA – approximately the amount of data currently stored on the internet!

In some respects, the DIE is similar to anti-virus technology (AVT) but they belong to different generations - it's like comparing a bullet train to a steam locomotive. The DIE is built with smart AI components on a molecular scale and, unlike AVT, which resides on the internet, the DIE inhabits a smart nano-grid (its nervous system) and communicates with satellites and cloud technologies.

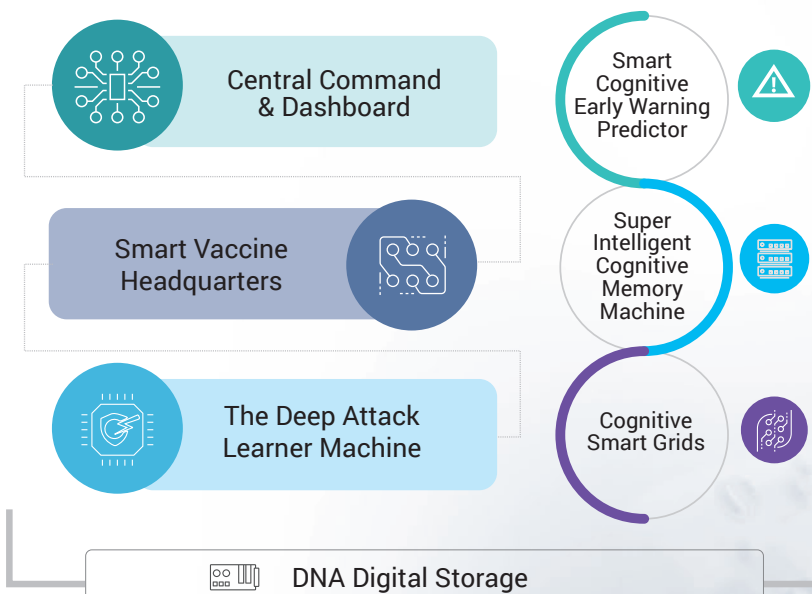
With the DIE smart nano-grid in place, the city of Dubai will be on permanent alert to potential cyberattacks. All critical systems, including the Internet of Things and Dubai blockchain systems, will be connected to the grid and will be routinely 'inoculated' to keep them immune from surprise attack.

DNA DIGITAL STORAGE

In 2012, Dr George McDonald Church, an American geneticist at Harvard University, described how he encoded digital information to DNA, including a 53,400-word book and several images and programmes. He was able to store 5.5 petabits in one cubic millimeter of DNA. [Ed: a petabit (Pb) is one of the largest types of data measurement; one petabit is equal to one million gigabits (Gb) of data.]

Today, computing architects and synthetic biologists are designing systems to automate the DNA storage process. DNA code may, in future, be used to store the operational data of all critical systems and Digital Immunity Operations Data on the DIE.

[Ed's note: original article edited and cut to fit]





ENCOURAGING THE YOUTH TO **CARVE A CAREER** IN CYBERSECURITY

Dubai Electronic Security Center (DESC) showcased the exciting opportunities available to the youth of the UAE in the field of cybersecurity when it participated in Careers UAE, held at the World Trade Centre in Dubai in March 2019.

In the era of big data, the importance of jobs aimed at protecting information and the security of the cyberspace in which it resides has become a critical priority and has witnessed an unprecedented demand, especially as data has surpassed even the most valuable of the world's resources. No generation has been as digitally savvy nor as technologically enthusiastic as the current youth, which is why DESC encourages youth to specialise in this sector and looks forward to having a generation superbly qualified and equipped to step up as future guardians of our cyberspace.

CAREERS UAE 2019

Contributing to the empowerment of high-calibre Emirati nationals with exciting, purposeful occupations, while promoting awareness of our leadership's vision to make Dubai the world's most cybersecure city, DESC participated in Careers UAE 2019 for the fourth consecutive year.



With demand for experts in the fields of Information Technology (IT) and Information Security (IS) steadily increasing, the diverse job opportunities offered at DESC provide a strong launching base for new graduates.

Commenting on the search for excellent employees, the Center's participation at the careers event and DESC's vision for the future, H.E. Yousuf Hamad Al Shaibani,

Director General of DESC, said: "DESC is taking an active role in recruiting the best national talents in a dynamic and innovative way, in order to continuously improve our digital capabilities, develop new techniques and evolve with the ever-changing trends and challenges in the cyber world."

"We are keen on fulfilling the Center's vision, which stems from the directives of our wise leadership that is reflected in our Cyber Security Strategy. DESC has achieved excellent results with Emiratization, with the Center being run 100% by nationals."

"Our participation this year is a great opportunity to continue attracting creative national talents that will be part of the team to achieve the Center's vision. Careers UAE attracts a wide array of talents and competent prospective leaders and administrators in various capacities. We are committed to participating in such employment exhibitions to target and empower UAE nationals who want to excel in cybersecurity. We look forward to welcoming more qualified and exceptional people to our team."

INNOVATIVE PARTICIPATION

DESC introduced a new interactive registration system at its Careers UAE stand this year. Applicants were requested to complete a digital registration form along with a personality assessment test. This innovation generated an indicative measurement of an individual applicant's suitability to the work segment in which they expressed interest. It also matched their personal characteristics and aptitudes to the professional criteria required by various DESC jobs. Visitors were able to review an array of vacancies available and log their interest electronically.

The Center also showcased newly introduced departments and streams serving various sectors, along with the latest projects and initiatives in which DESC is involved.

POSITIONS REQUIRED AT DESC INCLUDE:



Network engineer



Data center officer



Security systems officer



Researcher



IT support officer



Software developer



Security operations center officer



Information security regulations officer



A POPULAR CAREER CHOICE IN THE UAE

Recent research by global IT security training company SANS revealed that cybersecurity awareness and the popularity of the field as a career choice amongst youth in the UAE and the Kingdom of Saudi Arabia (KSA) are amongst the highest in the world.

Among the 4,000 14- to 18-year-olds surveyed across seven countries in the Middle East and Europe, the choice of IT (including cybersecurity) ranked highest in KSA (47%) and the UAE (46%). Of those, 63% of students in KSA expressed specific interest in cybersecurity, as did 58% in the UAE. The European countries surveyed were the UK, France, Germany, the Netherlands and Belgium.

When it came to cyber awareness, 85% of respondents in the UAE and 82% in the UK said they had heard of cybersecurity. SANS suggested that those countries whose young generation showed higher levels of awareness could have a competitive advantage when it comes to developing talent to meet future needs.

THE CHOICE OF IT AS PROFESSION



47%



46%

STUDENTS INTEREST IN CYBERSECURITY



KSA

63%

UAE

58%

CYBER AWARENESS

UAE

85%

IT EDUCATION SUPPORT

Indeed, schools and universities in the UAE are contributing to the global technology skills pool. As the country's student population grows, and in support of UAE Vision 2021, the government this year allocated AED 10 billion (17% of its national budget) towards the development of a first-rate education system.

Digital innovation and technology integration are also key criteria in the UAE school inspection system, as features like digital collaboration tools, high-performance research and development labs, and similar technologies help to transform learning experiences.



CLOSING A SERIOUS SKILLS GAP

By 2020, there will be approximately 24 billion internet-connected devices worldwide. Ned Baltagi, SANS managing director in the Middle East, considers this to be a potential cybersecurity challenge, in that there will be a severe global shortage of professionals to secure all those online devices and systems.

"Given the enthusiasm and aptitude of the iGeneration for digital technologies, the answer could lie in educating younger generations about cybersecurity now, to arm our future workforce," Baltagi advised.

Other key findings from the SAN research include:

- At 32% of most respondent's top five career choices, IT outranked even more

traditional careers, like doctor/nurse (21%), teacher (19%) and finance-related jobs (16%).

- IT was voted even higher as a top-five career choice among school-goers in the UAE (46%) and KSA (47%).
- App creation and software development topped the total list (61%) for those interested in IT careers, followed by IT system design (52%) and then cybersecurity (49%), however in KSA and the UAE cybersecurity was first choice at 63% and 58%, respectively.
- Nearly all students (81%) said they would be keen to learn more on the subject at school, with respondents from KSA (93%) and the UAE (91%) again proving the most interested in cybersecurity.

SO, YOU WANT TO BE A CYBERWARRIOR...

With so many outstanding accredited higher education institutions in Dubai, high school graduates are spoilt for choice when it comes to tertiary studies. If you or someone you know is keen on qualifying for this career, there are several tertiary academic routes you can follow. Do your homework to make sure you choose the path that is right for you.

Attend some of the excellent higher education and career expos that are held each year in Dubai, speak to your school's career guidance counsellor, and do some online research to get a good idea of what's available. Once you have a shortlist of the best university, college or other options, try to attend their open days or make an appointment to visit the relevant departments.

Typically (but not exclusively!), those working in the cybersecurity sector will hold specific certifications and specialists will hold at least a bachelor's



JOB OPPORTUNITIES IN CYBERSECURITY

Not all of the millions of jobs available in the cybersecurity sector are directly involved with digital technology. In fact, communication skills are probably more in demand than those requiring programming and coding. At Dubai Electronic Security Center, for example, a critical element in its mandate is the drafting and implementing of cyber-related policies to secure information exchange and data storage.

Digital forensics is another crucial aspect to cybersecurity. It involves digging around digitally when things go wrong, to find out who did what, when, where and, most importantly, how – so that it can be prevented from happening again in the future. Teamwork, problem-solving skills and an open and analytical mind are valuable in this job.

Here are just some of the top cybersecurity job titles held by IT/cybersecurity graduates:

- Vulnerability Analyst/Penetration Tester
- Network Architect
- Information Security/Cyber Threat Analyst
- Cybercrime Analyst
- Computer Forensics Analyst
- Software Developer
- Systems Administrator
- Cybersecurity Administrator
- Information Assurance Engineer
- IT Security Specialist
- Network Support Technician
- IT Audit Manager
- Ethical Hacker (so-called White Hat) 

degree in computer/information science, programming or engineering. The mathematics and statistics involved in such courses tends to be quite demanding.

Policy analysts and those with legal and business administration backgrounds also play important roles in keeping our digital spaces secure.

So, how do you know if cybersecurity might be the right field for you?

Many of those who are successful in this fast growing sector – from analysts to programmers and beyond – share certain personal attributes. You might enjoy career satisfaction amongst the cybersecurity gang if...

- STEM subjects are your favourites
- You're consumed with computers, video games and electronic gadgets
- Programming computers and writing digital codes fascinates you
- You love the challenge of solving puzzles and problems
- You pay attention to details
- You like to flex your imagination and think out of the box
- Multi-tasking is stimulating, not overwhelming for you
- You like to stay ahead of the curve and never stop learning
- You are proud of your country and want to play a role in keeping it safe
- You feel great when you are contributing towards a great cause



HEALTHIER TECH HABITS

Awareness and tips to manage
our increasing use of technology

As humanity enters the third decade of the 21st century, there can be little doubt that we are sharing our lives with a supremely domineering partner: digital technology. This relationship has grown to be (almost) inescapable, but it is essential that we regularly practise putting some healthy distance between ourselves and our habits.

The dangers of tech overload are increasingly evident – attention deficit, learning challenges, obesity, social withdrawal, addiction, even physical deformities among growing children (like ‘text neck’) are commonly reported.

But how do we stop?!

“Nomophobia” is the irrational fear of being without your mobile phone or being unable to use your phone for some reason, like no signal or no battery power. Yes, there is an official term for smartphone addiction!

Here, Esharat looks at digital addiction, especially smartphone obsession, and offers some practical tips to handle what has fast become normal: all day, every day use of technology. By introducing some simple rules into our lives, we can restore the balance of power in this relationship.

SWITCH OFF BEHIND THE WHEEL

We know we shouldn’t text or talk and drive – there are strict laws prohibiting the use of phones while driving. Yet still there are many of us who, even if we don’t place calls, feel compelled to answer the phone when it rings while speeding down the freeway. It’s hard to resist! Switch off or bury your phone in your bag or the boot if you have to.

SAY NO TO NOTIFICATIONS

Notification beeps are invasive, annoying and increase stress levels by continually







SOME DISTURBING SMARTPHONE STATS

Various 2018/2019 digital health research studies have reported these average statistics in worldwide iOS and Android smartphone usage:



HIGH TECH DEMANDS ON THE HUMAN BODY

In addition to the extremes of smartphone attachment, many of us now spend more than half of every day on our work chairs, shackled to our PCs or laptops. Some of the negative physical effects of long-term screen use can include:

- Backache
- Headaches
- Blurred vision or eye strain
- Weight gain (or weight loss, in the case of extreme gamers and hackers)
- Carpal tunnel syndrome (nerve damage affecting the arm, wrist and hand)
- Oedema (swollen legs and feet)
- Sleep disturbances

It can be difficult to avoid technology if your daily life or job involves using computers and other devices. So, let's take a look at some of highly recommended ways to alleviate the impact on our bodies:

STRAIGHTEN UP

Check your posture. If your ears are not positioned directly over your shoulders, you are stooping forward. Slouching will weaken your stomach and back muscles over time, so make sure to sit up straight.

MAXIMISE YOUR WORK STATION

Your laptop or monitor should be placed straight in front of you, with the screen at eye level.

RELAX

While typing or using the mouse, your wrists should be straight and relaxed. If your wrists are raised, your arm muscles will be tense, your shoulders will rise and your neck will take strain.

TAKE IT EASY ON THE EYES

Did you know that we blink less when we look at screens? Maintaining constant screen focus also weakens the eye muscles. Look away out of the window or to the other side of the office to give your eyes a break. 📺

