

DUBAI CYBER SECURITY STRATEGY 2023

TO ESTABLISH DUBAI AS A CYBER SECURITY
LEADER IN THE DIGITAL WORLD



TABLE OF CONTENT

PREAMBLE	10
FOREWORD	12
EXECUTIVE SUMMARY	14
DIAGRAM OF DOMAINS AND OBJECTIVES	15
STRATEGY DOMAINS & OBJECTIVES	16
DOMAIN 1 – CYBER SECURE SOCIETY	16
DOMAIN 2 – INCUBATOR FOR INNOVATION	16
DOMAIN 3 – RESILIENT CYBER CITY	16
DOMAIN 4 – ACTIVE CYBER COLLABORATION	17
DUBAI’S CYBER SECURITY LANDSCAPE	18
DIGITAL SOCIETY	18
THREATS AND RISKS OF CYBERSPACE	19
GUIDING PRICIPLES	20
FREE FLOW OF INFORMATION AND OPENNESS	20
COMPLIANCE WITH LAWS AND REGULATIONS	20
APPROACH	23
VISION	23
MISSION	23
SCOPE	23
DOMAIN 1: CYBER SECURE SOCIETY	25
INTRODUCTION	25
OBJECTIVES	25
1.1 CULTIVATE CYBER SKILLS	25
1.2 FOSTER ACCESSIBLE CYBER SECURITY	26

DOMAIN 2: INCUBATOR FOR INNOVATION	25
INTRODUCTION	25
OBJECTIVES	25
2.1 PROMOTE CYBER SECURITY RESEARCH AND BUILD AN INNOVATION ECOSYSTEM	25
2.2 SECURE APPLICATION OF EMERGING TECHNOLOGIES	29
2.3 GROW THE ASSURANCE ECOSYSTEM	29
DOMAIN 3: RESILIENT CYBER CITY	31
INTRODUCTION	31
OBJECTIVES	31
3.1 SHAPE THE GOVERNANCE OF CYBER SECURITY	31
3.2 EXTEND THE RESILIENT CYBER ECOSYSTEM	32
3.3 MANAGE CYBER CRISIS AND INCIDENT RESPONSES	33
3.4 AMPLIFY RESILIENT CYBER INFRASTRUCTURE	33
DOMAIN 4: ACTIVE CYBER COLLABORATION	36
INTRODUCTION	36
OBJECTIVES	36
4.1 EXTEND LOCAL COLLABORATIONS	36
4.2 CONTRIBUTE TO INTERNATIONAL CYBER SECURITY EFFORTS	37
ACHIEVEMENTS ROAD MAP	38



HIS HIGHNESS SHEIKH MOHAMMED BIN RASHID AL MAKTOUM
VICE PRESIDENT AND PRIME MINISTER OF THE UAE AND RULER OF DUBAI

“CHALLENGES HAVE NEVER PREVENTED US FROM PURSUING OUR AMBITIONS, AND THEY NEVER WILL. WE ARE DETERMINED TO TRANSFORM CHALLENGES INTO OPPORTUNITIES FOR CREATIVITY AND INNOVATION, AND EXPLORE NEW IDEAS AND INITIATIVES THAT CAN HELP US ACHIEVE OUR ASPIRATIONS.

THE DUBAI CYBER SECURITY STRATEGY, WHICH ADDS TO THE GOVERNMENT’S NUMEROUS ACHIEVEMENTS, GIVES FURTHER IMPETUS TO OUR JOURNEY OF EXCELLENCE IN CYBER SPACE.

ON THE OCCASION OF THE LAUNCH OF THIS STRATEGY, I WOULD LIKE TO THANK ALL THOSE WHO CONTRIBUTED TO ITS DEVELOPMENT AND CALL ON THEM TO RECOMMIT TO THE HIGHEST EXCELLENCE AND LEADERSHIP AND FORGE AHEAD WITH OUR GOALS SO THAT WE CAN CREATE EVEN MORE HAPPINESS AND PROSPERITY FOR OUR PEOPLE.

WE HAVE GREAT CONFIDENCE IN THE ABILITY OF THE GOVERNMENT AND PRIVATE SECTORS IN THE UAE TO SUCCESSFULLY IMPLEMENT THE DUBAI CYBER SECURITY STRATEGY. LET US DOUBLE OUR EFFORTS AND WORK DILIGENTLY TO MAKE THE UAE ONE OF WORLD’S DIGITALLY SAFEST COUNTRIES.”

HIS HIGHNESS SHEIKH MOHAMMED BIN RASHID AL MAKTOUM

VICE PRESIDENT AND PRIME MINISTER OF THE UAE AND RULER OF DUBAI



HIS HIGHNESS SHEIKH HAMDAN BIN MOHAMMED BIN RASHID AL MAKTOUM
CROWN PRINCE OF DUBAI AND CHAIRMAN OF THE EXECUTIVE COUNCIL

**“DUBAI CYBER SECURITY STRATEGY, A
VISIONARY BLUEPRINT DESIGNED TO
SAFEGUARD THE DIGITAL BACKBONE OF
OUR CITY AND PRIORITIZE THE SAFETY OF
OUR CITIZENS.”**

**HIS HIGHNESS SHEIKH HAMDAN BIN MOHAMMED BIN RASHID AL MAKTOUM
CROWN PRINCE OF DUBAI AND CHAIRMAN OF THE EXECUTIVE COUNCIL**



HIS EXCELLENCY HAMAD OBAID AL MANSOORI

**DIRECTOR GENERAL
DIGITAL DUBAI AUTHORITY**

PREAMBLE

Digital Dubai, represented by the Dubai Electronic Security Center, continues to implement its mission towards building a comprehensive and sustainable digital future for the city of Dubai. The concept of comprehensiveness requires considering all aspects and dimensions that guarantee happiness, well-being, and safety for all residents of Dubai and the United Arab Emirates.

The Dubai Cyber Security Strategic Plan was therefore created to cover an important aspect of our ambition that combines openness with digital technology on one hand and maintains the safety and security of the society in cyberspace on the other hand.

This document gains its importance from several points related to the specifics of today's day and age. The technologies included in the Fourth Industrial Revolution grant wide opportunities to achieve a qualitative leap in societies economically, culturally, and intellectually. At the same time, the risks and challenges arising from the expansion of digital applications are increasing.

Maintaining a balance requires a lot of vigilance, flexibility, and keeping pace with latest developments. It also requires effective coordination between institutions and strengthening of the synergies and partnership principles to reduce and manage risks, while transforming potential threats into opportunities that lead to address any gaps, ensuring we meet the goals set by our wise leadership to make Dubai a model city of the future.

This plan is comprehensive, detailed and is the result of cooperation between several teams working in the field of cyber security and digital transformation in Dubai. Thus, it is a highly important document, but its true value lies in its actual application. This is the responsibility of all of us, whether in government entities or private sector institutions, as we are all partners in this strategic mission.

I take this opportunity to invite everyone to consider this plan as a guide to strengthening processes and procedures, building competencies, spreading awareness, and applying the latest standards in the field of cyber security.

HIS EXCELLENCY HAMAD OBAID AL MANSOORI

**DIRECTOR GENERAL
DIGITAL DUBAI AUTHORITY**



HIS EXCELLENCY YOUSUF HAMAD AL SHAIBANI

**CHIEF EXECUTIVE OFFICER
DUBAI ELECTRONIC SECURITY CENTER**

FOREWORD

The world today is rapidly changing across all aspects of life, including digital technologies, the key driver of the Fourth Industrial Revolution. As much as these technologies are witnessing unprecedented developments, the risks are also evolving, and we are observing previously undiscovered patterns.

This highlights the importance of the Dubai Cyber Security Strategy 2023, which complements and updates the previous strategy, as a new starting point that ensures keeping pace with the rapid changes witnessed in the digital world. The strategy enables dealing with such changes proactively and efficiently, and effectively addressing any potential negative implications that may affect the cyberspace, and the community's safety and security.

The strategy foresees the future, taking into account the urgent need for resilience, vigilance, and constant preparedness to adapt to changes, due to the fact that the applications, tools and methods used to achieve cyber security are constantly changing. This strategy however is based on firm principles that are set to meet our vision of enhancing Dubai's position as a global leader in cyber security.

Forming part of Digital Dubai, we realize that digital transformation is a comprehensive and integrated journey, and that cyber security is the cornerstone and the safety valve that ensures city digitization objectives and goals are fulfilled safely and securely. The Dubai Electronic Security Center is therefore committed, under this ambitious strategy, to carry on harnessing its efforts, capabilities, and resources, and continues exerting its utmost efforts to ensure the provision of a safe, open, and free cyberspace for Dubai's society and economy. The Center will provide the highest levels of security, reliability, and dependability, by taking all necessary actions to support the city's digital infrastructure, accelerate its digital transformation and protecting it from cyber security attacks, in cooperation with all partners and stakeholders, boosting Dubai's position as a global leader in the field of digital economy and as an incubator of business, innovation and creativity.

HIS EXCELLENCY YOUSUF HAMAD AL SHAIBANI

**CHIEF EXECUTIVE OFFICER
DUBAI ELECTRONIC SECURITY CENTER**



EXECUTIVE SUMMARY

Dubai Electronic Security Center was founded in 2014 by Sheikh Mohammed Bin Rashid Al Maktoum to make Dubai a leader in cyber security and protect it from external cyber threats.

Today, we are proud to announce the launch of the 'Dubai Cyber Security Strategy 2023', marking a significant milestone in our commitment to safeguarding the digital ecosystem of our city. With a focus on digital transformation and smart city initiatives, our new 'Dubai Cyber Security Strategy 2023' aims to protect the digital fabric that underpins the success and well-being of Dubai.

As we reflect on the successful 'Dubai Cyber Security Strategy 2017' launched six years ago, we recognize the need to adapt and evolve in response to the constantly changing cyber landscape.

This new strategy captures the essence of these shifts, ensuring that our cyber security posture effectively aligns with Dubai's digitization strategies and proactively protects Dubai cyberspace.

In today's rapidly evolving digital landscape, cyber security has become paramount for organizations across all sectors. Dubai is no exception. As we navigate the challenges and opportunities brought forth by the digital era, our digital shifts have propelled the new strategy towards a city-centric approach; recognizing that cyber security encompasses not only government entities but the entire city, including critical infrastructure, businesses, residents, and visitors.

Moreover, our commitment to ensuring the integrity, privacy, and compliance of information processing and management systems is reflected in our cyber security approach, as we aim to enhance decision-making processes.

By adopting a proactive stance on cyber protection and resilience, and fostering collaborations and partnerships, Dubai is poised to lead the way in cyber security excellence and reinforce our position as a global digital leader.

The 2023 Strategy, builds on the triumph of its 2017 predecessor, encompassing 4 new domains:

- **CYBER SECURE SOCIETY**
- **INCUBATOR FOR INNOVATION**
- **RESILIENT CYBER CITY**
- **ACTIVE CYBER COLLABORATION**

Through the engagement of all stakeholders in Dubai, the 2023 Strategy aims to create a trusted and reliable cyberspace, propelling Dubai towards digital cyber security excellence.

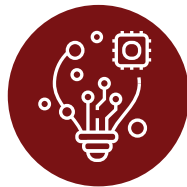
DIAGRAM OF DOMAINS AND OBJECTIVES

VISION

To establish Dubai as a cyber security leader in the digital world.

MISSION

Create a safe, secure, reliable, and trusted cyberspace in Dubai, to support its digital infrastructure.



DOMAIN 1

CYBER SECURE SOCIETY

OBJECTIVES

- 1.1**
CULTIVATE CYBER SKILLS
- 1.2**
FOSTER ACCESSIBLE CYBER SECURITY

DOMAIN 2

INCUBATOR FOR INNOVATION

OBJECTIVES

- 2.1**
PROMOTE CYBER SECURITY RESEARCH & BUILD AN INNOVATION ECOSYSTEM
- 2.2**
SECURE APPLICATION OF EMERGING TECHNOLOGIES
- 2.3**
GROW THE ASSURANCE ECOSYSTEM

DOMAIN 3

RESILIENT CYBER CITY

OBJECTIVES

- 3.1**
SHAPE THE GOVERNANCE OF CYBER SPACE
- 3.2**
EXTEND THE RESILIENT CYBER ECOSYSTEM
- 3.3**
MANAGE CYBER CRISIS & INCIDENT RESPONSES
- 3.4**
AMPLIFY RESILIENT CYBER INFRASTRUCTURE

DOMAIN 4

ACTIVE CYBER COLLABORATION

OBJECTIVES

- 4.1**
EXTEND LOCAL COLLABORATIONS
- 4.2**
CONTRIBUTE TO INTERNATIONAL CYBER SECURITY EFFORTS

STRATEGIC DOMAINS & OBJECTIVES

The Dubai Cyber Security Strategy 2023 has a set of four main domains, which, together with the Guiding Principles listed below, will be established, and implemented to achieve cyber security to support and secure Dubai's digital infrastructure.

DOMAIN 1 CYBER SECURE SOCIETY

Continually increasing the awareness, skills, capabilities, and outreach to manage cyber security risks for Dubai's public and private sectors.

OBJECTIVES:

- **Cultivate cyber skills:** Adequate formal training should be provided to build a skilled workforce. A clear career path should be outlined for cyber security experts and increase the number of cyber security experts in the city.
- **Foster accessible cyber security:** Cyber security awareness for public and private sector employees should be provided, that cover the ever-increasing number of technologies that will become a part of daily life in Dubai.

DOMAIN 2 INCUBATOR FOR INNOVATION

Promoting research and invention for cyber security, and establishing a free, fair, and secure cyberspace fostering innovation in Dubai.

OBJECTIVES:

- **Promote cyber security research and build an innovative ecosystem:** The city needs to create an environment that supports research, development, and innovation to build a secure cyberspace.
- **Secure application of emerging technologies, such as Internet of Things (IoT), Artificial Intelligence (AI), Virtual Reality (VR):** These emerging technologies bring both opportunities and big risks to the city. Therefore, suitable solutions and processes should be developed using a secure by design philosophy before using these technologies.
- **Grow the assurance ecosystem:** Achieving this will rely on creating and enforcing certification schemes in emerging technologies that cover products, services and people based on international security standards.

DOMAIN 3 RESILIENT CYBER CITY

Enhancing the controls in place to protect confidentiality, integrity and availability for Dubai's public and private sectors, and individuals, and ensuring the continuity and reliability of ICT systems in Dubai's cyberspace.

OBJECTIVES:

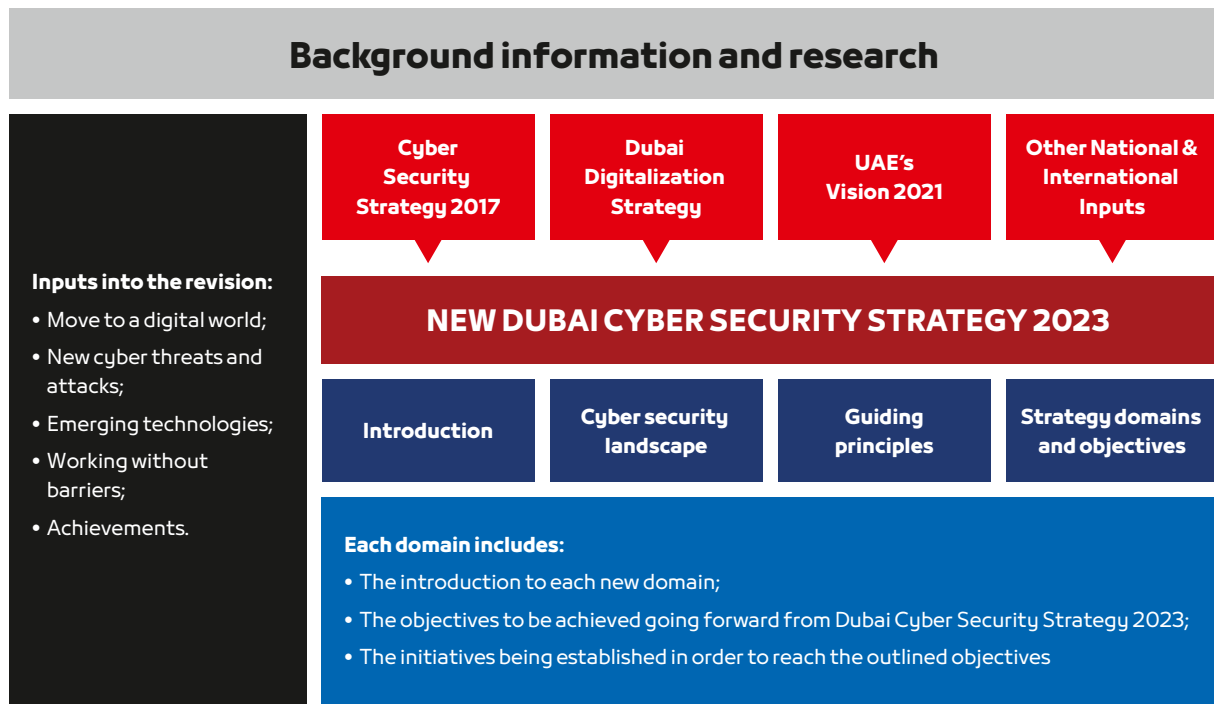
- **Shape the governance of cyberspace:** Senior management needs to understand and ensure governance processes are in place to enable organizational growth and achieve business objectives. They also should clearly outline responsibility, risk, and cyber security policy implementation plans.
- **Extend the resilient cyber ecosystem:** Support will be provided for the following areas; Security for the supply chain, security by design implemented in systems' development life cycle, cyber security insurance to protect organizations in areas they lack, emerging technology standards and guidelines.
- **Manage cyber crises and incident responses:** The Dubai Cyber Index is tracking incidents as they occur on any connected entity to build a more holistic picture of any potential attack at the city level. A threat intelligence sharing platform will be provided to increase the knowledge of cyber incidents and improve the chances of successfully responding to cyber incidents. Cyber drills will be conducted to prepare entities and build incident response plans, capabilities, and communication.
- **Amplify resilient cyber infrastructure:** There is a need to identify and manage incidents and to have a good understanding of threats and risks. Entities should be able to at least withstand the initial levels of attacks. Cross organizational resilience plans should be developed to combat attacks that might span across multiple organizations.

DOMAIN 4 ACTIVE CYBER COLLABORATION

Increasing active national, regional, and international collaboration to manage cyber risks.

OBJECTIVES:

- **Extending local collaborations:** Cross-sector cyber security and resilience protection plan for critical information infrastructure (CII) organizations should be developed, to address threats and risks. Keeping up on cyber security and cyber resilience policies, standards, and other activities should be in place to integrate these components with the UAE Cyber Council. Furthermore, trusted organizations should be added to the Dubai Cyber Index, and working with expertise from different areas (e.g., start-ups and SMEs) should be included as a suitable option to share information with private organizations that does not conflict with any governmental policies
- **Contribute to international cyber security efforts:** Working with like-minded entities across the globe should be in place to tackle cyber-intrusion and adversaries from accessing each of the Institute's critical infrastructure.



The above diagram illustrates how this strategy was developed.

DUBAI'S CYBER SECURITY LANDSCAPE

DIGITAL SOCIETY

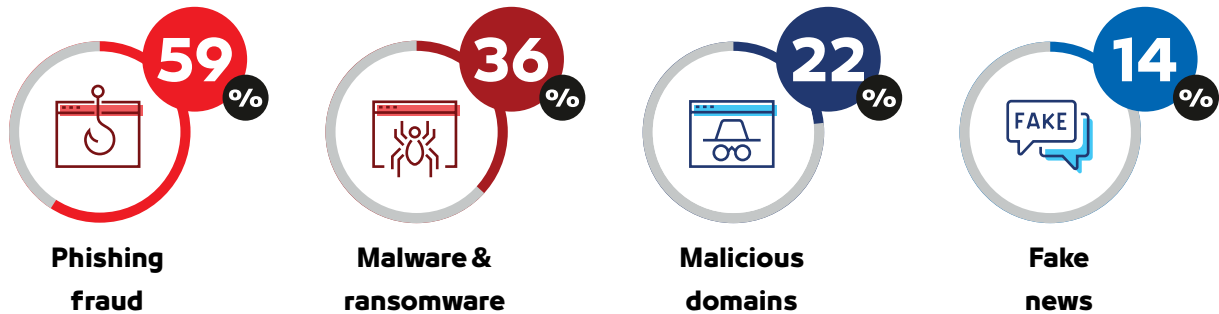
The UAE has a very high digital adoption rate. It has been increasing steadily over the last few years. The World Digital Report 2021 ranked 43 countries' use of digital media in 2020 and the UAE ranked above the global average. Last year, a resident in the Emirates spent on average seven hours and 24 minutes online per day. According to the report, 99 per cent of people in the UAE are active on social media and 97.6 per cent are smartphone owners. The increased use of IoT devices, along with wide-spread adoption of emerging technologies paints a picture of an advanced digital society in the country.

Covid-19 has dramatically changed how we work and live. This is not only true for the rise in use of digital products and services, but also applies to cyber-attacks. In the past year, the UAE has recorded a 300 per cent increase in cyber-attacks, and that number is likely to grow as the digital revolution continues. The pandemic and the digital revolution coincided, reinforcing the impact on life within and outside of the cyberspace. Cyber challenges we have faced in the past are only getting more complex, cyber security threats have become more sophisticated, and attacks are getting more concerted. Therefore, the reliance on technology is introducing several new vulnerabilities.

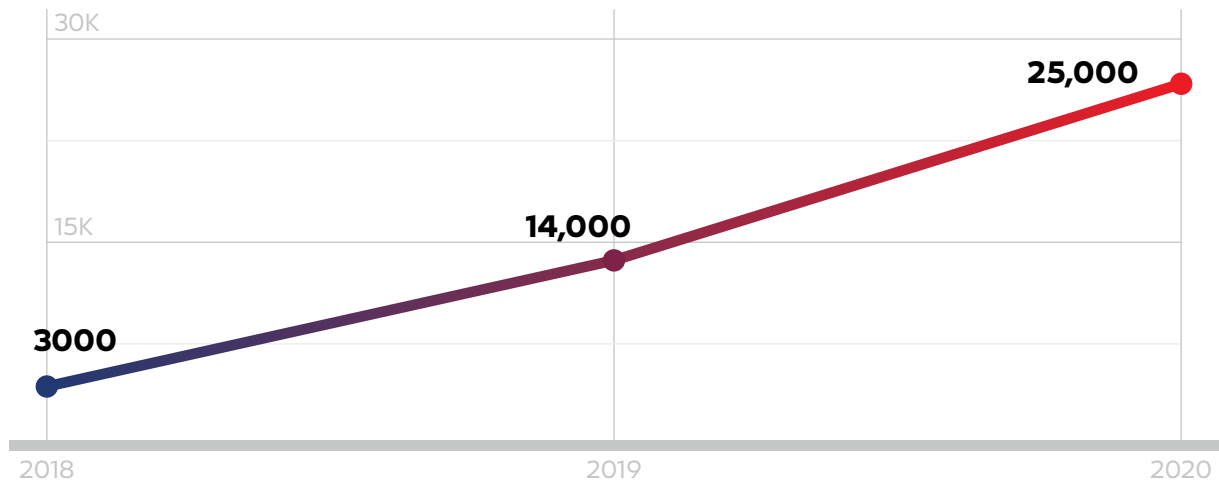
THREATS AND RISKS OF CYBERSPACE

COVID-19 LINKED TO MOST GLOBAL 2020 CYBER SECURITY ATTACKS

Cybercrime rose over 600% (PurpleSec¹)



E-CRIME REGISTERED CASES²



An interesting statistic highlights that the cyber security issues we are seeing in the UAE, are also happening on a larger scale across the globe.

Dubai Police registered 25,000 e-crime reports in 2020, as cyber criminals exploited the disruption caused by Covid-19 around the world. According to Dubai Police, reports have increased each year since the e-crime platform was established back in 2018, with 2020 accounting for the highest case numbers yet (3,000 cases in 2018, 14,000 cases in 2019 and 25,000 cases in 2020). Phishing and ransomware incidents were some of the most common forms of attack in the country.

The Dubai Cyber Security Strategy 2023 has been designed to protect Dubai's public and private sector organizations and individual citizens from these threats and risks, in order to make all of us safe and resilient in this constantly changing world.

1 Monster Cloud increase in attacks
2 Based on Dubai Police report

GUIDING PRINCIPLES

The vision of the Dubai Cyber Security Strategy 2023 is underpinned by guiding principles, which are essential to achieve its objectives. They are also the foundation of ensuring the well-being of Dubai's digital future, built through a secure cyberspace. The guiding principles highlighted in the 2017 Strategy have been modified to avoid overlap with the new objectives and topics, yet the basic ideas are the same.

FREE FLOW OF INFORMATION AND OPENNESS

Dubai's cyberspace provides plenty of opportunities for innovation, creativity, and success by providing a secure space for the free flow of information. It is eminent that information is not altered, or the information flow hindered in any way, so that messages reach their intended recipients, and that no specific interest group dominates the cyberspace.

Digital infrastructure and smart services are key pillars of our future. Strong cyber security is crucial to ensure we can deal with all threats and risks proactively and efficiently. In many ways, protecting our electronic borders is similar to protecting our maritime and land borders. Rapid technological advancement brings with it growing risks. As Dubai speeds up the pace of its digital transformation, reinforcing cyber security is vital to our sustained progress.

Dealing with challenges associated with cyber security is a common responsibility. To provide individuals and society a high degree of protection from cyber threats, we need to consolidate and synergize the efforts of various stakeholders. The Dubai Cyber Security Strategy and Dubai Cyber Index seek to create comprehensive protection from security risks, which is a critical element in bolstering Dubai's leadership in the digital arena. We will continue our journey of innovation and development to make Dubai the world's safest city in the digital world."

His Highness Sheikh Hamdan bin Mohammed bin Rashid Al Maktoum, Crown Prince of Dubai, and Chairman of The Executive Council of Dubai.

COMPLIANCE WITH LAWS AND REGULATIONS

With the all-pervasive threats and risks in the cyberspace, it becomes more and more important to have a legislative framework in place that can and will act, if required. The following legislation and regulations have been put in place in Dubai and the UAE with regards to cyber security.

There is a need to respect individual rights of privacy and to provide proper protection of intellectual property. In this sense, due consideration should be made to maintain the proper balance between open technology and individual rights of privacy. Overall, the cyberspace should be a competitive environment that ensures a fair return on investment in infrastructure, services, and content.

- Federal Law No. (7) of 2002 on Intellectual Property;
- League of Arab States, Model Arab Law on Combating Offences related to Information Technology Systems of 2004 ('the Model Law');
- Federal Law No. (1) of 2006 on Electronic Commerce and Transactions;
- Federal Law No. 2 of 2006 on the Prevention of Information Technology Crimes;
- League of Arab States, Arab Convention on Combating Information Technology Offences of 2010 ('2010 Convention');
- Federal Law No. (5) of 2012 on Cybercrime Prevention;
- The Executive Council of Dubai Government Resolution No. (13) of 2012 for Information Security Regulation in Dubai Government;
- Amends UAE Cybercrime Law No.5 of 2012;
- Updates provisions in Federal Law No. 5 of 2012, includes online activities taken for the interest of a terrorist group;
- Dubai Law No. 26 of 2015 on the Regulation of Data Dissemination and Exchange in the Emirate of Dubai, ("Dubai Data Law");
- Law No. (4) of 2016 on Dubai Economic Security Center;
- Emiri Decree No. 02 of 2018;
- Federal Decree Law No. 20 of 2019 on the Establishment of the Monitoring and Control Centre;
- Federal Decree-Law No. 45 of 2021 regarding the Protection of Personal Data;
- Federal Decree by Law No. 46 of 2021 on Electronic Transactions and Trust Services.

The Dubai cyber security strategy 2023 was implemented with the support of many stakeholders.

It would not have been possible without great efforts and cross collaboration from all trusted entities involved.

Going forward it is imperative that each person and organization do their part, in order for our goals to be achieved.



APPROACH

VISION

The Dubai Cyber Security Strategy 2023's vision is to establish Dubai as a cyber security leader in the digital world. This vision aims to position Dubai as a leading authority on cyber security, not just in the region, but globally, as well as protect and support its digital economy. Achieving this vision requires significant investment in research and development, innovation, and collaboration. This will help to raise Dubai's profile as a destination of choice for cyber security expertise and attracting talent and investment from across the globe.

MISSION

The mission of the 2023 Strategy is to create a safe, secure, reliable, and trusted cyberspace in Dubai to support its digital infrastructure. This mission statement focuses on the development of a robust and secure digital ecosystem that can be trusted by the public and private sectors. This includes implementing cutting-edge security technologies, robust policies and procedures, and effective regulatory frameworks that ensure the protection of critical infrastructure and sensitive data in the city.

SCOPE

The 2023 Strategy's main scope is to create a safe, secure, reliable, and trusted cyberspace in Dubai and apply the best techniques in cyber security to ensure it is not disrupted in any way. This is achieved by touching on some aspects of cyber security in Dubai. One of them is being able to increase cyber security awareness and overall cyber security skills, in both government entities and the private sector. Another aspect is being able to engage with different stakeholders on improving innovation in the city, by initiating collaborations with government and private sector entities, as well as developing curricula for cyber security training in the city. This approach will ensure the advancement of robust cyber security tools, solutions, and knowledgeable cyber security personnel available in Dubai. This can also be connected to increasing cyber resilience capabilities, by incorporating state of the art cyber security solutions into the city's digital infrastructure to make sure that the digital experience is impacted at a minimum level. Lastly, the city will also establish local and international collaborations with different stakeholders to improve communication from a cyber security point of view and help increase the city's cyber readiness from internal and external threats.



**“THE FUTURE
BELONGS TO
THOSE WHO
CAN IMAGINE IT,
DESIGN IT, AND
EXECUTE IT.”**

His Highness Sheikh Mohammed bin Rashid Al Maktoum
Vice President and Prime Minister of the UAE and Ruler of Dubai



DOMAIN 1

CYBER SECURE SOCIETY

INTRODUCTION

To create a safe digital infrastructure and to manage the challenges of an ever changing and evolving cyber security landscape, it is essential for Dubai's public and private sector to have sufficient cyber security capabilities. Starting from executives and experts through to any employee. To accomplish this, suitable training needs to be provided, as well as dedicated up-skilling and re-skilling of experts, through individually shaped courses.

Another important element of the Cyber Secure Society domain is to ensure that any individuals in Dubai, irrespective of background, education, or personal situation, have awareness of cyber security. Programmes designed for children, students and other individuals will achieve that.

OBJECTIVES

1.1. CULTIVATE CYBER SKILLS

Cyber security risks and attacks are constantly increasing. In this environment, it is important for Dubai's well-being that both public and private organizations have a well-educated workforce.

- Adequate formal training should be provided to build such a workforce. It needs to include training for executives, operational and technical training for cyber security experts, and all other employees of an organization. The training should be accompanied by conferences, workshops, and other activities.
- A clear career path for cyber security experts needs to be outlined, starting from well-planned internships and training programmes, through the use of national and international certification of security professionals, based on the needs identified by the industry and

government. Incentives for individuals to take such a career path, and for public and private organizations to support such initiatives, should be provided.

- Dubai's public and private sector and universities should work together to increase the number of cyber security experts and motivate talented people to join the field. This development needs planning and should start early on and schools and universities should include cyber security in their curricula. In addition, interest raising for cyber security should start in school, and schools should develop curricula to address this subject.

1.2. FOSTER ACCESSIBLE CYBER SECURITY

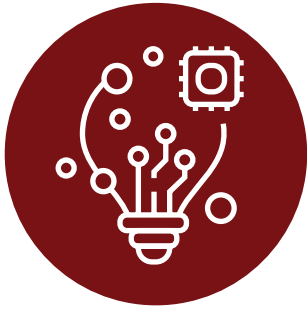
In addition to cultivating cyber skills, cyber security awareness should be provided to public and private sectors' employees.

- This needs to cover cyber security threats and risks, and the employees' responsibilities for information security, why their support is needed, and what happens if cyber security policies and procedures are violated. Organizations should implement a holistic and continuously developing awareness programme, addressing all employees, including newcomers. More and more people have been subject to cyber-attacks in the last few years, and this number is rapidly increasing, especially with new technologies that will play a larger part in our lives.
- A campaign should be developed coordinating cyber security awareness at the Dubai level to provide awareness to individuals about cyber security, the threats, and risks of the cyberspace, and how to protect against them.
- The individual campaigns should be oriented to target groups using different forms of delivery to raise awareness for cyber security, addressing the general public, children, elderly people, different language groups, and other target groups. It is important that no one is excluded and that all means of outreach are used. The campaigns should also use the offers made by DESC and other entities to learn more about cyber security.



**“UAE IS AN
INCUBATOR OF
INNOVATION
AND FUTURE
TECHNOLOGY.”**

His Highness Sheikh Mohammed bin Rashid Al Maktoum
Vice President and Prime Minister of the UAE and Ruler of Dubai



DOMAIN 2

INCUBATOR FOR INNOVATION

INTRODUCTION

Strong research and innovation capabilities, activities, institutions, and partnerships are needed to keep Dubai at the forefront of cyber security and protected against cyber-attacks. This helps to strengthen ongoing resilience and the generation of new economic opportunities.

Dubai leadership's support for research and the adoption of emerging technologies makes Dubai an ideal hub for bringing new ideas to life. This will inevitably lead to the development of new solutions, with significance in managing the latest cyber security challenges.

OBJECTIVES

2.1. PROMOTE CYBER SECURITY RESEARCH AND BUILD AN INNOVATION ECOSYSTEM

The different activities listed below demonstrate how Dubai creates an environment that supports research and development and achieves innovation by building a secure cyberspace. These outcomes include a combination of public and private sector organizations, universities, and talents—all of these should work together to arrive at new cyber security solutions:

- It is important to further promote interdisciplinary research, finding ways of effective dissemination of new solutions, technologies, or processes. Dubai's cyber security research and development (R&D) programme will address emerging technologies, but also link into non-technical fields like social, business, and management to address the all-pervasiveness that cyber security has nowadays.
- The R&D support will continue by creating new incentive schemes for cyber security innovations, in addition to those already existing, and to encourage the development of innovative cyber security solutions, products and services.

2.2. SECURE APPLICATION OF EMERGING TECHNOLOGIES

- Emerging technologies, such as Internet of Things (IoT), Artificial Intelligence (AI), Virtual Reality (VR), Blockchain, and other technologies used in building smart cities are already in common use and in most people's minds; with all the huge opportunities these technologies bring, they can also pose risks as attackers might use these technologies to their advantage. It is therefore necessary to understand these emerging technologies, and the individual risks they can bring; a good example is quantum computing, which poses a big threat to conventional encryption. Once the risks and potential attack vectors have been identified, suitable solutions, services and processes can be developed that integrate security by design. This will help to promote the secure use of the emerging technologies, as well as establishing Dubai as the place for their development.
- Secure use of emerging technologies is a complex topic, using combination of different approaches and technologies are most promising. One part of this is the support for start-ups that work in the area of emerging technologies' security, through accelerator programmes or incorporation in the R&D programme. In addition to creating new solutions, the integration of already existing capabilities can be very helpful. This includes the attraction of cyber security companies that have been demonstrating success in other parts of the world, as well as strengthening the cyber security capabilities of Dubai's government entities, and the identification and growth of local champions.

2.3. GROW THE ASSURANCE ECOSYSTEM

One important cornerstone of using emerging technologies securely is the trust that organizations and people will have in the cyber security products, services, and experts provided. An internationally agreed means of providing trust is certification.

Initiatives should introduce new certification schemes that address security in emerging technologies, such as:

- Certification of products can use the international scheme for product certification with additions, modifications and the specific requirements of the technologies involved that reflect the local environment.
- Certification of services, such as insurance or Blockchain, can expand on international standards on the topic in consideration with the right number of additions related to the environment in which the services are provided.
- Certification of cyber security experts for emerging technologies can include activities that relate to the current specifications of cyber security work roles, including any other tasks that may be relevant.

The standards for this scheme and the associated certifications need to be developed and should be based on international best practices.

**“IN THE FACE OF
CONSTANTLY EVOLVING
THREATS, WE CONTINUE
TO BE COMMITTED TO
REINFORCING OUR
CYBER SECURITY
MECHANISMS. THE NEW
STRATEGY OUTLINES
OUR DETERMINATION TO
MAINTAIN THE HIGHEST
LEVELS OF PROTECTION,
RESILIENCE AND
SECURITY AWARENESS.”**

His Highness Sheikh Hamdan bin Mohammed bin Rashid Al Maktoum
Crown Prince of Dubai and Chairman of the Executive Council



DOMAIN 3

RESILIENT CYBER CITY

INTRODUCTION

Cyber resilience is a very important concept in achieving protection of Dubai's public and private sector; some of the underlying concepts play a fundamental part in achieving adequate protection, such as governance, risk management, resilience, and Critical Information Infrastructure (CII) protection.

- It is the objective of this strategy to expand the cyber security governance structures in Dubai's public and private sector to enable successful digital transformation, based on the activities that have been completed. DESC will support Dubai's organizations in implementing the identified levels of security. All cyber security efforts should be based on the management of risks, therefore understanding the risks an organization is facing is key to establishing the necessary protection.
- Another aim of this strategy is to ensure that organizations of Dubai's public and private sectors, particularly organizations in the Critical Information Infrastructure (CII) are resilient to cyber-attacks and can continue their important business operations even in cases of problems. A key element to delivering such resilience is the establishment of a facility that provides support for the management of cyber security incidents, threat intelligence and a platform for information sharing.

OBJECTIVES

3.1. SHAPING THE GOVERNANCE OF CYBERSPACE

One of the most effective cyber security controls is the establishment of governance, in order to do so, the following points should be ensured:

- Senior management understands the importance of cyber security and sees it as an enabler for the organization to grow and achieve their business objectives; senior management ensures that governance processes are in place.
- Responsibilities for cyber security are clearly assigned; employees have the knowledge and skills for these responsibilities or receive the necessary training; success is clearly measured, communicated, and rewarded.
- Cyber security risks are well managed; the right risk assessment approaches are in place; the specific risks an organization faces are understood and making decisions based on these understandings are a fundamental part of governance.
- A plan for the implementation of cyber security policies, procedures, and technical controls are in place, including timelines and measures of success.

3.2. EXTEND THE RESILIENT CYBER ECOSYSTEM

DESC will continue to support Dubai's public and private sector and collaborate with competent authorities to set further standards, guidelines and tools for cyber security and resilience. The main topics that are of interest for future developments include, but are not limited to the following:

- Security for the supply chain: Securing the trustworthiness of the elements comprising the supply chain including devices being manufactured, the data generated and distributed in devices, and the services that use them.
- Security by design: Developing and implementing the approach to include cyber security in the system development lifecycle.
- Cyber security insurance: A new concept to support organizations achieve protection, possibly in areas where their own capabilities might not suffice.
- Standards and guidelines related to emerging technologies: Threats and risks related to emerging technologies might make the development of standards and guidelines in these sectors necessary.

This will be supported by a programme for the implementation of the standards, including activities to further explain the standards, their content and what to do for their implementation, as well as certification efforts.

In addition, DESC is in the process of developing a detailed breakdown of cyber security roles, in terms of tasks, knowledge, skills, abilities, experience, and qualifications. This will help Dubai organizations to better understand their needs and shape a clear career path for those wishing to have a career in cyber security. The implementation and associated training courses will be provided through international collaboration.

3.3. MANAGE CYBER CRISES AND INCIDENT RESPONSES

The first step in managing a cyber crisis is to identify that a crisis is happening. The Dubai Cyber Index plays a major part in this endeavor. The more organizations join this index, the greater the system is able to understand what is taking place in the region. This provides a better, holistic picture of attacks, making it possible to alert organizations and suggest rectification plans, in order to avoid possible vulnerabilities.

DESC already monitors and analyses the cyber threat and risk landscape and is working to extend the information sharing and threat analysis capabilities.

- For the development of a new information sharing platform, public and private sectors must build relationships of trust. The more they actively collaborate and cooperate in providing information, the more benefit they receive from the system. This initiative should start with the public sector, relationships with the private sector are expected to follow when all participants understand that proactively sharing information about cyber security incidents is positively regarded. Once the information sharing platform is established, DESC will provide intelligence by linking different sources and using the information and technical capabilities available.
- Once cyber incidents or crises have been identified, and the information sharing platform and the threat analysis capabilities have helped to categorize the event, it is time to take counter action. This includes each organization's individual response, framed by overarching plans relating to e.g., the CII. Any of these activities have a greater chance for success if everyone involved is aware and knowledgeable of what they need to do. Cyber drills are an important part of building incident response plans and capabilities. They also improve communication and coordination between the CII operators and government agencies. Exercises for specific sectors can go into more complex scenarios and more sophisticated, individual attack methods. Dubai-wide exercises will incorporate more sectors, with an emphasis on the interdependent nature of essential services. This will facilitate coordinated management of any given situation.

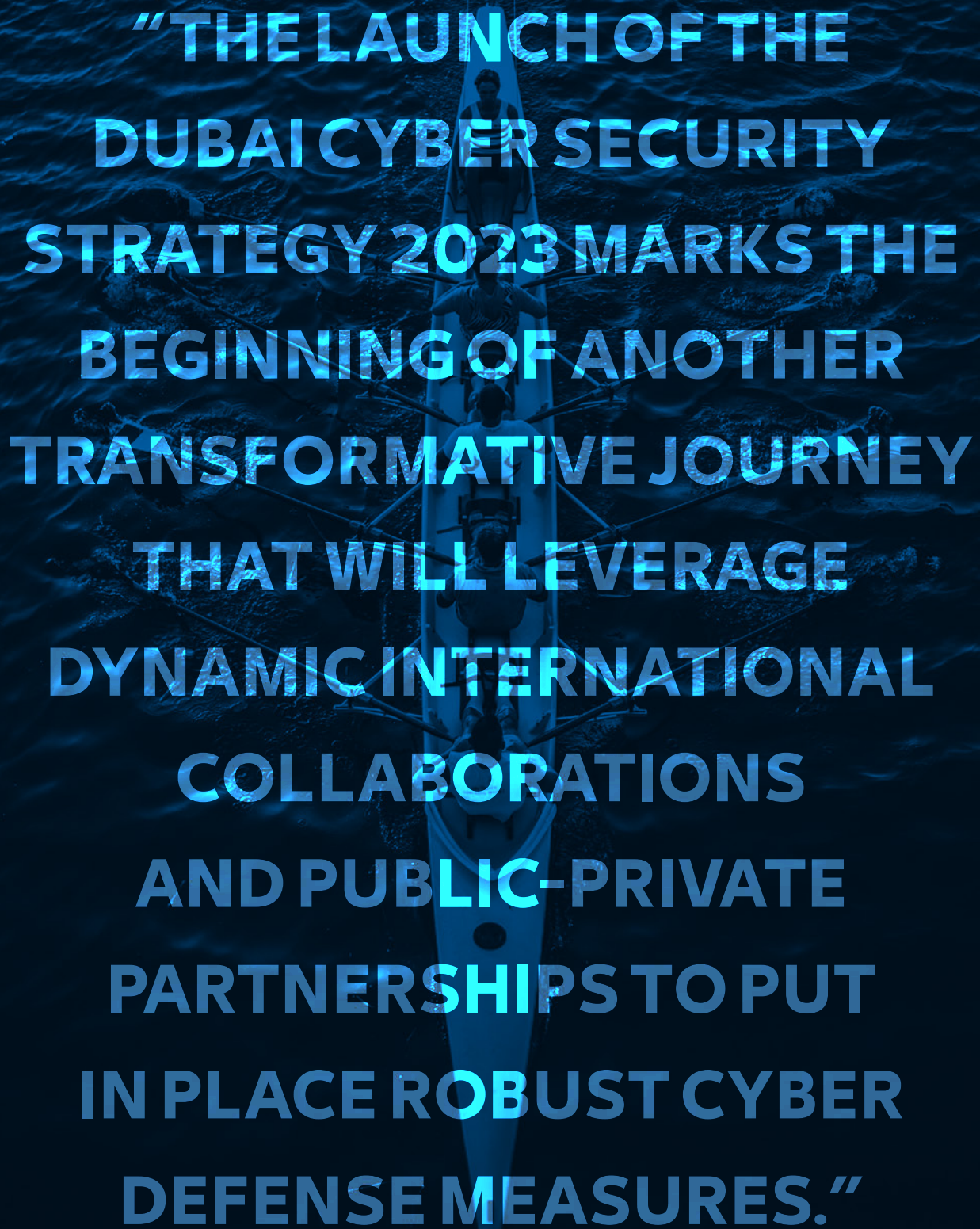
3.4. AMPLIFY RESILIENT CYBER INFRASTRUCTURE

Resilience is essential in times when incidents occur, and breaches cannot be entirely ruled out. This particularly applies to Critical Information Infrastructure (CII) organizations, but all of Dubai's important organizations should be sufficiently secure and resilient. This requires a multi-tier approach:

- There is a need to identify and manage incidents, and, as part of that, to have a good understanding of threats and risks.
- There is also a need for organizations to be strong enough to withstand at least initial levels of attack. This need exists for all organizations in Dubai's public and private sector. All organizations should be able to revert to normal operations in pre-determined time frames,

based on their business continuity and disaster recovery plans. Depending on the nature of business or as part of the CII, there might also be a need to operate in a restricted fashion over some time – all of this is also dependent on the functional plans these organizations have. It is mainly the responsibility of the organization to have good business continuity and disaster recovery in place, but DESC and other governmental agencies can support this through the provision of standards, audits, technical support and more.

- Finally, there are the attacks that span across multiple organizations leading to an attack on Dubai as a city or significant parts of it. Cross-organizational resilience plans need to be developed, applying the understanding of interdependencies of the CII organizations with others, and making plans to protect against a holistic attack. First steps in this direction have been made (cyber resilience guideline). Now is the time to bring this to the next level, particularly regarding the collaboration between Dubai's public and private sector. This can and should also make use of the new technologies to achieve more automation in resilience efforts.

A rowing team in a blue boat on dark water, with the text overlaid.

**“THE LAUNCH OF THE
DUBAI CYBER SECURITY
STRATEGY 2023 MARKS THE
BEGINNING OF ANOTHER
TRANSFORMATIVE JOURNEY
THAT WILL LEVERAGE
DYNAMIC INTERNATIONAL
COLLABORATIONS
AND PUBLIC-PRIVATE
PARTNERSHIPS TO PUT
IN PLACE ROBUST CYBER
DEFENSE MEASURES.”**

His Highness Sheikh Hamdan bin Mohammed bin Rashid Al Maktoum
Crown Prince of Dubai and Chairman of the Executive Council



DOMAIN 4

ACTIVE CYBER COLLABORATION

INTRODUCTION

In a world that relies on the use of digital communications to conduct trade and other business on an ever-growing scale, it is important to realize the cross-boundary characteristics of the threats and risks involved. Threats and risks do not stop at national borders; equally, they do not recognize barriers between different areas, peer groups, or organizations. Quite often, commonalities even facilitate attacks. Therefore, national, and international collaboration, with regard to many different topics is imperative.

OBJECTIVES

4.1. EXTEND LOCAL COLLABORATIONS

While the track record of initiating and fostering local collaborations is already very impressive, there is room for expansion:

- Development of a cross-sector cyber security and cyber resilience protection plan for CII organizations, to address threats and risks that target more than just a few organizations.
- Further harmonization with regards to cyber security and cyber resilience policies, standards, and other activities across the UAE, utilizing for example the UAE Cybersecurity Council.
- Incorporation of more organizations in the Dubai Cyber Index.
- Identification of more areas of public-private collaborations, including start-ups, to make use of their expertise in particular areas, and ways of information sharing with private organizations that are not in conflict with any governmental policies.

4.2. CONTRIBUTE TO INTERNATIONAL CYBER SECURITY EFFORTS

One of the main interests in increasing participation in international forums is to enhance Dubai's global image as a cyber security leader, by bringing additional value to discussions.

- This can be achieved through the continuation of efforts in aligning national and international policies, standards, and certification processes. The harmony achieved in this matter will strongly support cross-border handling of problems, information exchange, and experts moving seamlessly from one place to another.
- Another area is to continuously look for other partners by fostering international collaboration, possibly extending the approach from well-known global organizations to more research and development focused groups, or even private companies. To this end, bilateral agreements, memoranda of understanding, formal and informal communications, and anything else that works can be used. In the end, the better cyber security threats and risks are managed, the more beneficial the results will be.
- Finally, support from the national efforts is needed in order to make international collaboration of any kind successful. The more the United Arab Emirates as a nation and Dubai as a city have to offer in terms of knowledge and expertise, the more fruitful our international collaboration will be.

ACHIEVEMENTS ROADMAP



MAY 2017

DUBAI CYBER
SECURITY
STRATEGY



JUNE 2017

ESHARAT
MAGAZINE



OCTOBER 2017

INFORMATION
SECURITY REGULATION
VERSION 2



DECEMBER 2017

INTERNET OF THINGS
(IOT) SECURITY
STANDARD



FEBRUARY 2019

DATA CENTRE (DC)
SECURITY
STANDARD



NOVEMBER 2018

CONNECTED
VEHICLE (CV)
SECURITY
STANDARD



OCTOBER 2018

CYBER SECURITY
LABS



FEBRUARY 2018

CALL FOR
RESEARCH



MAY 2019

WEB SECURITY
POLICY



AUGUST 2019

CLOUD SERVICE
PROVIDER (CSP)
SECURITY
STANDARD



JANUARY 2020

MALWARE
INFORMATION
SHARING PLATFORM



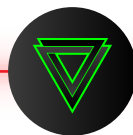
MARCH 2020

INDUSTRIAL
CONTROL SYSTEMS
(ICS) SECURITY
STANDARD



MARCH 2022

DUBAI CYBER
INNOVATION PARK
(DCIPARK)



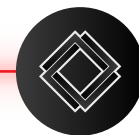
JUNE 2021

TIRS



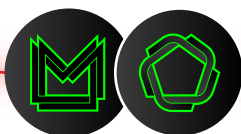
DECEMBER 2020

ELECTRONIC
BIOMEDICAL DEVICES
SECURITY STANDARD



JULY 2020

DUBAI CYBER
INDEX



MARCH 2022

TAREH &
ALKASHIF



MARCH 2023

CYBER FORCE &
RZAM



JUNE 2023

DUBAI CYBER
SECURITY STRATEGY
2023

