



المركز العربي الإقليمي للأمن السيبراني  
ITU - ARAB REGIONAL CYBERSECURITY CENTER



# ITU Arab Regional Cybersecurity Center

Annual Report 2018-2020

## Contents

	<b>Speech of the Ministry</b> of Transport, Communications & Information Technology	<b>3</b>
	<b>Speech of Arab Regional Cybersecurity Centre</b>	<b>5</b>
	<b>About the Centre and the Report</b>	<b>7</b>
	<b>First: Capacity Building</b>	<b>10</b>
	<b>Second: Institutional Organisation</b>	<b>24</b>
	<b>Third: International Co-operation</b>	<b>28</b>

### **Dr. Ali bin Amer Al Shidhani**

**Undersecretary of the Ministry of Transport, Communications and Information Technology for Communications and Information Technology**

### **Speech of the Ministry of Transport, Communications & Information Technology**

The Sultanate, represented by the Ministry of Transport, Communications and Information Technology, attaches great importance to cybersecurity because it is a basic component of technology and communications, as well as being important for the digital economy. Moreover, with the rapid technological development in this field and the consequent restructuring of economic and social dealing forms and professional and educational practices in line with the Fourth Industrial Revolution and its accompanying applications, in addition to the conditions imposed on the world by Covid-19 pandemic, which have necessitated finding effective means to confront the cyber risks and threats that have become a major challenge to national and international security more than ever.

The Ministry has been keen, through the ITU Regional Cybersecurity Centre (ITU-ARCC), which the Sultanate has been hosting since 2012, to reinforce the role of the ITU in building confidence and security in the use of information and communication technology, to contribute to enhancing cybersecurity in the region and the world. ITU-ARCC is in support of Member States in raising readiness in the field of cybersecurity.



In addition, cybersecurity is not only limited to the technological risks and threats, but it is also an economy in its own in light of what has been imposed by the rapid developments in the fields of communications and information technology and the Fourth Industrial Revolution and the consequent development in the methods used by Internet and information hackers to carry out their electronic hacking. Therefore, through ITU-ARCC, the Sultanate has focused on addressing the services provided by the Centre to include capacity building, technological, institutional and legal aspects, in addition to international coordination and cooperation in line with the global agenda of cybersecurity.

In addition, while we affirm Oman's commitment to contribute to strengthening international peace and security at the regional and global levels, the situation applies at the same time to the aspect of cybersecurity which has become the cornerstone of enhancing international security and peace, especially in light of the digital economy whose pace is accelerating in a way that achieves the aspirations of the peoples and countries of the world. Accordingly, efforts and initiatives of the Regional Cybersecurity Centre will continue to provide support and assistance to the Member States of the Union in everything that serves their needs to strengthen the cybersecurity system and contribute to advancing comprehensive development.



### Eng. Badar Al Salehi

Director General, Oman National CERT  
Head of the ITU Arab Regional Cybersecurity Centre (ITU-ARCC)

### Speech of ITU-ARCC

On behalf of ITU-ARCC work team, it gives me great pleasure to review the most important achievements and initiatives that the Centre has implemented, in cooperation with the Member States and the ITU, in various aspects of work during the past three years, which have contributed to enhancing cybersecurity at the regional and global levels and building confidence and security in the uses of information and communication technology. We also seek, through this report, to highlight the efforts and initiatives made by the Member States of the ITU in cooperation with the Centre in the field of cybersecurity, which indicates the regional and global interest in this vital and important sector at the strategic and operational levels in light of the accelerating trend towards digital transformation and electronic services activation, in addition to the paradigm shift associated with the Fourth Industrial Revolution and its challenges.

The past three years witnessed a continuation of ITU-ARCC work in the fields of cybersecurity adopted by the ITU, realising the trust conferred by the ITU and the Arab countries to the Sultanate to play this important strategic regional role. Despite the economic crisis that the world is going through, the Centre has been able to interact with the challenges thanks to the strenuous efforts of its employees and the various concerned work teams at Oman National CERT, bearing in mind the implementation of ITU-ARCC vision. We extend our appreciation and thanks to them and look forward to a new phase of work and construction in the coming years, seeking to enhance confidence and security in the use of information and communication technology.

ITU-ARCC has supported the Member States in the Arab region to develop and improve aspects of cybersecurity through the development of the strategies, policies, human capabilities, the necessary tools, applications, models and procedures that enhance cybersecurity at the regional and international levels.

The achievements of the Centre included the following aspects:

- Assistance and responding to the cybersecurity requirements in the least developed countries in the region.
- Acting as an administrative centre and platform for carrying out the cybersecurity goals in the region.
- Creating a common umbrella that brings together Member States to enable them to manage cybersecurity programs and initiatives in the region.
- Enhancing awareness and experience in dealing with the cybersecurity aspects of the vital infrastructure sectors.
- Preparing national strategies for cybersecurity and capacity building in this field.
- Organising conferences, seminars and specialised workshops.
- Creating partnerships and cooperation with international organisations and institutions concerned with cybersecurity to enhance what the centre offers to the ITU Member States.
- Organising regional drills to assess readiness to respond to emergencies and cybersecurity incidents.
- Organising national and regional competitions in the field of cybersecurity.

The efforts and initiatives of the Centre over the past years resulted in the implementation of more than 162 projects and events in various fields of cybersecurity that targeted more than 10000 participants from 26 countries around the world.

In conclusion, once again I extend my thanks and appreciation to my colleagues at ITU-ARCC and all the countries, institutions and experts who contributed to the success of the Centre's activities and participated in the aforesaid achievements.



**Adel M. Darwish**  
Regional Director  
Arab Regional Office

It is a pleasure for me to see the great activities and impressive achievements of the Arab Regional Cybersecurity Center (ARCC) in enhancing the regional cooperation in the cybersecurity field.

At ITU, building confidence and security in the use of ICTs remains one of our top priorities. As we have our eyes fixed on bringing the unconnected 3.6 billion people online, we must also give equal attention to areas that may hinder the meaningful and effective use of the web. Digital security in the context of digital transformation, is at the heart of the opportunities and challenges of future digital development. Digitalization is increasingly integrated into societies, modern economies, governments, and countries worldwide.

Never before have ICTs been so vital to our lives, and to keep our economy and society working, as during the COVID-19 crisis we are living through today, Pandemic has thrown a spotlight on connectivity and the need for resilient digital infrastructure. We find ourselves at a critical point trying to leverage the transformational power of ICTs and the Internet to act as catalysts for economic growth and social development. Cybersecurity is essential to ensure effective and inclusive digital transformation.

Therefore, I would like to emphasize how crucial is the role of the ARCC in developing and implementing its activities in building capacity and awareness, supporting countries in developing cybersecurity strategies and establishing cybersecurity centers, and support cooperation in the region.

It is clear from this report that ARCC activities and impact are enhancing in maturity and reach, and I am sure that ARCC will gain new momentum in the near future with innovative services in Cybersecurity.

I am very grateful to the Government of Oman for making available its expertise and financial contributions, to support and develop this center together with ITU, Also I would like to praise the ARCC management and staff for the quality of their work, which is the result of their commitment and professionalism.

ARCC, which has been the first Regional Cybersecurity Centre, has today become a successful model for future Cybersecurity Regional Centers all around the world.

I would like to emphasize that in our world which is typified by interconnectedness, cybersecurity has become a shared responsibility that should unite us in committing to enhancing capacity, resilience, and inclusiveness in digitalization at the national, regional and international levels.

To reap the benefits and manage the challenges of digitalization, countries need to frame the proliferation of ICT-enabled infrastructure within a comprehensive cybersecurity posture. ITU is fully committed in facilitating the establishment of more regional cybersecurity centers worldwide. This will support the access and use of the services and capabilities that can concretely assist Member States, and specifically developing countries, in building confidence in ICT and digitalization.



## About the Centre

ITU-ARCC was established as an initiative by ITU and Sultanate of Oman in December 2012 represented by the Ministry of Transport, Communications and Information Technology (formerly Information Technology Authority) and was officially launched on March 3, 2013 in Knowledge Oasis Muscat, and is being hosted, managed and operated by Oman National CERT of the Ministry.

The Centre aims to enhance cooperation in the field of cybersecurity and strengthen the role of ITU in building confidence in the use of information and communication technology.



## About the Report

This report includes the achievements and projects of the ITU-ARCC during the past three years (2018, 2019 and 2020) through reviewing the most important events, seminars, drills and various activities which were implemented during that period. The report includes several axes:



### First: Capacity Building

Drills

Competitions

Seminars & Conferences

Courses & Workshops

Awareness



### Second: Institutional Organisation

Cybersecurity Strategy

Establishing Information  
Emergency Response  
Centres



### Third: International Co-operation

Regional & International  
Meetings

Joint events



# First: Capacity Building



- 1 - Drills
- 2 - Competitions
- 3 - Seminars & Conferences
- 4 - Courses & Workshops
- 5 - Awareness

## First: Capacity building in the field of cybersecurity





## First: Capacity building in the field of cybersecurity

During the past three years, the Centre made great efforts in the field of training and qualifying, as follows:

### 1. Drills

Based on the Centre's role to improve the skills of national cadres in the Member States, a number of specialised drills were organised targeting capacity building and expertise to handle various risks in cyberspace. Among the most important drills that were carried out during the years 2018, 2019 and 2020 are the following:

#### The sixth regional cybersecurity readiness assessment drill

23-25 October 2018 | Kuwait

On the side-lines of Regional Cybersecurity Week, ITU-ARCC organised the sixth edition of the regional drill for assessing readiness in the field of cybersecurity, during the period from 23 to 25 October 2018.

The drill aimed to strengthen cooperation between Arab and regional countries in the field of information security and to identify appropriate mechanisms to deal with attacks and threats in cyberspace, as well as exchanging experiences and ensuring the readiness of participating countries in handling cyber-attacks and confronting them.



#### ITU Cybersecurity Drill, 2018

26 - 30 November 2018 | Limassol - Cyprus

ITU-ARCC participated in the activities of the ITU's International Cybersecurity Drill, which was organised in Saint Raphael Resort, Limassol, Cyprus during the period 26-30 November 2018.

The drill aimed to enhance the cyber readiness to handle cyber incidents facing governmental institutions in the participating countries, by enhancing cooperation between emergency response centres and security incidents around the world, as well as training and qualifying national cadres to deal with cyber threats at the international level.



### Regional Drill for Emergency and Security Incidents Response Teams for Asian Countries

23-27 September 2019 | Kuala Lumpur, Malaysia

A number of experts from ITU-ARCC participated in the activities of the regional drill for emergency and security incidents response teams, which was organised during the period from 23<sup>rd</sup> to 27<sup>th</sup> September 2019 in Kuala Lumpur, Malaysia.

The drill included workshops and scenarios simulating malware threats and training on how to analyse and handle them.



### The seventh regional readiness assessment drill

October 31, 2019

The seventh regional readiness assessment drill was organised on the sidelines of the activities of the Regional Cybersecurity Week. Its idea relied on implementing hypothetical attacks for the participating teams to analyse and handle them. The drill included 7 scenarios which simulated attacks against Internet of Things (IOT) systems and smart city applications. Interactive scenarios were also implemented by a number of companies: (Kaspersky, Fortinet, Silentech, and Cyber Services).



### The eighth regional drill and the OIC Cybersecurity Readiness Assessment 2020 drill

September 22, 2020 | Virtual

Within the cooperation between ITU-ARCC and the Organisation of Islamic Cooperation (OIC-CERT), the eighth regional drill for Arab countries was organised in the Sultanate for the third time, respectively, by Oman National CERT in conjunction with the OIC-CERT Cybersecurity Readiness Assessment Drill, under the circumstances of Covid-19 pandemic, under the name "The Eighth Regional Drill and the Organisation of Islamic Cooperation Drill for Cybersecurity Readiness Assessment 2020."



The joint drill was organised virtually (via the Internet) under the slogan «Control of cybersecurity risks associated with remote work», with the participation of 25 teams from 24 countries, representing the national and Arab teams for information emergency response, special teams and information security centres in the main sectors.

### International Cybersecurity Drill 2020- Virtually 27th October – 5th November, 2020

ITU-ARCC, in cooperation with ITU, organised the activities of the International Cybersecurity Drill during the period from October 27 to November 5, 2020, with the participation of more than 400 specialists from 57 countries.

The drill focused on: Cyber threats and challenges resulting from Covid-19 pandemic in the health care sector, with the aim of enhancing cyber readiness to handle cyber incidents that government institutions are exposed to in the participating countries, by strengthening coordination and cooperation between emergency response centres and security incidents around the world, as well as training and qualifying national cadres to handle cyber threats better at the international level.



### 2- Competitions

Over the past 3 years (2018, 2019 and 2020), the Centre organised a number of competitions with the aim of qualifying national cadres and improving their skills in the field of cybersecurity, and enhancing their capabilities to compete at the regional and international levels. The most important of these competitions are:

#### Threat Hunters competition in partnership with Silensec

This competition is organised in some Member States of the Centre, after which the winners from each country are qualified for the regional competition. At the local level, this competition was organised as follows:

Years	Country	No. of Participants	Years	Country	No. of Participants
2018	Sultanate of Oman	284	2020	Sultanate of Oman	300
	Tunisia	59		Kuwait	20
	Qatar	20		Syria	95
	Egypt	90		Tunisia	95
	Palestine	62		Qatar	35
	Kuwait	73		Sudan	42
2019	Sultanate of Oman	22		Lebanon	20
				Egypt	60
		Morocco		20	
		Palestine	48		



The Centre also organised the activities of the threat hunter competition at the regional level as follows:

Years	Drill axes	Participating countries	No. of participants
2018	<ul style="list-style-type: none"> <li>Ethical hacking</li> <li>Protecting the information technology and communication Infrastructure systems</li> <li>Malware analysis</li> <li>Digital evidence analysis</li> </ul>	10 Arab countries: Sultanate of Oman, Tunisia, Egypt, Kuwait, Qatar, Libya, Palestine, Jordan, Algeria and Saudi Arabia.	<p>The competition targeted 738 specialists, students, and those interested in cybersecurity. 114 of them were qualified to compete in the qualifying stage. In the final stage 27 participants were qualified, 3 contestants of them won, they are:</p> <p>Rami bin Thani Al Amri from Sultanate of Oman won in the "Attacker" category,</p> <p>Moaz Abdul Qadir Qadura from the State of Qatar won in the "Defender" category, and Barakat Abdul Rahim Barakat from the State of Palestine won in the category of Responders for Security Incidents.</p>
2019	<ul style="list-style-type: none"> <li>Ethical hacking</li> <li>Protecting the information technology and communication Infrastructure systems</li> <li>Malware analysis</li> <li>Digital evidence analysis</li> </ul>	7 Arab countries: Sultanate of Oman, Tunisia, Kuwait, Libya, Palestine, Lebanon and Sudan.	<p>In its third edition, the competition targeted more than 300 professionals, students and those interested in cybersecurity; 114 of them were qualified to compete in the qualifying phase to confront a series of challenges; After that 27 participants were qualified for the final stage and 3 contestants won in the following categories:</p> <p>Defender Category: Moaz Abdul Qadir, from Qatar.</p> <p>Attacker Category: Rami Bin Thani Al Amri, from Sultanate of Oman.</p> <p>Responder to Security Incidents Category: Barakat Abdul Rahim, from Palestine.</p>
2020	<p>The 2020 edition was distinguished by the development of scenarios which simulate the security challenges resulting from Covid-19 pandemic in the fields of cybersecurity to prepare the next generation of interested and specialists in the field of cybersecurity and to enhance their capabilities to compete at the regional and international levels.</p> <p>The competition focused on several questions and challenges in different areas of cybersecurity, namely:</p> <ul style="list-style-type: none"> <li>Ethical hacking</li> <li>Protecting the information technology and communication infrastructure systems.</li> <li>Malware analysis.</li> <li>Digital evidence analysis.</li> </ul>	10 Arab countries: Sultanate of Oman, Kuwait, Egypt, Qatar, Palestine, Syria, Sudan, Tunisia, Morocco and Lebanon.	<p>The competition targeted more than 1000 participants, including specialists, students, and those interested in cybersecurity.</p> <p>The results were as follows:</p> <p>Category A, (Age: 17-24), the winners are:</p> <p>First place: Sama Crow, from Tunisia.</p> <p>Second place: Seif El-Din Tariq Aziz, from Egypt.</p> <p>Third place: Yasser Mohammed Abdul Monem Ali, from Egypt.</p> <p>Category B, (Age: 24 and over), and the winners are:</p> <p>First place: Seif-Eddin Aidi, from Tunisia.</p> <p>Second place: Ayman Al-Borgi, from Tunisia.</p> <p>Third Place: Anis Hamdi, from Tunisia.</p>

### 3. Seminars & Conferences

ITU-ARCC held a number of seminars and conferences and participated in some of them as a supporter or partner. The following are among the most important of them:

#### Middle East and North Africa Health Information Security Conference

26-27 March 2018 | UAE

The Centre participated as a support partner in the Middle East and North Africa Health Information Security Conference, which was organised in Dubai, United Arab Emirates, during the period from 26<sup>th</sup> to 27<sup>th</sup> March 2018. The conference discussed issues and challenges of cybersecurity in the health sector and developed strategies and solutions to avoid cyber threats and risks.



#### Arab Information Security Conference

23-24 September 2018 | Cairo, Arab Republic of Egypt

ITU-ARCC participated in the Arab Information Security Conference as a supporting partner the event, which was held in Cairo, Arab Republic of Egypt, from 23<sup>rd</sup> to 24<sup>th</sup> September 2018, at the Nile Ritz-Carlton Hotel.



#### Regional Cybersecurity Week-2018

21-25 October 2018 | Kuwait

Under the slogan "Cybersecurity Readiness in the Fourth Industrial Revolution", the Centre organised the activities of the Regional Cybersecurity Week (RCW) during the period from 21<sup>st</sup>-25<sup>th</sup> October 2018. The events of the week were hosted by the Public Authority for Communications and Information Technology, at the Jumeirah Hotel, Messilah Beach, Kuwait, with the participation of 36 international speakers and 270 specialists from 35 countries.

Among the objectives of the conference: reviewing the best strategies to address cyber threats, exchanging experiences, enhancing cooperation between Arab countries in the field of information security, and identifying appropriate mechanisms to handle the attacks and threats in the Arab and international cyberspace, especially in light of technological progress.



## Information Society Summit Forum - 2019

8-12 April 2019 | Switzerland

Within a delegation from the Ministry of Transport, Communications and Information Technology, including Eng. Bader bin Ali Al Salhi (Head of ITU-ARCC) and a number of specialists from the Ministry, the Centre participated in the work of the Information Society Summit, which was held in Geneva, Switzerland, during the period from 8<sup>th</sup> to 12<sup>th</sup> April 2019. During the participation, a meeting took place with “Houlin Zhao”, Secretary General of the ITU.



## Regional Cybersecurity Week 2019

27-31 October 2019 | Sultanate of Oman

With the participation of more than 600 specialists from 45 countries, the Centre organised the regional cybersecurity week activities, during the period from 27<sup>th</sup> to 31<sup>st</sup> October, 2019, in Muscat, Sultanate of Oman, and it was hosted by the Ministry of Transport, Communications and Information Technology, represented by the Oman National CERT, under the patronage of His Highness Sayyid Shihab bin Tariq Al Said, Advisor to His Majesty the Sultan.



### The activities of the week included:

- Organising the Eighth Regional Cybersecurity Conference on October 27-28, 2019, which focused on the technological development of the Fourth Industrial Revolution, assessed the measures necessary to reduce risks in integrated systems, and discussed the best practices for defining the national cybersecurity policy.
- Implementation of the Eighth Arab Regional Cybersecurity Drill under the title “Applied Learning for Emergency Response Teams in the Arab Region”. The drill targeted: national and Arab information emergencies response teams, special teams and information security centres in key sectors, with the aim of raising the level of communication and reducing the response time to information security incidents.
- The consultative meeting of the heads of the Arab National Centres for

Cybersecurity on October 28, 2019.

- The symposium of “First”, ITU-ARCC and the eleventh annual conference of OIC for Computer Emergency Response Teams, on October 29, 2019.
- The meeting of OIC Board of Directors on October 30, 2019.
- A training course provided by “First” for two days, 30-31 October 2019.
- Honouring the winners of the regional threat hunters competition, from Sultanate of Oman, Palestine and Egypt, at the conclusion of the Regional Cybersecurity Conference on October 28, 2019.

## First National Cybersecurity Conference

December 2-3, 2019 | Arab Republic of Egypt

ITU-ARCC participated in the activities of the First National Cybersecurity Conference, which was organised by the National Telecom Regulatory Authority in the Arab Republic of Egypt through a visual presentation on: “The best practices in cybersecurity centres”. The experience of the Sultanate of Oman was reviewed in a working paper entitled “The best practices in Oman National CERT”.



## The Fifth Gulf Forum on the Security of Operational Technology

1-4 March 2020 | Sultanate of Oman

ITU-ARCC participated as a “support partner” in the Fifth Gulf Forum on the Security of Operational Technology, which was held from 1<sup>st</sup> to 4<sup>th</sup> March 2020 in Sultanate of Oman, under the slogan: “Building a flexible infrastructure ICS”.



## The annual virtual conference of Middle East Women in Cyber Security

14-15 November 2020 | Sultanate of Oman

The Centre participated in supporting the annual Cybersecurity conference of the Middle East Women’s Association, which was organised virtually on 14<sup>th</sup> and 15<sup>th</sup> November 2020 under the slogan “To empower and secure together”. The Centre’s support for this event resulted from its role in supporting the empowerment of women in the information and communication technology sector.





### The 12th Annual Conference of OIC Member States for Cybersecurity Emergency Response Teams (OIC-CERT)

23 & 24 November 2020 | Sultanate of Oman

Under the slogan “Cybersecurity strategies and practices during the COVID-19 crisis”, the twelfth annual conference of the OIC Member States for Cybersecurity Emergency Response Teams (OIC-CERT) was organised virtually on 23<sup>rd</sup> & 24<sup>th</sup> November 2020 and chaired by Sultanate of Oman.

The annual conference is an ongoing initiative by OIC-CERT aiming to increase awareness and exchange experiences on cybersecurity issues, enhance the effectiveness and efficiency of members by improving handling of cyber incidents as well as creating a channel for communication about strategic trends and future challenges in cybersecurity.



## 4. Training Courses & Workshops

Among the most prominent training courses and workshops organised by the Centre during the past three years are the following:

### Specialised training courses in cybersecurity

11 & 12 November, 2018 | Muscat, Sultanate of Oman

The Centre, in cooperation with the National Centre CERT of the Ministry of Transport, Communications and Information Technology in Sultanate of Oman, organised a set of specialised training courses in the field of cybersecurity to build capacity to respond to cybersecurity emergencies, held in Muscat, Sultanate of Oman, on 11<sup>th</sup> & 12<sup>th</sup> November 2018.



### Network Traffic Analysis Workshop

14 & 16 January 2019 | Muscat, Sultanate of Oman

On 14<sup>th</sup> and 16<sup>th</sup> January 2019, the Centre organised a workshop entitled “Network Traffic Analysis” in cooperation with EGuardian Company, with the participation of more than 30 specialists in the field of network security and cybersecurity from various governmental institutions and the private sector. The workshop covered the challenges of network systems and how to handle and protect them from cyber threats.



### A training course in the field of cybersecurity

April 28 - May 2, 2019 | Muscat, Sultanate of Oman

The Centre provided a specialised training course for 5 days in the field of cybersecurity in cooperation with Oman National CERT in Sultanate of Oman. BSI was the strategic partner of the course.

The course focused on how to assess information security networks and introduce policies, procedures and models in the field of emergency response and cyber incidents.



### An intensive training course on ethical hacking

19-22 November 2019 | Kyrgyz Republic

The Centre organised an intensive training course on ethical hacking in the Kyrgyz Republic from 19<sup>th</sup> to 22<sup>nd</sup> November 2019, in the presence of more than 20 specialists in the field of cybersecurity.



### A workshop on protecting infrastructure for vital communications

October 27- November 5, 2020 | Virtual

In cooperation with the Centre for Humanitarian Dialogue in Switzerland, the Centre organised an online virtual workshop on October 26, 2020, entitled “Protecting the Infrastructure for Vital Communications”. Gulf Cooperation Council (GCC) and a group of OIC Member States were invited.

The workshop aimed at raising awareness level of the main electronic risks of vital communication infrastructure and developing recommendations on the ways of reducing these risks at the national and regional levels. A group of experts participated in the workshop, and gave a number of presentations and studies on protecting the infrastructure of the Internet, space, aviation, maritime navigation and ports systems.



### SAS accelerator program workshops for cybersecurity January 16, 2020 | Muscat, Sultanate of Oman

SAS Cybersecurity Accelerator Program is the first accelerator of its kind in the Middle East and North Africa. 55 cybersecurity professionals participated in the first group. They were divided into 8 teams and participated in a number of intensive workshops over a period of 5 months. Some of those workshops were held at the Ministry headquarters in Muscat and others were presented virtually, and organised by CyLon Cokmpany in the United Kingdom, with the aim of helping them improve their products and develop their ideas and projects.



## 5. Awareness

ITU-ARCC attaches great importance to awareness of various aspects of information technology. Hence, the Centre is keen to implement a number of awareness programs and campaigns in addition to participating in exhibitions and events that witness attendance of a great number of the public. The following are some of the most important efforts implemented by the Centre in this regard during the past period:

### Communications and Information Technology Exhibition (COMEX) 2018 and 2019 | Muscat, Sultanate of Oman

The Communications and Information Technology Exhibition (COMEX) is considered one of the most important specialised exhibitions in Sultanate of Oman. It witnesses an increasing demand from the public, as well as from government and private institutions.

The Centre participated in COMEX exhibition in 2018 and 2019 with the aim of introducing the roles and services provided by the Centre to the Member States of the ITU, in addition to raising awareness of information and communication technology crimes and meeting those interested and specialists in this sector.



### Cybersecurity Awareness Campaign “Tanabah”

1-4 March 2020 | Virtual

As a result of the repercussions of the global spread of the new Corona virus (Covid-19) and in line with the goals and vision of ITU-ARCC to create a safer and more cooperative environment in the Arab region, the Centre launched the electronic campaign “Tanabah” in March 2020 with the aim of enhancing awareness and culture of cybersecurity through the Centre’s social media platforms.

The campaign was carried out in cooperation among 7 countries, namely: Oman, Saudi Arabia, Egypt, Qatar, Tunisia, Lebanon, Syria, and in partnership with: Silensec, Kaspersky.

The Omani Association for the Hearing Impaired also participated in a sign language visual material which discussed the security measures that should be followed while using the Internet in light of Covid-19 pandemic.

The electronic campaign was implemented on the Centre’s social media sites:

- Facebook
- Twitter
- Instagram
- website





# Second: Institutional Organisation



- 1 - Developing Cybersecurity Strategies
- 2 - Establishing Cybersecurity Centres

## Second: Institutional Organisation



## 1. Developing Cybersecurity Strategies

### Workshop on National Cybersecurity Strategy

26-28 June 2019 | Skopje, Republic of North Macedonia

Hosted by the Republic of North Macedonia, the Centre participated in organising a 3-day workshop to develop national strategies in the field of cybersecurity for Eastern European countries.

The workshop included more than 30 decision-makers trainees from cyber emergency response Centres, relevant government institutions, and a number of companies and experts, with the aim of developing a framework for adopting a national cybersecurity strategy, which included programs and recommendations that contribute to enhancing cybersecurity capabilities.



### Workshop on National Cybersecurity Strategy

26-28 August 2019 | Jakarta, Indonesia

The Centre participated in organising a 3-day workshop in the capital Jakarta, Indonesia, to develop national cybersecurity strategies for East Asian countries.

The workshop included 50 participants from different institutions and decision-makers from cyber emergency response Centres and relevant government institutions, as well as a number of companies and experts, with the aim of developing a general framework for adopting a national cybersecurity strategy, which includes programs and recommendations that contribute to enhancing cybersecurity capabilities.



### Cybersecurity Strategies Workshop for the Arab Region and Africa

10 - 13 December 2019 | Republic of Tunisia

The Centre participated in organising a cybersecurity strategies workshop for the Arab region and Africa during the period from 10<sup>th</sup> to 13<sup>th</sup> December 2019, in the Republic of Tunisia.

The workshop aimed to review the best international practices in preparing national cybersecurity strategies and to benefit from the experiences and strategies of some participating countries in preparing action plans to implement the strategies.



## 2. Establishing Cybersecurity Centres

### Establishing a cybersecurity emergency and incident response Centre

5-9 November 2018 | Lilongwe, Malawi

The Centre held a workshop (Program for Establishing a Cybersecurity Emergency and Incident Response Centre) in the Republic of Malawi, Southeast Africa, from 5<sup>th</sup> to 9<sup>th</sup> November 2018. During the course, the program for building a sustainable team for responding to cybersecurity emergencies was reviewed.



### Establishing the emergency response centre and cyber incidents for the State of Palestine

17-28 March 2019 | Cairo, Egypt

The Centre contributed to the establishment of the Centre for Cyber Incident Emergency Response Teams for the State of Palestine and assisted and trained specialists in the Palestinian Ministry of Communications and Information Technology to be able to provide initial response services to security incidents to institutions and departments.

The Centre provided workshops and training courses accompanying the establishment of the Centre to build capacity and enhance cadre readiness for the emergency response team and cyber incidents. A number of primary axes were covered, including:

- Training on emergency response process and cyber incidents by implementing, reviewing and testing the tools required to operate the Centre.

- Improving the degrees of anticipation, identifying threats and responding to them promptly, and working out future solutions for the beneficiary institutions that have been identified by the Centre.

- Ensuring the use and operation of the Centre by building a highly efficient response system to respond and confront cyber threats.

- Increasing the ability to assure the effectiveness of security measures and controls, and readiness to respond quickly when security incidents occur.

- Training on implementing, reviewing and testing processes and treatments developed for emergency response centres and for cyber incidents.



# Third: International Co-operation



- 1 - Regional & International Meetings
- 2 - Joint Events

## Third: International Co-operation





## 1- Regional & International Meetings

With a view to uniting efforts and consultations among the Member States of the Centre, the last period from 2018 to 2020 witnessed a number of important meetings, including:

### The seventh meeting of the Arab Cybersecurity Cooperation Team October 22, 2018 | Kuwait, State of Kuwait

On the side-lines of the seventh regional conference on cybersecurity, a consultative meeting was held for the general directors and heads of the Arab National Cybersecurity Centres to discuss fields of enhancing cybersecurity in the Arab region.

The meeting discussed the most important aspects of joint cooperation, the most prominent challenges facing cyberspace, the rapid development of software, and threats that pose risk to institutions and individuals.



### The second Arab meeting of Study Group 17 of the ITU October 25, 2018 | Kuwait, State of Kuwait

Sultanate of Oman chaired the second meeting of the regional team for the Arab region of the ITU Study Group 17 (SG17RG-ARB). During the meeting, new members of the group were elected: the Kingdom of Bahrain, the Arab Republic of Egypt, the State of Qatar, and the Republic of Sudan. The meeting discussed the main issues in the field of cybersecurity in the Arab region, identifying priorities and initiatives of common interest, as well as reviewing the initiatives that were adopted during the first meeting of the work group in Muscat, 2017.

The meeting focused on the security of infrastructure institutions, and the fields of the Fourth Industrial Revolution, and a set of initiatives in these areas were reviewed.



### The consultative meeting of the heads of the Arab National Centres for cybersecurity

October 28, 2019

The consultative meeting of the heads of the Arab National Centres for cybersecurity, participating in the conference, resulted in a number of recommendations and initiatives, the most important of which are: the need to strengthen joint Arab cooperation, and the importance of holding a workshop on national cybersecurity strategies in the Republic of Tunisia in December 2019.

In addition, a meeting was held for the regional team for the Arab region of Study Group 17 (SG17RG-ARB) in which successful experiences and practices in cybersecurity were presented from the various participating Arab countries, and a number of innovation initiatives in the field of cybersecurity were launched and activated.



### Meeting of OIC Board of Directors October 30, 2019

On October 30, 2019, OIC Board of Directors' meeting was held and chaired by the Sultanate of Oman. The meeting discussed the work plan for 2019, developments in the approved projects, and areas of cooperation with the organisations in the field of cybersecurity.



### ITU Global Event Meeting, Regional Dialogue for the Arab Region on the Lessons Learned from COVID-19 Pandemic September 22, 2020 | Virtual

ITU-ARCC participated in the ITU global event meeting. During the meeting, the most important lessons learned from Covid 19 pandemic were reviewed, with the aim of sharing countries' experiences in dealing with the challenges posed by the pandemic.





## 2. Joint Events

The agenda of the Arab Regional Centre during the years 2018, 2019 and 2020 included a number of various joint events and activities, the most important of which are:

### Celebrating the World Safe Internet Day 6 - 11 February 2018 | Virtual

From 6<sup>th</sup> to 11<sup>th</sup> February 2018, the Centre celebrated, with the rest of the world, the World Safe Internet Day, which comes within the European Union initiative and the European Organisation for Internet Awareness (ENSIF), with the aim of promoting joint work among countries of the world to raise awareness of the dangers of the Internet, the importance of preserving privacy, warning against misuse and its legal consequences, in addition to developing ethical and behavioural standards and regulations when using Internet.

The participation of the Centre included a number of awareness activities and educational work sessions targeting parents, teachers and children from the age group 5-18 years old. The National Centres for cybersecurity in the Arab region, which include 22 Arab countries, were invited with the aim of strengthening international cooperation in spreading the message of awareness of protecting children from Internet dangers, under the slogan (Create, communicate and exchange respect: a safer Internet starts from your side).

Sultanate of Oman, Tunisia, Egypt, Libya and the ITU have participated in some targeted awareness-raising activities, including:

#### Tunisia:

- Data integrity “storage and retrieval”  
<https://www.youtube.com/watch?v=DWuN9D4QZnE>
- The security of smartphones and digital tablets  
<https://www.youtube.com/watch?v=gPurNd>
- Preventive practices for integrity of access data  
<https://www.youtube.com/watch?v=B72RY9vSWww>



#### Sultanate of Oman:

- Educational packages and awareness-raising presentations that were translated into Arabic by the National Centre CERT team:  
[http://cert.gov.om/library\\_publication\\_arabic.aspx?category=3 ...](http://cert.gov.om/library_publication_arabic.aspx?category=3...)  
[http://cert.gov.om/library\\_publication.aspx?category=3 ...](http://cert.gov.om/library_publication.aspx?category=3...)

#### Egypt:

- Awareness booklet entitled:
- “The principles of using the Internet safely through games”  
[http://mcit.gov.eg/Ar/Publication/Publication\\_Summary/1047](http://mcit.gov.eg/Ar/Publication/Publication_Summary/1047)

### The World Summit on the Information Society 2018 March 19-23, 2018 | Geneva, Switzerland

The Centre participated in the activities of the World Summit on the Information Society within an official delegation from the Sultanate of Oman (the headquarters of the Centre) and with the participation of Engineer Bader bin Ali Al Salhi, Director General of the National Centre CERT and Head of ITU-ARCC. During the participation, a meeting was held with the Secretary-General of the ITU and there was participation in a number of workshops.



### World Safe Internet Day 2020 6-11 February 2020 | Virtual

February 11, 2020 was chosen to participate in the seventeenth anniversary of the “World Safe Internet Day” under the slogan (Together for a Safe Internet). ITU-ARCC invited the National cybersecurity Centres in the Arab region to participate in spreading awareness about the risks of the Internet.



The online campaign for the World Safe Internet Day targeted: children, youth, parents, teachers and educators, social workers and decision-makers, in order to encourage everyone to contribute to an effective role for a safe Internet.

The following were among the participations of the Member States of the Centre:

### A signing ceremony for a partnership agreement with the Centre for Humanitarian Dialogue in Switzerland 26 August 2020 | Virtual

On August 26, 2020, the Centre signed a partnership agreement with the Centre for Humanitarian Dialogue in Switzerland. The signing ceremony was virtual via the Internet, with the participation of Engineer Bader bin Ali Al Salhi, Head of ITU-ARCC, and a number of organisers at the Centre for Humanitarian Dialogue.

#### Syria:

National Agency for Network Services (NANS) in the Syrian Arab Republic participated by an awareness study entitled: “Protecting the child from the dangers of the Internet is a family and community responsibility.”

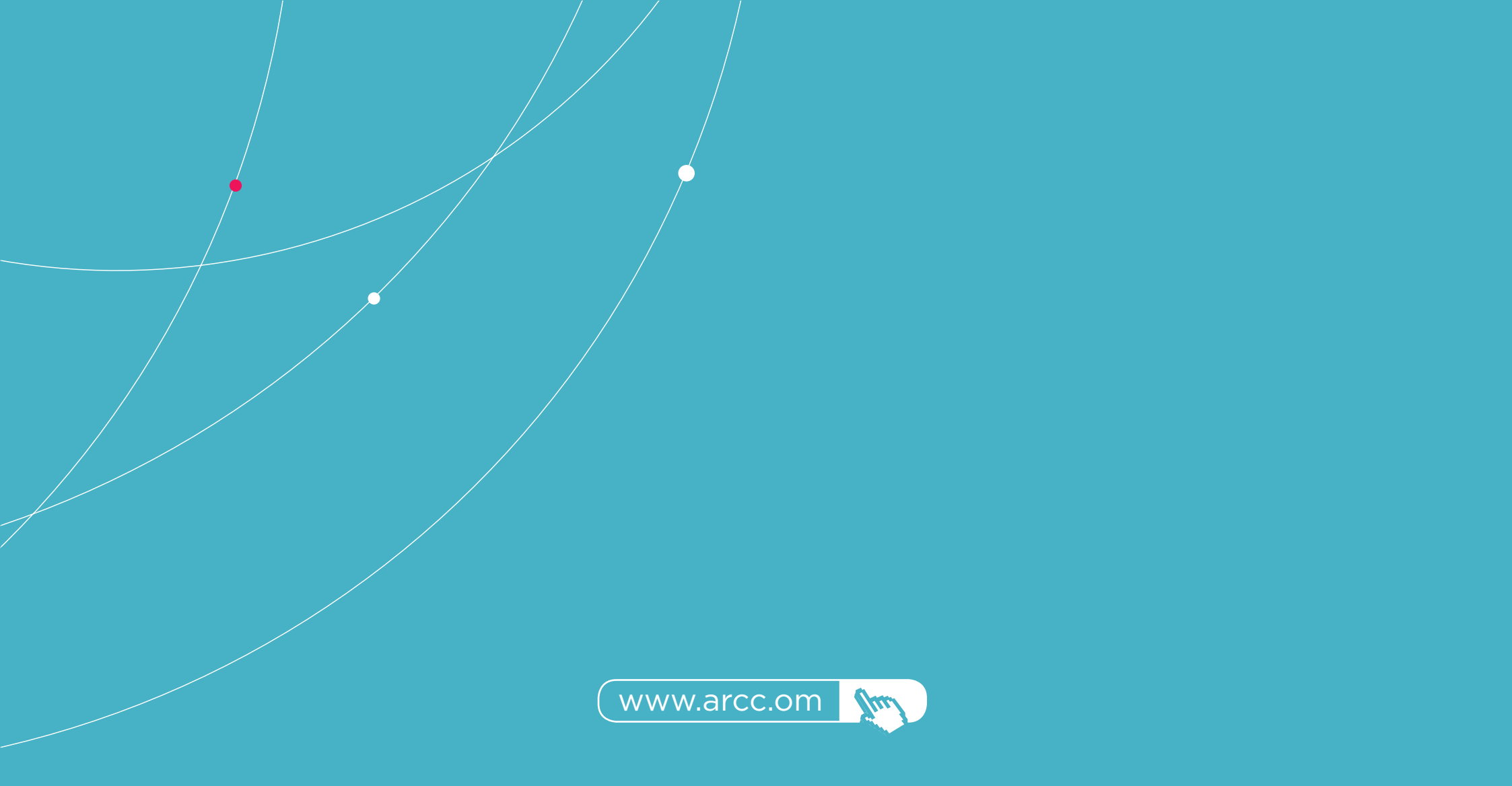
[https://www.nans.gov.sy/ar/article/protecting\\_children\\_from\\_the\\_dangers\\_of](https://www.nans.gov.sy/ar/article/protecting_children_from_the_dangers_of)

#### Tunisia:

The National Agency for Computer Security (Agence nationale de la sécurité informatique- ANSI) in the Republic of Tunisia participated by the game “Watchful use of the Internet” and “the guide on using the Internet”.

[https://play.google.com/store/apps/details?id=com.toufoulakids.arpack&hl=en\\_US](https://play.google.com/store/apps/details?id=com.toufoulakids.arpack&hl=en_US)

<https://www.ansi.tn/actualite/lansi-adh-re-au-safer-Internet-day-2020>



[www.arcc.om](http://www.arcc.om) 

