

**Speech of Hon. Deepak Balgobin, Minister of Information
Technology, Communication and Innovation
Online Launching of ITU Centre of Excellence in the Field of
Cybersecurity
Monday, 28th September 2020**

--

Ms. Sandrine Valere, Permanent Secretary of my Ministry

**Mr. Andrew Rugege, Regional Director, International
Telecommunication Union,**

Mr. Jean Robert Hountomey, Executive Director, AFRICACERT

**Mrs Joanne Esmot, Executive Director of the National Computer
Board,**

Heads of Departments,

Distinguished guests,

Participants of the Training Programme from all around the world,

Ladies and Gentlemen,

Good Afternoon and welcome to this online launching of the ITU Centre of
Excellence in Cybersecurity.

This Centre has been setup by the **Computer Emergency Response Team of Mauritius** of the National Computer Board, an organisation which falls under the aegis of my ministry.

I am proud that Mauritius has been chosen as the Centre of Excellence in the priority area of Cybersecurity in Africa, following a meticulous evaluation process from a large number of submissions received by the International Telecommunication Union.

I thank the ITU for having selected our Republic !

I am happy to note that Mauritius will be a Centre of Excellence for at least four years.

Ladies and Gentlemen,

I understand that the objective of the ITU is to share expertise, resources and capacity-building know-how. The selection of our country as one of ITU Centres of Excellence reflects the recognition of Mauritius as a high-quality training provider in the region and in the field of ICT. The role of Mauritius in this programme will be to build national and regional capacity on cybersecurity, particularly in Eastern and Southern Africa.

Ladies and Gentlemen,

Information Security today is a rapidly evolving game of advanced skill and strategy. Thus, the security models of the past decade are no longer useful. Today's information security leaders acknowledge that playing the game at a higher level is required to achieve effective security.

They know that the very survival of their organisations relies on their security staff being capable of fully understanding cyber threats and to be fully prepared to respond to them in a timely manner.

Given the always evolving landscape, organisations should keep on developing capabilities for detecting incidents when they arise, minimizing the impact on business and critical infrastructure.

Therefore, one of the fundamental elements to focus on is the capacity building.

Ladies and Gentlemen,

Good security requires highly-skilled professionals. Today, there is a shortage of cybersecurity manpower around the world including Mauritius. Qualified professionals are in great demand as Governments and

organisations have realised how important it is to protect their assets from cyberattacks.

This demand for security professionals will only increase as the frequency and consequences of cyber threats continue to grow.

To ensure that this demand is met, we need to have an adequate and well-trained cybersecurity workforce in the public and the private sector.

I truly believe that the setting up of this ITU Centre of Excellence in Cybersecurity will contribute enormously in bridging this gap.

Ladies and Gentlemen,

One of our Government's main objective is to shape the right environment to make the Internet more accessible and secure to the citizens of Mauritius. My Ministry is working hard to enhance Internet development by devising appropriate strategies and policies to provide a secure environment for one and all. We see the Internet as a major driving force to transform Mauritius into a high-income, inclusive and green economy as per Vision 2030 of the Government.

Ladies and Gentlemen,

I strongly believe that in order to achieve a resilient and secure environment, national cyber strategies play an important role for a country. In the course of last 5 years, national strategies on cybersecurity have been developed and implemented in Mauritius.

Through these strategies, a number of projects have taken shape. Recently, the Government has approved the **National Cyber Incident Response Plan** which has been developed to manage cyber incidents of national ramification.

Another project which is being finalised is the development of a **Critical Information Infrastructure Protection Policy**. The development of this policy is based on the UN Resolution 58/199 '**Creating a Global Culture of Cybersecurity and Protection of Critical Information Infrastructures**' and focuses on leadership, risk mitigation and awareness. The policy defines a plan of immediate actions to strengthen security and resilience.

By the end of the year, my Ministry will formulate a new national Cybersecurity Strategy to make sure that our network infrastructure is protected in the best way possible and in the interest of our citizens.

Ladies and Gentlemen,

At this point, allow to mention that Mauritius is already party to the **Commonwealth Cyber Declaration** signed by our Honourable Prime Minister, Pravind Kumar Jugnauth, in April 2018 in London, on the occasion of the holding of the **Commonwealth Heads of Government Meeting**.

Mauritius also has a Memorandum of Understanding with the Government of Estonia in the field of ICT, signed in November 2017.

Finally, Mauritius is also represented on the **United Nation's Open-Ended Working Group** and **Group of Governmental Experts** on cyber Norms, Confidence Building Measures and International Law on Cyberspace.

Of course, these initiatives have played an important role in the ranking of Mauritius in the **Global Cybersecurity Index** and has placed our country **1st in Africa** for the past 6 years.

Ladies and Gentlemen,

I am delighted that today, during the first training on **Cybersecurity Risk Management**, there will be 128 participants from 59 countries including Mauritius.

Of course, because of the COVID-19 pandemic, the training is offered online and is free of charge to make it accessible to a larger audience in the African continent and in other parts of the world.

I understand that at the end of this training there is an exam for the participants. I wish 'Good Luck' to all those who are attending.

A second training programme on **Cybersecurity Strategy and Policy** will be organised online in November and it will also be offered at no cost.

Ladies and Gentlemen,

Before I conclude, I would like to thank the ITU, the National Computer Board and everyone who contributed in the organisation of these training sessions.

I wish that all participants make the most of it.

I now have the pleasure to officially launch the ITU Centre of Excellence and declare the **Cybersecurity Risk Management Training** officially open.

Thank you for your attention.