Speech of Hon. Deepak Balgobin, Minister of Information Technology, Communication and Innovation

African Cyber Resilience Conference by the Cyber Resilience for Development Project (EU)

Monday, 25th April 2022

Hennessy Park Hotel, Ebène

Protocol:

- **Honourable Alan Ganoo, Minister of Land Transport and Light Rail, Minister of Foreign Affairs, Regional Integration and International Trade**
- **Honourable Miss Paula Ingabire, Minister of ICT and Innovation of the Republic of Rwanda,**
- **His Excellency, Mr Vincent Degert, Ambassador of the European Union,**
- **Miss Sandrine Valere, Permanent Secretary of my Ministry,**
- **Mr. Raul Rikk, National Cybersecurity Coordinator, Estonia**
- **Mr. Jean Robert Hountomey, Executive Director, AFRICACERT,**
- **Dear delegates,**
- **All protocols observed,**
- **Ladies and Gentlemen,**

Very Good Morning and warm welcome to you all.

1. It is my privilege and honour to address you all, distinguished peers, in the spirit of partnership and collaboration. The African Cyber Resilience Conference is a first of its kind being organised by Cyber Resilience for Development Project (Cyber4D), an initiative of the European Union, in close collaboration with my Ministry, the Ministry of Information Technology, Communication and Innovation.

2. The Cyber4D project started in Mauritius, through the Ministry of Foreign Affairs in 2018. As I am informed, many activities have been organised during these past four years, with a view to enhance cyber

resilience across Mauritius.

3. The activities include capacity building on different aspects of cybersecurity, including the activities for the Computer Emergency Response Team Mauritius (CERT-MU), a unit under my Ministry.

4. The capacity building was rightly focused on areas of national cybersecurity strategies, monitoring and evaluation, table top exercises, Security Incident Management Maturity Model (SIM3) assessment, communication skills development for cybersecurity trainers, among others.

5. The quest for cyber security is a journey, not a finality. I am, accordingly, pleased to announce that today's conference has been organised to primarily launch "Mauritius as the Cyber4D Hub" and also to enable African countries, to engage in discussions with the Cyber4D experts and learn from their experience on diverse aspects of cyber resilience.

Ladies and Gentlemen,

6. As the world continues to recover from the disruptions caused by the COVID-19 pandemic, coping mechanisms such as increased use of virtual workspaces, online marketplaces and e-Governance have become the norm. While this presents opportunities to revamp economies and streamline public service delivery, it also unfortunately increases exposure to cybercrime.

7. In the African continent, many countries have seen a rise in digital threats and malicious cyber activities. These include sabotaged public infrastructure, losses from digital fraud and illicit financial flows, and national security breaches involving espionage and intelligence theft amongst others.

8. Addressing these vulnerabilities requires an ever greater commitment to cybersecurity. It is now the opportune time for Africa to take full advantage of the digital revolution to empower its citizens and enhance transparency in both the public and private sectors. This will not happen until data is stored in safe and trusted systems that protect privacy and are difficult for criminals to breach.

9. A good start would be to explore and assess the state of cybersecurity in Africa from the perspective of the five building blocks of the International Telecommunications Union (ITU) Global Cybersecurity Index (GCI), namely legal, technical, organisational, capacity building and cooperation.

10. The African Union's Agenda 2063, the continent’s blueprint and master plan for transforming Africa into the global powerhouse of the future, identifies cybersecurity as one of the key programmes and initiatives for accelerating Africa’s economic growth and development. This Agenda sets out a plan for leveraging emerging technologies through cybersecurity for the economic and social benefit of fellow Africans.

11. It is worth noting that there have been some recent commitments to strengthening the cybersecurity landscape in Africa. Many countries, including Mauritius, are investing in a robust cybersecurity structure, becoming a model for countries in Europe and other West African countries. Fourteen African states (*including, Rwanda, Botswana, Kenya, Malawi and Mauritius*) also have a national strategy on cybersecurity with an additional four countries with draft legislation in progress.

12. Collaborations at the regional and sub-regional levels on capacity building and development, and the drafting of frameworks, also reflect attempts to better position the continent to deal with increasingly sophisticated cyber threats. For example, in 2014, the African Union (AU) adopted the Convention on Cyber Security and Personal Data Protection (Malabo Convention), although, by 2018, only 8 out of 54 African countries had a national strategy on cybersecurity.

13. In 2019, the AU also hosted the Global Forum on Cyber Expertise (GFCE) in Addis Ababa, Ethiopia. This forum is a multi-stakeholder community of more than 140 members and partners from all regions of the world, aiming to strengthen cyber capacity and expertise globally.

14. More recently, in early 2021, the Economic Community of West African States (ECOWAS) adopted a regional strategy for cybersecurity. This regional body has convened 15 African states and the Council of Europe

to harmonise legislation on cybercrime and electronic evidence within the rule of law and with human rights safeguards.

Ladies and Gentlemen,

15. Now, please allow me to elaborate on what we are doing here in Mauritius for combatting cybercrime.

16. One of the fundamental elements to prevent cyber-attacks is capacity building. Good security requires highly-skilled practitioners with deep expertise. Today, there is a shortage of cybersecurity manpower around the world, including Mauritius. Qualified professionals are in great demand as governments and businesses have to pay more and more attention to cyber risks.

17. To ensure that this demand is met, Mauritius has set up the ITU Centre of Excellence in the field of Cybersecurity and I had the pleasure to launch this Centre in 2020, with an online training facility on Cybersecurity Risk Management. To date, six cybersecurity training sessions have been conducted and a number of countries, including African countries, have benefited from these.

Ladies and Gentlemen,

18. Cybercrime is not only a question of attacks against the confidentiality, integrity and availability of computer data and systems but against the core values and the human development potential of societies increasingly relying on information technology. In light of this, we have

the duty to protect our society and individuals against such cybercrimes. To this effect, an efficient criminal justice response is vital.

19. I have, with a view to modernizing the legal framework, presented in our parliament a new Cybersecurity and Cybercrime legislation, enacted last year, to ensure that the Mauritian legislation remains strong and resilient to cybercrime. This piece of law has been reviewed with the help of the Council of Europe and has been aligned with technological developments, international conventions, norms and standards, as well as legal and regulatory changes.

20. Talking about international norms, it is also imperative to highlight that Mauritius has already acceded to the Budapest Convention on Cyber Crime in 2014 and ratified to the African Union Convention on Cyber Security and Personal Data Protection in 2018. The new law has been aligned with the European and African conventions.

21. Other initiatives include the approval of the National Cyber Incident Response Plan by our government to manage cyber crisis situations, setting up of a centralised incident reporting system, namely the Mauritian Cybercrime Online Reporting System (MAUCORS).

22. Mauritius is also actively engaged with regional partners such as AfricaCERT, African Union Commission and Southern African Development Community (SADC) on cybersecurity matters.

23. CERT-MU, in collaboration with the AfricaCERT, organised the first online Africa Cybersecurity Drill for national security and response teams

in Africa, Asia-Pacific and the Organisation of the Islamic Cooperation in 2021. Some 32 teams from 24 countries participated in the drill.

24. With regards to international cooperation, Mauritius is a member of the Forum of Incident Response and Security Teams (FIRST) since 2012 and hosted two FIRST Technical Colloquia in 2016 and 2017 respectively, where a number of countries from the region have taken part.

25. Moreover, Mauritius is party to the Commonwealth Cyber Declaration, signed by the Prime Minister in April 2018 in London on the occasion of the holding of the Commonwealth Heads of Government Meeting (CHOGM). Mauritius has also signed an MoU with the Government of Estonia in the field of Information and Communication Technology in November 2017.

26. These initiatives have played an important role in the ranking of Mauritius in the ITU Global Cybersecurity Index and has placed our country FIRST in Africa since the past 8 years. Currently, Mauritius is ranked 17th globally.

27. I recognise this as a great achievement and it has been possible by the hard work put in by my Ministry and the unfailing support of the Government led by our Prime Minister, Honourable Pravind Jugnauth.

Ladies and Gentlemen,

28. Before I conclude, I would like to thank the Cyber4D team and my team at the Ministry for the organisation of this event. I wish this Conference all the success it deserves and wish you all fruitful deliberations.
29. I also wish to express my gratitude to all my fellow colleagues from Africa, as well as the experts and delegates who have travelled over long distances to make this event a success.

I thank you for your kind attention.