



**SADC Capacity Building Workshop on Cyber Security
and SADC Regional Cyber Drill
10th to 13th September 2018
Cyber Tower 1, CyberCity
EBENE, MAURITIUS**

1. The SADC Capacity Building Workshop on Cyber Security and SADC Regional Cyber Drill was convened from the 10th to 13th September 2018 in Mauritius. This event was hosted by the Government of Mauritius. The Meeting was attended by delegates from fourteen (14) SADC Member States namely; Angola, Botswana, Democratic Republic of Congo (DRC), Kingdom of Eswatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Zambia and Zimbabwe. SADC ICT Implementing Agency, the Communications Regulators' Association of Southern Africa (CRASA) and our Cyber Security partners, the International Telecommunication Union (ITU) and Kaspersky Labs.
2. SADC Capacity Building Workshop on cybersecurity and Regional Cyber Drill was organized with the objective of enhancing the cyber-threat preparedness of SADC Member States.
3. The Minister of Technology, Communications and Innovation (MTCI) of Mauritius, Yogida Sawmynaden who was the Guest of Honour delivered Key Note Address in which noted that the cyber-threat landscape of the SADC region has changed drastically with the high Internet penetration and increased usage of smart phones amongst youth. The Minister noted that the high adoption of social networks such as Facebook, Twitter, Whatsapp, YouTube, Instagram as well as the ease of downloading and viewing online content are contributing in making the cyber space more vulnerable to attacks.
4. The Honourable Minister Sawmynaden noted that the number and impact of cyber incidents continue to grow and that there need to detect and act upon cyber-attack vulnerabilities, backdoors and incidents as early as possible. He urged Member States to be proactive and maintain a rigorous approach in implementing effective measures to protect themselves against cybercriminals.
5. A National Cyber Incident Response Plan sets out the roles and responsibilities of all stakeholders, critical infrastructure owners and operators and other public and private sector partners in the coordination of addressing incidents of national importance. Lastly, he said that this
6. A representative from Republic of Namibia, the current Chair of SADC, Mrs. Linda Aipinge, said the workshop is one of the activities for the SADC Expert Group on Public Key Infrastructure (KPIs) and Client Information and Registration Tracking Systems (CIRTs) meant to assist Member States to accelerate the establishment of the PKI and CIRT. Mrs. Aipinge encouraged Member States to make optimal use of the opportunity availed by the Government of Mauritius and intensify awareness on the importance of cyber security at household and organizational levels.
7. Speaking on behalf of the SADC Director of Infrastructure, the Acting Senior Programme Officer for ICT, Dr. George Ah-Thew, stated that this first SADC Cyber Drill is to serve as a platform for

cooperation, information sharing, and discussions on current cyber security challenges, incident response capabilities and communications, as well as a hands-on exercise for national CIRTs.

8. Dr. Ah-Thew emphasised that no entity can confront cyber-crime on their own. And SADC must continue to build its collective capabilities to fight cyber threat. He said the Private sector, especially the financial sector, and other critical infrastructures, operators, including the central banks, should participate in SADC Cyber Security meetings, as they have a vested interest in cyber security. A National CIRT should assist the Public and Private Sector. The skills and hands on experience obtained from this SADC Capacity Building Workshop should enable participants to now organize National Cyber Security Drills in their own country.
9. The SADC Expert Group on PKI and CIRT was set up in March 2018 in Pretoria, South Africa. Among the proposals to be submitted by Group to the workshop for discussion are the Guidelines for Setting up a National CIRT and the Draft Framework for Establishing the SADC Regional CIRT.
10. During the workshop, the ITU made a presentation on the Global Cybersecurity Index (GCI) and the rankings of SADC Member States while the SADC Secretariat presented the Cyber Security Indicators to be collected and Performance Key Indicators for National CIRTs. The SADC Secretariat also presented on the Ratification of African Union (AU) Convention on Cyber Security and Data Protection. To date, Mauritius has ratified while Comoros and Zambia have signed the AU Convention.
11. The presentation by CRASA centered on the establishment of links for both, international and regional cooperation in containing cybercrime. It was noted that there were already international conventions, such as the Budapest Convention on Cyber Crime 2004 and African Union Convention on Cyber Security and Data Protection 2014 which could be used to leverage assistance from other nations. It was also noted that at SADC level, there were already existing protocols including, the Protocol on Mutual Legal Assistance (MLA) in Criminal Activities and Protocol on Extradition could also be used to leverage legal basis for obtaining assistance across the SADC Borders.
12. It was further noted, that there was need to provide SADC Member States with a Model Strategy that could be used in harmonizing the cooperation and coordination of cyber security issues and the for an inclusive approach towards skilling and capacity building of critical stakeholders.
13. The Chair of the SADC Expert Group on CIRT and PKI circulated draft SADC Guidelines for the Establishment of National CIRT and the Draft Framework for the SADC Regional CIRT which will be submitted to the meeting of Senior Officials responsible for ICT in September 2018 in Windhoek, Namibia.
14. It was noted that, to date, only four (4) SADC Member States, namely; Mauritius, South Africa, United Republic of Tanzania and Zambia had established and operational CIRT. Six (8) Member States, namely; Angola, Botswana, DRC, Eswatini, Lesotho, Mozambique, Namibia and Zimbabwe have completed the ITU CIRT Assessment and are awaiting the enactment of appropriate legislation to operationalise their National CIRT. The process is currently ongoing for Madagascar and Seychelles. Botswana and Zimbabwe are being assisted by the ITU to implement their National CIRT. Malawi is presently designing its CIRT.
15. The SADC Capacity Building Workshop on Cyber Security and SADC Regional Cyber Drill came up with the following recommendations:
 - Member States were urged to submit statistics data (for ICT for Development Index (IDI), GCI etc) on a timely manner to the ITU so that they may be ranked among other ITU States;
 - Member States were urged to validate their statistic data, even after it has been published and to advise the ITU;
 - Member States were encouraged to participate in the meetings of the GCI and IDI;
 - Member States are encouraged to ratify the AU Convention on Cyber Security and Data Protection;
 - Member States were urged to expedite the deployment of the National CIRT before the deadline of December 2019;

- The SADC Regional Cyber Drill must now become an annual event, which will later be coordinated by the SADC Regional CIRT;
 - Member States were urged to monitor the various types of authentication schemes being introduced instead of PKI and to provide advice so as to protect them from cyber threats;
 - Member States were encouraged to participate in the Cyber Security Conference planned to be convened from the 22nd to 23rd November 2018 in Mozambique;
 - Member States were encouraged to participate in the upcoming 5th ITU-Applied learning for Emergency Response Teams (ALERT) International Cyber Drill for Africa Region from the 1st to 5th October 2018 to be convened at the Afrikland hotel in Grand Bassam, Ivory Coast;
 - SADC Secretariat to continue promoting capacity building initiatives relating to cyber security;
 - The SADC Secretariat urged to develop a list of harmonised indicators to measure progress in cyber security commitment of all SADC Member States and to include these indicators under the SADC ICT Observatory;
 - The SADC Secretariat urged to develop a SADC Model Cyber Security Strategy that would be utilised by SADC Member States in developing their own National Cyber Security Strategy;
 - The SADC Secretariat urged to explore partners and mobilise resources for the development of the SADC Model Cyber Security Strategy;
 - Member States are urged to develop and implement anti-child abuse and human trafficking strategies to protect women and the African Child in the context of the Cyber Security framework; and
 - Member States are encouraged to join the Global Forum for Cyber Expertise (GFCE), which and participate in their events. The GFCE is a global forum for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building (www.thegfce.com).
16. The next SADC Capacity Building Workshop on Cyber Security and SADC Cyber Drill is to be convened in South Africa and the Cyber Drill component would be the 6th ITU-ALERT International Cyber Drill for Africa Region hosted by South Africa.
17. The SADC Capacity Building Workshop on Cyber Security and SADC Cyber Drill was officially closed by Mr. Kaleem Usmani on behalf of Mrs. Rooba Yanembal Moorghen, the Permanent Secretary of the MTCI of Mauritius.

Done at Ebene, Mauritius, 13th September 2018.