AFRICA CENTER
FOR STRATEGIC STUDIES
IMPACT THROUGH INSIGHT
25 YEARS

Advancing Regional Cyber Security and Stability in Africa

PEACE, PROSPERITY AND
REGIONAL INTEGRATION

IGAD's Cybersecurity Efforts and Initiatives

Workshop on Advancing Regional Cyber Stability and Security

21-23 May 2024
Port Louis, Mauritius

Nejat Abdulrahman Issa
IGAD SSP Senior PO

STRUCTURE

- Introduction – IGAD SSP, Vulnerability
- Efforts and initiatives
- Challenges, Successes, and Lessons Learned

IGAD SSP

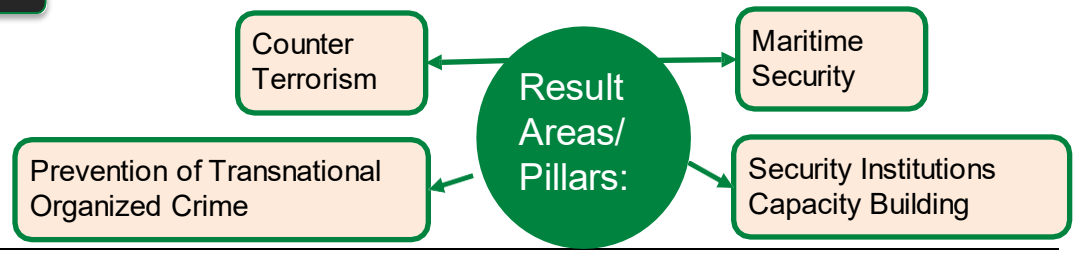
Pillar of the IGAD Revitalized Peace and Security Strategy

Objectives

Advancing Predictive, Preventive, Responsive, and Adaptive (PPRA) institutional and Human Capabilities of IGAD and Member States in addressing EEE-TSTs

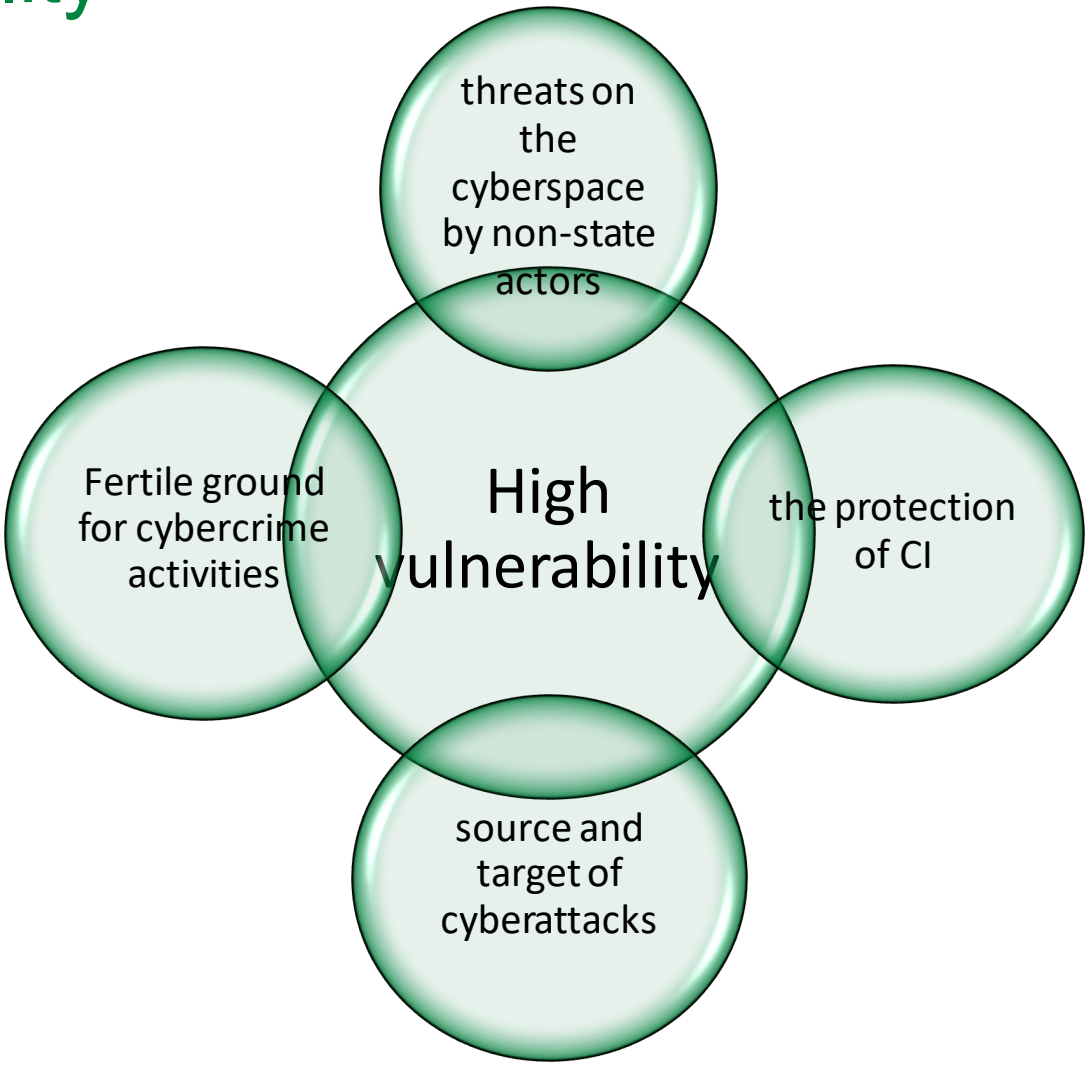
Strategic Priority Areas

- Strengthen regional cooperation and coordination
- Enhanced MS's and IGAD's institutional and human capacities
- Improved progress in ratification, domestication, and implementation of regional and international relevant instruments



IGAD SSP Security Sector Programme

Vulnerability



Efforts & Initiatives

Strengthen regional cooperation and coordination

- 2013/4 onwards, studied, assessed, and consulted various MS practitioners to establish a reginal mechanism for cooperation and coordination through criminal information & intelligence sharing

Enhanced MS's and IGAD's institutional and human capacities

- Theme based CB programs for awareness, skills and knowledge capabilities, informal network creation, and confidence building:
  - Investigation techniques of Cybercrime
  - Role of Technology and Online Platforms, SM as recruitment tools
  - Cyber/Digital Forensics/Evidence on CTIP
  - Review of MS cybersecurity frameworks
  - Security threats of UAVs & emerging technologies

Improved progress in ratification, domestication, & implementation of relevant instruments

- Sensitization and promotion of the available legal instruments including identified gaps, challenges, and success stories.

Next Plans:

- Continue with CB programs, promotion of legal instruments
- in-depth assessment on existing cyber security frameworks, capabilities,& limitations
- Develop a regional cybersecurity strategy

IGAD

SSP
Security Sector Programme

Challenges

Member States

- Rising internet penetrations - Personal Data Protection (PDP) - huge amounts of personal data are collected, stored and transmitted across the globe
- Digital sovereignty
- Trust between government and the community
- digital transformations and use of technology within the public service providers - Internet, mobile networks, and related ICT tools

Institutional – LEAs

- Low capacity/technical capability
- awareness, capability to detect, investigate, acquiring forensics, prosecute, issues of HR – how to balance and utilize, etc
- Resources vs technological advancement – new techs, infrastructure, accessibility, etc
- Weak legislations and implementation
- Absence of comprehensive info on the transnational networks operating on cyber space

Regional

- Different MS threat level – affecting priority and response
- Practice of bilateral engagements

IGAD
SSP
Security Sector Programme

Success and Lessons Learnt

IGAD
SSP
Security Sector Programme

Thank you for your Attention!

Nejat Abdulrahman Issa
Senior Program Officer
IGAD SSP

Nejat.Abdulrahman@igad.int

@NejatIssa @IGADISSP

AFRICA CENTER
FOR STRATEGIC STUDIES
IMPACT THROUGH INSIGHT
25 YEARS

Advancing Regional Cyber Security and Stability in Africa

Overview of the SADC Cybersecurity Framework

Presented to: Advancing Regional Cyber Stability and Security Workshop

Presented by: Dr. George Ah-Thew, SADC SPO ICT

22nd May 2024

Port Louis, Mauritius

U.S. DEPARTMENT of STATE

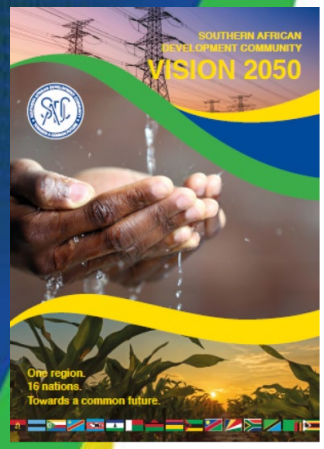
AFRICA CENTER FOR STRATEGIC STUDIES

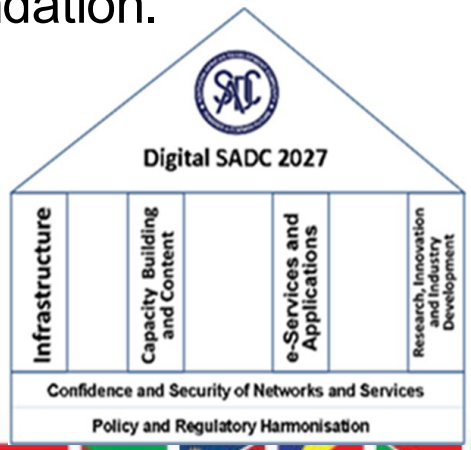
Presentation Outline

- Background
- SADC Harmonised Cybersecurity Legal and Regulatory Framework and Enforcement
- Achievements, Challenges and Lessons Learned
- Recommendations

Background

- SADC comprises of 16 Member States with an estimated population of 360 Million people.
- **SADC Vision 2050** is built on a foundation of Peace, Security, and Good Governance and anchored on 3 pillars, which are interlinked with Gender, Youth, Environment and Climate Change, and Disaster Risk Management as cross-cutting issues. **Pillar II**: Infrastructure Development in Support of Regional Integration.
- **Digital SADC 2027** is the ICT Chapter of the SADC **Regional Infrastructure Development Master Plan** (RIDMP) 2012-2027, the blueprint for ICT Infrastructure development for the SADC Region. RIDMP includes "Ensuring **Confidence and Security of Networks and Services**", as a foundation.



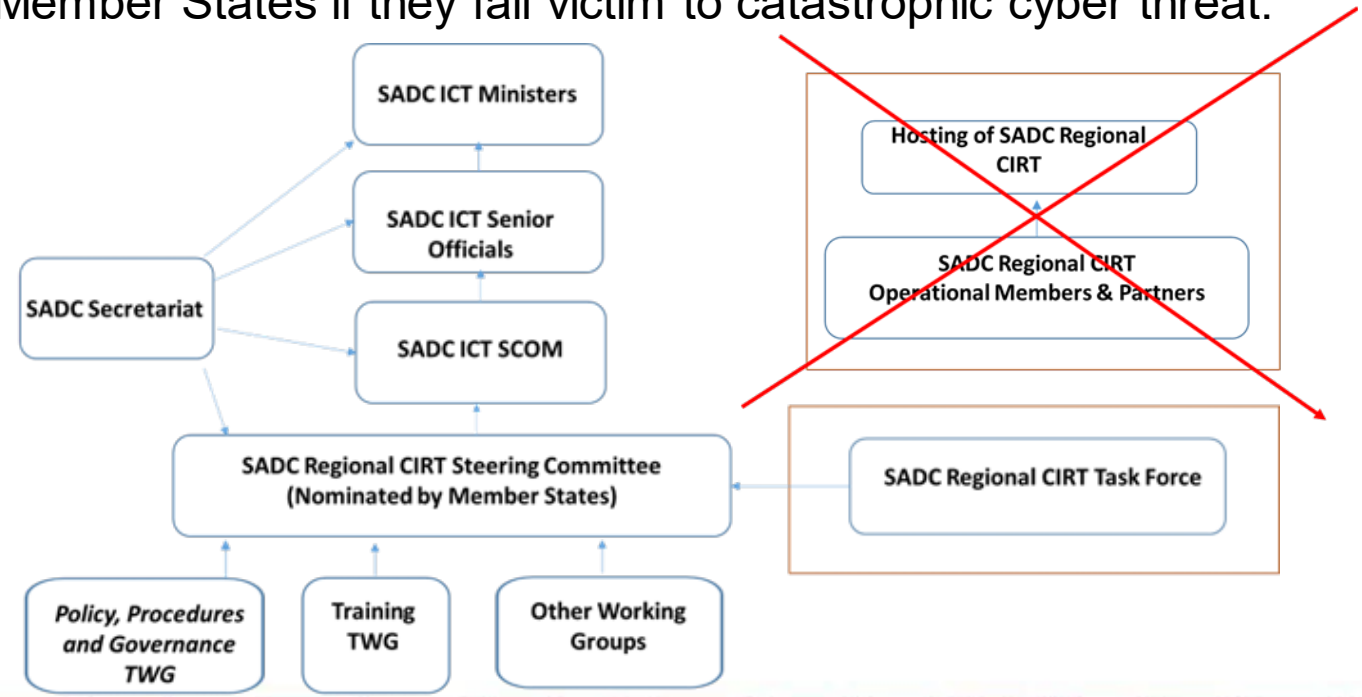


SADC Harmonised Cybersecurity Legal and Regulatory Framework and Enforcement

- The SADC Harmonised Cybersecurity Legal and Regulatory Framework consists of three (3) SADC cybersecurity model laws developed under HIPSSA Project and were approved in November 2012:
  - SADC E-Commerce/E-Transaction Model Law;
  - **SADC Data Protection Model Law**; and
  - **SADC Cybercrime Model Law**.
- All Member States have either transposed the SADC e-Commerce/e-Transaction and Cybercrime Model Laws or have an existing legal framework in place. Thirteen (13) Member States have put into place laws on data protection.
- SADC Data Protection and SADC Cybercrime Model Laws have been revised. They each include Implementation Guidelines and a Schedule and now being domesticated by Member States.
- Five (5) Member States have ratified the AU Convention on Cybersecurity and Personal Data Protection (Malabo Convention) of 2014 which came into effect on the 8th June 2023.

SADC Harmonised Cybersecurity Legal and Regulatory Framework and Enforcement

- Nine (9) Member States have established their National CIRTs.
- Annual SADC Cyber Drills continue to build capacity of CIRT Officers, inclusive of Posts and Central Banks).
- Established the **SADC Regional CIRT (SR-CIRT) Framework** in September 2019 - A regional collaboration platform to strengthen the regional cybersecurity readiness, protection and incident response capabilities.
- The Host for the SR-CIRT has been operationalised through the setting up of the SR-CIRT Task Force with currently 8 Members (Heads of CIRTs) to assist Member States if they fall victim to catastrophic cyber threat.



Achievements, Challenges and Lessons Learned

- Member States are at different levels of development, and some require assistance to domesticate the Revised SADC Model Laws.
- Cybersecurity is a shared responsibility and everyone has a role to play and it requires a coordinated action.
- Cybersecurity legal and regulatory framework require Institutional Mechanisms for enforcement, (e.g. CIRT/DPA) which some Member States are yet to establish.
- Leading Member States are taking leading roles and supporting those lagging behind (e.g. Peer Exchange/FIRST membership sponsorship).
- Consistent and inclusive capacity building initiatives (e.g. cyber drills) on TTX on areas identified by Member States (e.g. Postal/Finance Industry).
- Mauritius Cybersecurity Academy (CERT-MU) supporting SADC and Africa with free cybersecurity courses via the ITU Academy.
- Support from ITU (development of model laws & cyber drill) and Continental Institutions (e.g. AfricaCERT), International Cooperating Partners (ICPs) and SADC ICT Implementing Agencies (e.g. CRASA/SATA) have had a significant impact.

Recommendations

- Technical Assistance (TA) facility to support Member States in need to domesticate the Revised SADC Data Protection and SADC Cyber Crime Model Laws – resulting in harmonisation across SADC.
- Support Member States establish their CIRT/DPA and operationalisation of the SADC Regional CIRT (SR-CIRT) and linkages to other regional CIRTs/Partners.
- Support CRASA to establish the SADC Regional DPA.
- Support the development of the SADC Cybersecurity Strategy, which will include a Situational Analysis – Cyber Maturity Assessment - baseline.
- Enhance existing Cybersecurity Academy (e.g. CERT-MU) and support the SADC Regional ICT CoE.
- Avoid duplication and support REC-Led cybersecurity initiatives driven by Champions in the region.
- Offer scholarships via RECs and free access to specialized training opportunities to boost pool of regional cybersecurity Experts.
- Convene a continental forum on cybersecurity, to also attract youth.
- Establish a SADC Digital Evidence/Cyber Forensic Laboratory - Identification, seizure, acquisition, examination and maximizing the value of e-evidence.

AFRICA CENTER
FOR STRATEGIC STUDIES
IMPACT THROUGH INSIGHT
25 YEARS

Advancing Regional Cyber Security and Stability in Africa