Common Market for Eastern and Southern Africa

International Telecommunication Union

ITU Regional Cybersecurity Forum for Eastern and Southern Africa, Lusaka, Zambia, 25-28 August 2008[1]

Document RFL/2008/REC01-E

28 August 2008

Original: English

Forum Recommendations

The ITU Regional Cybersecurity Forum for Eastern and Southern Africa was held in Lusaka, Zambia from 25 to 28 August 2008. The forum, which was hosted by the Communications Authority of Zambia and the Government of Zambia, and jointly organized by the ITU and COMESA, aimed to identify the main challenges faced by countries in the region in developing frameworks for cybersecurity and CIIP, to consider best practices, share information on development activities being undertaken by ITU as well as other entities, and review the role of various actors in promoting a culture of cybersecurity.

Approximately 60 people from 21 countries and 4 regional organizations participated in the event. Among the participants were professionals from governments, regulatory authorities, private sector, and civil society. Full documentation of the event, including the final agenda and all presentations made, is available on the event website at www.itu.int/itu-d/cyb/events/2008/lusaka/.

[1] ITU Regional Cybersecurity Forum website: www.itu.int/ITU-D/cyb/events/2008/lusaka/

Forum Recommendations

ITU Regional Cybersecurity Forum for Eastern and Southern Africa[2]

At the conclusion of the Regional Cybersecurity Event, the participants agreed on the following outcomes and recommendations:

- Recognized that improving cybersecurity is a global problem and that each country in the region must improve its national efforts and undertake actions to join and support regional and international efforts to improve cybersecurity.
- Requested countries to join in a harmonized regional approach to addressing cybersecurity.
- Agreed that a critical component of developing a national cybersecurity strategy is joining regional and international efforts to promote a culture of cybersecurity.
- Recognized the existing initiatives, actions and approaches that have worked in a number of countries and in other regions and the efforts of the ITU and other organizations to elaborate projects and develop tools which can support national efforts for Eastern and Southern Africa.
- Recognized that the ITU integrated approach on cybersecurity related activities, and its effort in fostering international cooperation, for instance through the ITU Global Cybersecurity Agenda, offers a useful guide for raising awareness and initiating and/or reviewing national cybersecurity action as well as ensuring consistency and compatibility at international level.
- Requested countries in the region to utilize the ITU Cybersecurity/CIIP Self-Assessment Toolkit as a means to develop their institutions, policies and strategies for cybersecurity and for protecting critical information infrastructures.
- Requested each country in the region to identify a leading institution to act as a focal point for cybersecurity efforts.
- Emphasized the importance of developing regional and international cooperation that can provide guidance in implementing initiatives aimed at strengthening cybersecurity among countries within and outside the region.
- Encouraged the development of models for capacity building that can be adapted to the needs of each country in the region.
- Recognized that countries in the region may need support and assistance to formulate and implement the national cybersecurity strategy and use the ITU Cybersecurity/CIIP Self-Assessment Toolkit to review cybersecurity readiness, and requested that ITU and Regional Integration Organization (RIOs) provide support in this effort.
- Agreed that each country in the region should:
    1. Develop a national cybersecurity strategy (See Annex 1);
    2. Review and, if necessary, revise current cyber-legislation, and draft new legislation, to criminalize the misuse of ICTs, taking into account the rapidly evolving cybersecurity threats (See Annex 2), and;
    3. Develop incident management capabilities with national responsibility and use current examples of CSIRTs/CERTs when developing these (See Annex 3).

    (See Annexes 1, 2, and 3 for more details)
- Agreed on the establishment of a working group to pursue cybersecurity efforts in the region, more specifically to consolidate and elaborate the regional strategy, legislation framework, and watch, warning and incident management draft documents developed by the Forum. The working group will consist of Member States as well as COMESA, UNECA, ITU, African Union, IOC, EAC, and Regional Integration Organizations.
- Requested ITU-D in partnership with COMESA and other regional and international organizations as well as national entities to undertake initiatives necessary to follow-up on implementing the

[2] The Cybersecurity Forum Recommendations can also be found online: www.itu.int/ITU-D/cyb/events/2008/lusaka/recommendations-and-outcomes-lusaka-aug-08.pdf

recommendations from the regional forum and to provide updates on progress and regional and international cooperation.

- Commended the cooperation and collaboration between ITU and COMESA in jointly organizing this regional event and encouraged the cooperation to be extended to include other regional and international organizations.