International
Telecommunication
Union

Common Market
for Eastern and Southern
Africa

# Opening Remarks 25 August 2008

## ITU Regional Cybersecurity Forum for Eastern and Southern Africa[1]

## Lusaka, Zambia
## 25-28 August 2008

Marcelino Tayob
Head, ITU Area Office for Southern Africa

Mr. Marawa, Director of Infrastructure Development, COMESA,

Distinguished Guests,

Colleagues and Friends,

Ladies and Gentlemen,

It is for me a great honor and pleasure to participate in this event and in particular to, on behalf of the ITU, address you in this opening ceremony.

First of all, on behalf of the ITU Secretary General, Dr. Hamadoun Touré, the Director of the BDT, Mr. Sami Al Basheer Al Morshid and all ITU staff I would like to convey our condolences to the Government and people of Zambia for the loss of the President Mwanawasa. Indeed Zambia, SADC, COMESA and Africa in general had lost a great leader.

Ladies and Gentlemen:

[1] See the ITU Regional Cybersecurity Forum for Eastern and Southern Africa website at www.itu.int/ITU-D/cyb/events/2008/lusaka/

This Forum has been co-organized by COMESA and ITU and it is kindly hosted by the Government of Zambia through the Communications Authority of Zambia. On behalf of the ITU I would like to take this opportunity to thank the Government of Zambia and the CAZ for your kindness in hosting this event despite the particular moments Zambia is going through.

As I have mentioned before, this is the second event that ITU has co-organized in partnership with COMESA recently. The first was held in Addis Ababa, Ethiopia and was a workshop on Competition and Changing Marked Conditions: Impact on ICT Regulations and Tools Kits for Eastern and Southern Africa. This is the second event from a list of activities we have agreed to undertake together, subject to availability of resources.

This sort of partnership is in line with the ITU policy to work with Regional Organization in order to better deliver to our common membership, better services, rationalize the use of our resources, complementing to each programs and activities rather than duplicate and/or compete to each other.

Ladies and Gentlemen:

As indicated in the agenda for this forum, the aim of this event is to identify the main challenges faced by countries in this region in developing frameworks for Cybersecurity and Critical Information and Infrastructure Protection (CIIP), share information on the best practices on the matter, look on what ITU and other entities are doing and what they can do to assist countries in this domain and also to review the role of the various actors in promoting a culture of cybersecurity.

As you all know, more we move into information era, more we depend on the computers and communications networks that are more and more interconnected to each other creating risks that due to its global nature has to be managed both at national and international level. This makes cybersecurity an issue that cut across economic, technical, legal and social arenas. In other words is not enough to have good national and international legislation if the environments are conducive for its enforcement. A technical failure in one country can affect technically and economically other countries.

During these three or four days we will have the opportunity to go into details of these and other related issues.

Ladies and Gentlemen:

Due to its recognized importance the ITU mandated by its Plenipotentiary Conference is active in cybersecurity activities in all sectors i.e. ITU-T, ITU-R and ITU-D. The activities include Study Groups, capacity buildings, etc. In one of the sessions one of my colleagues will lead you through what ITU is doing in this area, and I hope you will discuss what we as a region would like to see ITU doing that would impact on the countries needs in cybersecurity matters.

You may recall that leaders from around the globe at the World Summit on the Information Society (WSIS), held in two phases in 2003 and 2005, recognizing the importance of international cooperation for cybersecurity, entrusted ITU to play a leading role in coordinating the worldwide response to these global challenges. This is why, just over a year ago on 17 May 2007, ITU launched the Global Cybersecurity Agenda (GCA), which is the ITU framework for international cooperation, aiming at proposing strategies for solutions to enhance confidence and security in the globalized information society.

Through the establishment of a multi-stakeholder High Level Experts Group (HLEG), GCA builds on existing national, regional and international initiatives to avoid duplication of work and encourage collaboration amongst all relevant partners. The HLEG advises ITU's Secretary-General on global strategies in all five work areas of the GCA. In this regard, I am pleased to share with you some of the recent initiatives by ITU Secretary-General, such as:

1) Collaboration with the International Multilateral Partnership Against Cyber Terrorism (IMPACT) initiated by Malaysian Prime Minister, as one of the physical homes for the GCA;
2) A series of interviews and meetings with Japanese Prime Minister and numerous ministers during OECD Ministerial in Seoul as well as media during his recent missions to Japan and Korea with the objectives to combat cybercrime in addition to climate change and roles of ICTs; and
3) A special High Level Segment session on cybersecurity will be held at the forthcoming ITU Council in 2009, which the Malaysian Prime Minister together with other Heads of States have been invited to attend.

Should there be any organizations and countries interested in exploring possibilities of collaboration with the ITU to meet the GCA goals, we would be happy to pursue various ways of the public-private partnerships. More information on this and matters can also be found in the ITU website that I invite you visit.

Having said that, Ladies and Gentlemen I would conclude by thanking all participants that have travel to this beautiful resort and the speakers (some sacrificing their summer vacation) that have accepted to join and lead us through the process and share their experiences with us.

I thank you for listening.