Common Market
for Eastern and
Southern Africa

International
Telecommunication
Union

ITU Regional Cybersecurity Forum 2008 Lusaka, Zambia

Document RFL/2008/01-E Rev.1

29 August 2008

Original: English

Meeting Report :

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

Please send any comments you may have on this draft meeting report to cybmail(at)itu.int

Purpose of this Report

1. 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 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. The forum also considered initiatives on the regional and international level to increase cooperation and coordination amongst the different stakeholders.

2. The forum was held in response to ITU Plenipotentiary Resolution 130: Strengthening the role of ITU in building confidence and security in the use of information and communication technologies (Antalya, 2006) and the 2006 World Telecommunication Development Conference Doha Action Plan establishing ITU-D Study Group Question 22/1: *Securing information and communication networks: Best practices for developing 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/. This meeting report[2] summarizes the discussions throughout the four days of the ITU Regional Cybersecurity Forum for Eastern and Southern Africa, provides a high-level overview of the sessions and speaker presentations, and presents some of the common understandings and positions reached at the event.

3. The third day of the ITU Regional Cybersecurity Forum, 27 August 2008, was dedicated to specific working sessions on developing national and regional cybersecurity/CIIP capacity through three working groups. The working groups focused on 1) developing a national cybersecurity strategy, 2) legislation and enforcement and, 3) watch, warning, and incident response. In addition to the overall forum recommendations, Annexes 1, 2, and 3 at the end of this document has more information on the recommendations and suggestions that were developed by the three ad hoc working groups[3].

ITU Regional Cybersecurity Forum for Eastern and Southern Africa held in Lusaka, Zambia, 25-28 August 2008

4. As background information, considering that modern societies have a growing dependency on information and communication technologies (ICTs) that are globally interconnected, countries are increasingly aware that this creates interdependencies and risks that need to be managed at national, regional and international levels. Therefore, enhancing cybersecurity and protecting critical information infrastructures are essential to each

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

[2] This Forum Report is available online: http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/lusaka-cybersecurity-forum-report-aug-08.pdf

[3] The Forum Recommendations and the outputs of the three ad hoc working groups can be found at: http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/recommendations-and-outcomes-lusaka-aug-08.pdf

nation's security, social and economic well-being. At the national level, this is a shared responsibility requiring coordinated action related to the prevention, preparation, response, and recovery from incidents on the part of government authorities, the private sector and citizens. At the regional and international level, this necessitates cooperation and coordination with relevant partners. The formulation and implementation of a national framework for cybersecurity and critical information infrastructure protection therefore requires a comprehensive, multi-disciplinary and multi-stakeholder approach. The Regional Cybersecurity Forum discussed some of the key elements in developing such policy and regulatory frameworks and proposed some concrete actions that can be taken in implementing these.

Meeting Opening and Welcome

5. The Regional Cybersecurity Forum for Eastern and Southern Africa was opened with a welcoming address[4] by Amos Marawa, Director for Infrastructure Development, Common Market for Eastern and Southern Africa (COMESA). On behalf of COMESA, Mr. Marawa welcomed the forum participants to the event and highlighted why this regional cybersecurity event is an important step towards building cybersecurity capacity in the region. He noted that the country is in mourning after the death of the President and in this regard before proceeding with the forum, together with the forum participants he observed a minute of silence to join in the mourning of the late President. Mr. Marawa further thanked the ITU for organizing the event together with COMESA and the Communications Authority of Zambia (CAZ) for the hosting of the event. He then reminded the forum participants of the vision of COMESA to establish a fully integrated and competitive community through increased cooperation and integration in all fields of development, including information and communications technologies. He mentioned that COMESA through its regional integration agenda and in accordance with the COMESA Treaty has been developing policies, regulations, and programmes aimed at enhancing and deepening regional integration in this respect.

6. Mr. Marawa continued by emphasizing the need for harmonized techno-legal legislation to move forward in the fight against cybercrime and related threats, as neither law nor technical solutions alone are sufficient. In Africa, he said, the ICT revolution might fail to bring the desired and much needed results if countries do not adopt a sound regional approach to establishing national cybersecurity policies and legislation. In this respect he noted that constant developments in ICT make up an ever-changing environment which is too complicated for any one country to understand and handle alone. Therefore, countries in the region need external expertise to effectively meet the challenges posed by ICTs. Over time, the region as a whole must develop collective expertise and establish public-private partnerships to help each other in their respective approaches in building cybersecurity capacity. As the regional today does not have a sound security base, Mr. Marawa concluded by noting the need for national, regional and international partnerships in areas such as e-commerce, internet business law, etc. He asked the forum participants to come up with a regional legislative cybersecurity framework, a possible model for a regional cybersecurity strategy, and to establish a pool of experts and a regional cooperation system to ensure follow up and implementation of the forum recommendations.

7. Marcelino Tayob, Head, ITU Area Office for Eastern and Southern Africa[5] followed with some opening remarks[6] on behalf of the ITU, ITU's Secretary-General Dr. Hamadoun Touré, and the Director of the ITU Telecommunication Development Sector (ITU-D), Sami Al Basheer Al Morshid. He started his remarks by conveying condolences on behalf of the ITU to the government and people of Zambia for the loss of the President Mwanawasa, highlighting that Zambia, SADC, COMESA and Africa has lost a great leader. Mr. Tayob further thanked the Government of Zambia and CAZ for hosting the Regional Cybersecurity Forum despite the particular moment Zambia is going through. He noted that this is the second event that ITU has co-organized with COMESA this year. The first was held in Addis Ababa, Ethiopia and was a workshop on Competition and Changing Marked Conditions: Impact on ICT Regulations and Toolkits for Eastern and Southern Africa. Working closely with COMESA and other regional organizations in organizing workshops and other capacity building activities is the sort of partnership that is in line with the ITU policy to work with regional organizations in order to deliver to the common membership improved services, rationalize the use of resources and complementing each organization's programmes and activities rather than duplicating and competing with one and other.

8. Mr. Tayob noted that ITU is committed to working together with the membership to come to a common understanding on the importance of promoting a global culture of cybersecurity. Due to its recognized importance, ITU, mandated by its Plenipotentiary Conference, has ongoing cybersecurity activities in all of its sectors, ITU-T, ITU-R, and ITU-D. These activities include Study Groups, capacity building initiatives, and so on, noting that the ITU representatives present at this Forum look forward to discussing further with the countries in the region what Member States would like to see ITU doing that would assist countries when it comes to cybersecurity. You may recall, he continued, that leaders from around the globe at the World Summit on the Information Society (WSIS), held in two phases in 2003 and 2005, recognized the importance of international cooperation for cybersecurity and entrusted ITU to play a leading role in coordinating the worldwide response to

[4] Not available in print.

[5] http://www.itu.int/ITU-D/afr/

[6] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/itu-opening-remarks-lusaka-aug-08.pdf

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, aimed at proposing strategies for solutions to enhance confidence and security in the information society. The GCA builds on existing national, regional and international cybersecurity-related initiatives to avoid duplication of work and encourage collaboration amongst all relevant partners.

9. Mr. Tayob also shared with the forum participants some of the recent initiatives by ITU Secretary-General in this regard. This includes, collaboration with the International Multilateral Partnership Against Cyber Terrorism (IMPACT) initiated by the Malaysian Prime Minister, a series of meetings with the Japanese Prime Minister and numerous ministers during the OECD Ministerial in Seoul, Republic of Korea, with the objective of combating cybercrime as well as addressing climate change, and a special high level segment dedicated to cybersecurity at the forthcoming 2008 ITU Council. Mr. Tayob called out to organizations and countries that may be interested in exploring possible collaborative activities with the ITU to meet the GCA goals, to contact the Secretariat. Mr. Tayob concluded his opening remarks by wishing the participants a successful event.

Session 1: Towards a Framework for Cybersecurity and Critical Information Infrastructure Protection

10. The necessity of building confidence and security in the use of ICTs, promoting cybersecurity and protecting critical infrastructures at national levels is generally acknowledged. As national public and private actors bring their own perspective to the relevant importance of issues, in order to have a consistent approach, some countries have established institutional frameworks while other countries have used a light-weight, non-institutional approach. Many countries have not yet established a national strategy for cybersecurity and CIIP. This first forum session, chaired by Sufian Dafalla, Telecom Officer, COMESA, introduced the concept of a national framework for cybersecurity and CIIP and presented some of the ongoing cybersecurity efforts in the ITU, in order to provide meeting participants with a broad overview of the issues and challenges involved. Mr. Dafalla opened the session and invited the two speakers in this session to proceed with their presentations sharing information on some of the ongoing and planned ITU activities to build capacity in the area of cybersecurity.

11. Marco Obiso, Advisor, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Bureau (BDT), in his presentation provided an overview of "ITU-D Activities in the Area of Cybersecurity and Critical Information Infrastructure Protection (CIIP)"[7]. He started by providing an insight into ITU's overall activities in the area of cybersecurity, noting that there are cybersecurity-related activities ongoing in all three ITU Sectors. The Development Sector, he said, is the front end for ITU activities in the different regions, working closely together with partners in implementing projects and initiatives. Adopting a multi-stakeholder approach is essential to all ITU activities, he continued, especially in the area of cybersecurity as the related challenges cannot be dealt with in isolation. Mr. Obiso highlighted that ITU's approach to address the challenges involved in WSIS Action Line C5 and building confidence and security in the use of ICTs, is the Global Cybersecurity Agenda (GCA), a tool that the ITU is using to aggregate and harmonize internal ITU activities on cybersecurity conducted in all three ITU sectors and to work with the external stakeholders, organizations and experts, ensuring also to implement the recommendations that have come out of the GCA.

12. Mr. Obiso went on to share details on the ITU-D Cybersecurity Work Programme to Assist Developing Countries (2007-2009)[8], with specific examples of what the ITU is trying to do to help developing countries in the domain of cybersecurity and CIIP. Some of the ongoing and planned ITU cybersecurity initiatives mentioned in his presentation included: activities dealing with the identification of best practices in the establishment of national frameworks for cybersecurity and CIIP; a national cybersecurity/CIIP readiness self-assessment tool; a botnet mitigation toolkit; cybersecurity guideline publications for developing countries; an international survey of national cybersecurity/CSIRT capabilities; a toolkit for model cybercrime legislation for developing countries; a toolkit for promoting a culture of cybersecurity as well as a number of planned regional events for awareness-raising and capacity building on cybersecurity and CIIP. He further noted that the *Work Programme* describes how ITU plans to assist countries in developing cybersecurity capacity, through providing Member States with useful resources, reference material, and toolkits on related subjects. As the related toolkits become more stable, the ITU-D is looking to disseminate them widely through multiple channels to ITU's 191 Member States.

13. Joseph Richardson, Consultant, United States of America, followed with his presentation providing a more detailed insight into the "ITU National Cybersecurity Approach" and the related "ITU National Cybersecurity/CIIP Self-Assessment Tool"[9]. Mr. Richardson described the approach for organizing national cybersecurity/CIIP efforts, which includes policy statements, identifies goals and specific steps to reach these goals, and references and material related to each specific step. Mr. Richardson further noted that the elaborated approach for organizing national cybersecurity/CIIP efforts is a living document and as such will evolve over time. Highlighting that the protection of cyberspace is essential to national security and economic well-being, Mr. Richardson continued by

[7] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/obiso-itu-cybersecurity-overview-lusaka-aug-08.pdf

[8] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf

[9] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/richardson-cybersecurity-framework-overview-lusaka-aug-08.pdf

provided some concrete ideas on how countries can get started on developing a national cybersecurity strategy. An important tool in this effort is the ongoing ITU work to develop a comprehensive National Cybersecurity/CIIP Self-Assessment Tool[10].

14. The tool can assist governments in examining existing national policies, procedures, norms, institutions and other elements necessary for formulating security strategies in an ever-changing ICT environment. It can help governments better understand existing systems, identify gaps that require special attention and prioritize national response efforts. Mr. Richardson highlighted that the toolkit identifies issues and poses a number of questions that might be worth considering; what actions have been taken to date, what actions are planned, what actions are to be considered, and what is the status of these actions? Mr. Richardson also noted that no country is starting at zero when it comes to initiatives for cybersecurity. Furthermore, there is no one right answer or approach as all countries have unique national requirements and circumstances. Continual review and revision is also needed of any approach taken, and it is equally important to involve all stakeholders, appropriate to their roles, in developing a national strategy. Countries interested in undertaking a facilitated national cybersecurity/CIIP self-assessment together with the ITU can contact the ITU Development Bureau at cybmail@itu.int.

Session 2: Organizing National Cybersecurity/CIIP Efforts and Country Case Studies: Promoting a Culture of Cybersecurity

15. In order to better understand the approach for organizing national cybersecurity/CIIP efforts and further explore how different countries are currently approaching cybersecurity, Session 2, moderated by Garry Mukelabai, Information Systems Manager, Communications Authority of Zambia, Zambia, looked closer at the building blocks needed to successfully Promote a Culture of Cybersecurity.

16. Christine Sund, Cybersecurity Coordinator, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Sector (ITU-D), in her presentation on "Promoting a Culture of Cybersecurity – Fundamentals"[11] provided an overview of what a culture of cybersecurity means and some of the possible roles of different stakeholders in the Information Society in creating a global culture of cybersecurity. She highlighted the nine elements for creating a culture of cybersecurity as stated in UN Resolution 57/239 (2002): "Creation of a global culture of cybersecurity", and UN Resolution 58/199 (2004): "Promotion of a global culture of cybersecurity and protection of critical information infrastructures". These nine elements include: a) awareness, b) responsibility, c) response, d) ethics, e) democracy, f) risk assessment, g) security design and implementation, h) security management, and i) reassessment. Through these Resolutions, UN Member States and relevant international organizations were asked to address and take these elements into account in preparation for the two phases on the World Summit on the Information Society (WSIS)[12] in 2003 and 2005. The outcome documents from the two WSIS phases further emphasized the importance of building confidence and security in the use of ICTs and countries' commitment to promoting a culture of security.

17. Ms. Sund's presentation mentioned some possible roles for governments in promoting a culture of cybersecurity, including: ensuring that a nation's citizens are protected; playing a central role in coordinating and implementing a national cybersecurity strategy; ensuring that the national policy is flexible and adaptive; coordinating responsibilities across authorities and government departments; creating new (or adapting existing) legislation to criminalize the misuse of ICTs; to curb abuses and to protect consumer rights; and to lead national, regional, and international cybersecurity cooperation activities. Ms. Sund emphasized that as ICT infrastructures are in many countries owned and operated by the private sector, their involvement in promoting a national and global culture of cybersecurity is crucial. Effective cybersecurity needs an in-depth understanding of all aspects of ICT networks, and the private sector's expertise and involvement is therefore paramount in the development and implementation of national cybersecurity strategies. Furthermore, Ms. Sund highlighted that governments and businesses need to assist citizens in obtaining information on how to protect themselves online. While cybersecurity at its core is a shared responsibility, with the right tools readily accessible, each participant in the Information Society is responsible for being alert and protecting themselves.

18. John Carr, Secretary, Children's Charities' Coalition on Internet Safety (CHIS), United Kingdom, continued with his case study dealing with "How to Make the Internet and Online Technologies Safer for Children and Young People"[13]. In his presentation he noted that the ICT industry must do much more to protect children and young people using the internet and related applications and technologies. He highlighted that children and young people make up a large proportion of today's internet users and at the same time they are being exposed to harmful or damaging materials online. Increasingly, he continued, across the world children are being abused by sexual predators where the internet plays a key part in facilitating the initial contact that lead to the abuse. When dealing with issues such as spam, viruses, phishing and other cyber threats, the internet industry has

[10] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html

[11] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/sund-promoting-a-culture-of-cybersecurity-lusaka-aug-08.pdf

[12] http://www.itu.int/wsis/

[13] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/carr-safety-for-young-people-lusaka-aug-08.pdf

shown a great willingness and ability to come together to develop common technical standards and protocols, and to agree on common and effective means of promoting these solutions. This is yet to happen when it comes to the field of child protection, he said. As an example, the Children's Charities Coalition on Internet Safety (CHIS) brings together United Kingdom's major child welfare and child protection organizations to focus on promoting children's interests in the online environment. One driver for promoting a culture of cybersecurity is children's and young people's use of ICTs, for the very obvious reason that governments and people see the protection of young people and children as an overall priority for society on the whole, he continued.

19. Mr. Carr shared with the forum participants some possible responses to address the different risks that exist, starting with the critical role of education and awareness for cybersecurity, followed by some technical solutions and legal responses, and finally providing examples of initiatives undertaken by different stakeholders to implement these responses. Mr. Carr noted that a whole range of technical measures have been put in place by industry when it comes to cybersecurity, often associated with companies' corporate social responsibility programs as well as companies' enforcement activities. In the area of child protection in the United Kingdom some successful self-regulation initiatives have also been put in place, he said. Child protection agencies, the police, actors from the internet industry are for instance working on a national strategy for child protection, and codes of practice to deal with child safety and protection have already been adopted. Filtering technology has developed significantly in the recent past and can also be seen as a useful tool towards the common goals, Mr. Carr concluded while noting at the same time that self-regulation efforts might not work in all countries even though they have proven successful in the United Kingdom.

20. Helmi Rais, Manager, CERT-TCC Tunisia, National Agency for Computer Security, Tunisia, continued with his presentation "Case Study on Promoting a Culture of Cybersecurity: The Tunisian Experience"[14]. Representing the only FIRST[15]-recognized Computer Emergence Response Team (CERT) on the African continent, the Tunisian CERT-TCC, Mr. Rais encouraged countries in Eastern and Southern Africa to establish their own government CERTs and/or national centers for coordinating watch, warning and incident response activities. Mr. Rais noted that in the region there is an overall lack of security awareness and understanding of what ICT security is. Some of the challenges that Tunisia has been faced with is the lack of awareness and the shortage of local experts in the security field, as well as the lack of money. In this regard CERT-TCC has been assisting other countries in the region and beyond with specific capacity building, awareness raising and training initiatives. Mr. Rais also shared information about some of the events that are being organized by CERT-TCC for the business community to promote a culture of cybersecurity. One pillar of the CERT-TCC solution talks for the use of open source security solutions, and using these resources to further develop national Tunisian cybersecurity solutions which can be shared with other interested parties on the African continent. He encouraged countries to use open source solutions, actively look for and apply for loans, such as World Bank loans, to initially fund the launch of national cybersecurity activities.

21. While cybersecurity awareness-raising initiatives are undertaken with the overall goal to promote a culture of cybersecurity, there is a clear need for specific and targeted awareness-raising material, Mr. Rais noted. In this regards he gave examples of awareness raising activities that CERT-TCC, in collaboration with other stakeholders, has been organizing for the internet community. This includes creating and distributing IT security awareness raising posters, dedicating personnel to prepare material targeted for journalists, radio and television, cartoons for children, a CD-ROM for parental control, and so on. Mr. Rais also mentioned a master degree in IT security that has been developed to further expand the pool of educated and trained IT security professionals in Tunisia. CERT-TCC is further encouraging the private sector to play an integral role in the awareness raising, training and education efforts. Mr. Rais concluded his presentation by discussing the importance of collaboration between and amongst the different stakeholders, including the collaboration between CERT-TCC and different associations, to get their feedback and input in order to improve the programmes that are being developed.

22. At the end of the sessions, with the help of a practical exercise, Joseph Richardson, helped the forum participants better understand how they can use the ITU National Cybersecurity/CIIP Self-Assessment Tool[16] to assess national cybersecurity readiness for each of the topics. The self-assessment process overall is intended to help governments understand their existing efforts and the practical implications of the initiatives that they are putting in place, identify gaps that require attention and based on this prioritize national efforts. In guiding the countries through the self-assessment process, Mr. Richardson noted that there is no one right answer or approach as all countries have unique national requirements and desires. A continual review and revision is needed of any approach taken and it is equally important to involve all stakeholders, appropriate to their roles, in developing all the components needed for an overall national strategy for cybersecurity. Mr. Richardson mentioned that updates to the toolkit and related resources are continuously made through the ITU-D cybersecurity website (www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html), and country pilot projects to test and evaluate the toolkit are being undertaken in conjunction with a number of regional capacity-building events, forums and workshops organized by ITU in 207, 2008, and 2009.

[14] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/rais-awareness-raising-tunisia-case-study-lusaka-aug-08.pdf

[15] Forum for Incident Response and Security Teams (FIRST) at http://www.first.org/

[16] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html

Session 3: Organizing National Cybersecurity/CIIP Efforts and Country Case Studies: Government — Industry Collaboration

23. The next session looked closer at the Government — Industry Collaboration element for organizing national cybersecurity/CIIP efforts and related country case studies. This session was moderated by Marcelino Tayob, Head, ITU Area Office for Southern Africa in Harare, Zimbabwe, International Telecommunication Union (ITU).

24. Nicholas Ngoma, Telecom Network Engineer, POTRAZ, Zimbabwe shared in his presentation a case study highlighting "The Zimbabwean Experience"[17]. As in many other countries, Mr. Ngoma noted, Zimbabwe stands no exception to the influx of development triggered by ICTs. In order to keep abreast with these developments, it is necessary for the country to empower all sectors, through government-lead initiatives, with enough knowledge on how to use ICT effectively. This in turn has prompted the government to look into new ways of protecting the nation from crimes triggered by the growth in the use of ICTs and the government has launched a national strategy to promote cybersecurity. As a result, Mr. Ngoma said, all concerned stakeholders in related industries must be made to comply with the laws and legislation aimed at curbing cybercrimes. The government has embarked on a drive to bring communication to Zimbabweans through the computerization of schools and communities and this is encouraging communities and schools to join the global online village. Unfortunately, this is also a chance for opportunistic hackers to commit cybercrimes by stealing vital information from these communities. Personal information and record holding communities e.g. government institutions and government financial houses, are the most vulnerable since they are not yet adequately armed to deal with the consequences of these attacks and theft. To date, many such communities are faced with a dilemma as to how to continue developing their online activities without the risk of being attacked by destructive criminal activities.

25. A national strategy for cybersecurity is now being developed and lead by the government to ensure the further promote cybersecurity on all levels of society. As a way forward a bill meant to both curb the misuse of ICTs and protection of the flow of information within the boundaries of Zimbabwe has been signed. The bill, known as Interception of Communication Act [Chapter 11:20], came into effect in 2007. The bill seeks to monitor communication in the course of their transmission through ICT networks in Zimbabwe, and provide the establishment of a monitoring center. This monitoring center is yet to be created as is the Single International Gateway. Mr. Ngoma noted that the main obstacles in implementing the programmes include the shortage of funds to pay for the systems required, the overall threats to the systems and networks in place, and the lack of trained professionals and educational programmes in the area of information and network security.

26. Violet Magagane, Regulatory and Public Policy, Telkom South Africa, continued with a "Case Study on Government — Industry Collaboration: Telkom South Africa"[18]. In presenting on Telkom's strategy in a changing environment, where Telkom is responsible for one of the critical infrastructure in South Africa, she noted that cybersecurity and cyber-related threats have been identified among the top 10 risks to the country. She further highlighted that the costs related to ensuring cybersecurity are estimated to be very high. Ms. Magagane went on to introduce the National Network Operations Center (NNOC) which is the center that is responsible for national cybersecurity. She shared information on the structure that has been established, mentioning also that there are people on call 24 hours a day to ensure that any attacks or threats to the systems are monitored and dealt with instantly when they occur. Routine security tests to assess threats and vulnerabilities on the system are taking place on a daily basis to minimize damage and recovery time from cyber attacks if and when they occur. South Africa's hosting of the 2010 Football World Cup is seen as a deadline for many of the activities that Telkom is planning in the security area.

27. Going forward, Ms. Magagane said, Telkom's technology strategy in the changing environment involves, among other things, security of the telecommunications infrastructure as legacy networks evolve towards next generation networks, and ensuring compliance with the technology strategy and integration (TSI). The strategy deals with the protection of the end-to-end resources, the seamless evolution of technologies overall, as well as stringent security measures in outgoing and incoming networks. She also shared information on the current situation concerning the 200 Electronic Communications and Transactions Act which provides a framework for dealing with cyber-related crime, noting the need to review this act to accommodate changes in today's environment. In conclusion, Ms. Magagane asked for the establishment of a regional forum that would seek to promote competitiveness and the development of an effective and more efficient and secure telecommunication infrastructure. The need to further foster regional cooperation for enhanced cybersecurity through increased information sharing, training and education were seen as some of the main actions required moving forward.

28. Isabel Nshimbe, IT Analyst, Common Market for Eastern and Southern Africa (COMESA) presented COMESA's strategy to get countries to work closely together to build cybersecurity capacity in "COMESA's Strategy to Deter Cybercrime"[19]. Ms. Nshimbe shared with the meeting participants some of the COMESA activities in the area of cybersecurity and noted that security is not a product but a process and everyone should be involved. She mentioned some interesting cases that Zambia has seen in the area of cybersecurity and cybercrime, for

[17] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/ngoma-zimbabwe-security-culture-lusaka-aug-08.pdf

[18] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/magagane-telkom-SA-case-study-lusaka-aug-08.pdf

[19] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/nshimbi-comesa-cybercrime-activities-lusaka-aug-08.pdf

instance the 1999 defacement of the Zambian Government website where hackers gained access to personal e-mail accounts and other personal information. Ms. Nshimbe noted that COMESA's cybersecurity strategy aims to focus on the people involved, the people using the different technologies and those who are in one way or the other involved in the related processes. Deterrence inside the COMESA network is done on three different levels; security in the networks, in the services and applications layer and with the actual end users and their computers. She shared statistics showing that 98 per cent of the e-mail traffic that enter the COMESA system on any ordinary day is still spam.

29. Ms. Nshimbe continued with sharing details on some of the current and planned cybersecurity activities on the regional level. Under the e-Legislation Programme, a study on e-Legislation has been prepared, and related workshops in 2007 and 2008 planned and implemented. The study and related workshops look at four different but inter-related areas, namely: legal certainty, legal security, legal protection, and legal deterrents. Under the 'legal deterrents' area she mentioned investigations into law reform initiatives including substantive criminal law, procedural criminal law, and the need for enhanced international cooperation. Ms. Nshimbe also brought up for discussion the possible creation of a regional and/or international CyberForensics entity to aid countries in the region in developing their forensics capabilities and expertise, and sharing resources in this regard.

Session 4: Organizing National Cybersecurity/CIIP Efforts and Country Case Studies: Legal Foundation and Enforcement

30. Appropriate legislation, international legal coordination and enforcement are all important elements in preventing, detecting and responding to cybercrime and the misuse of ICTs. This requires updating of criminal law, procedures and policies to address cybersecurity incidents and respond to cybercrime. As a result, many countries have made amendments in their penal codes, or are in the process of adopting amendments, in accordance with international conventions and recommendations. Session 4 looked closer at the need for a sound legal foundation and effective enforcement. The Session 4 moderator, Lucky Waindi-Kulecho, Legal Officer, Communications Commission of Kenya, Kenya introduced the speakers in the session, and mentioned the need for increased collaboration between countries in the region in this regard.

31. Marco Gercke, Lecturer, University of Cologne, Germany, provided the first presentation in the session with an insight into some of the "Legal Foundation and Enforcement Fundamentals"[20], highlighting what is currently happening in the international community and especially with regards to countries' efforts in revising existing laws and developing new legislation to criminalize the misuse of ICTs. Mr. Gercke noted that there are constantly new offenses and new challenges when it comes to the internet and because of this national legislation constantly needs to be revised and updated. Countries and stakeholders involved first need to look at the technology involved and see how it is being misused, and then protect the users through new legislation, keeping in mind that there is always a time gap between recognizing a crime and law adjustments. While there are many internet-related challenges that need to be addressed with legal solutions, he continued, not all challenges need legal solutions. Countries should therefore not start thinking about criminalizing things on the internet that would not be criminalized outside of the internet. Mr. Gercke noted that a legal foundation provides the framework to investigate, prosecute and deter cybercrime, promote cybersecurity, as well as encourage commerce.

32. While elaborating on national, regional and international cybercrime legislation, Mr. Gercke emphasized the importance of and need for further harmonisation of legislation. He noted that there are a number of international initiatives for cybersecurity and the fight against cybercrime, and that all these different initiatives have a role to play. With regards to the Budapest Convention on Cybercrime Mr. Gercke mentioned that it covers the relevant areas of cybercrime legislation (including substantive criminal law, procedural law, and international cooperation) and can be applied to common law and civil law countries. Mr. Gercke further noted that finding adequate solutions to respond to the threat of cybercrime is a major challenge for developing countries. Developing and implementing a national strategy for cybersecurity, including fighting cybercrime, requires time and can be quite costly, which in turn may prevent countries from taking the necessary steps. It is however increasingly important for each country to develop the capabilities and competences required to revise their legislation, investigate abuse or misuse of networks and ensure that criminals who attack or exploit the networks are punished.

33. Ehab Elsonbaty, Senior Judge, Damanhour Court, Egypt, with his presentation "Country Case Study and Overview – Legal Foundation and Enforcement"[21] provided an insight into some of the legal tools that are currently being used to address cybercrime in Egypt. He noted that as cybercrime is growing much more that physical crime, and critical infrastructures are increasingly run on and managed by computers and networks, the rules in the Egyptian legal system for cybercrime are currently being revised. All countries in the region, and beyond need to ensure that their criminal laws are revised to accommodate for the particular nature of cybercrime, he said. This updating may be done by modifying some articles regarding the classical crimes done via new media, abolishing some others which are not adequate or even by creating new rules for completely new

[20] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/gercke-legal-framework-lusaka-aug-08.pdf

[21] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/elsonbaty-legislation-enforcement-lusaka-aug-08.pdf

issues. Mr. Elsonbaty also noted that the levels of punishment, be it imprisonment or fines, should also be reviewed. The importance of developing training programmes for law enforcement officers, prosecutors as well as for judges and legislators was furthermore emphasized by Mr. Elsonbaty. The international nature of cybercrime, he continued, creates the need for an international solution which covers substantive, procedural and international cooperation rules. In this regard he mentioned the work done in Egypt and that he was looking forward to a modern Egyptian cybercrime act. Finally Mr. Elsonbaty mentioned the G8 24/7 High Tech Network as a useful contact network for dealing with cases that involve collecting electronic evidence across borders.

34. Garry Mukelabai, Manager, Information Systems, Communications Authority of Zambia (CAZ), Zambia, followed with a "Country Case Study: Cybersecurity in Zambia"[22]. Mr. Mukelabai noted that while Zambia was one of the pioneers of the internet in the region, the number of internet subscribers at 16,830, or 0.144 per 100 inhabitants, is still quite low. The reasons for this include the high cost of access, poor infrastructure, poor general awareness amongst users, and inadequate general ICT skills amongst end users and professionals. The country has realized that cybersecurity is very important as critical sectors of a nation's economy already today rely upon IP networks for transacting business, as well as for providing energy, transportation, water, banking, and other essential government services and in order to achieve maximum economic benefit from the use of IP networks, these networks need to be reliable, secure, and trusted.

35. In the area of legal responses to cybercrime a number of initiatives have been undertaken in Zambia. The 2004 Computer Misuse Act is in place however changes in the environment since its implementation have made this Act inadequate for meeting current requirements. Mr. Mukelabai also mentioned the 2007 ICT Policy March, the ICT Bill which is currently being reviewed by the Zambian parliament being, and the ongoing initiatives to draft an ICT Security Bill and an E-signature Law. He further highlighted the urgent need for trained judiciary and law enforcement officers in the country. To date, Mr. Mukelabai continued, Zambia has few recorded cases of cybercrime but a well published case involves the replacement of the portrait of the then republican President Fredrick Chiluba with a cartoon caricature. In this case the offender was charged using the Telecommunication Act of 1994 that was created to regulate the telephone industry and ISPs and thus the charge failed to stick. At the time a bill was being drafted that was specifically going to deal with computer-related crimes and since then the Zambian police has received several reports of online fraud and related cases. Today, the Fifth National Development Plan and the Zambia 2030 Vision includes, to some extent, the need to ensure that efforts are undertaken to build confidence and security in the use of ICTs. The 13th pillar of the related ICT Policy, which was launched in March 2007, is dedicated to "Security in the Information Society". The policy highlights that one of the greatest concerns in connected societies is security of information passing through networks and systems such as computers, financial transactions, health records, etc. As Zambia embraces ICTs, more security concerns and abuse shall arise if no counter measures are put in place, Mr. Mukelabai continued, asking for the different stakeholder groups to take the necessary steps to ensure that they understand what their respective responsibilities are in making cyberspace more secure. In order to move forward on cybersecurity in the country the Ministry of Communications and Transport are coordinating the establishment of a national cybersecurity agency which would be tasked with overseeing the running of the various aspects of this national effort, including incidence response, critical information infrastructure protection, national coordination, regional cooperation, security audits, and training and awareness raising initiatives, he concluded.

36. Thys Kazad Tshibind, Engineer, ARPTC, Democratic Republic of Congo, in his "Country Case Study: Democratic Republic of Congo"[23], shared some insights into the activities currently underway in the Democratic Republic of Congo. DRC is in the process of moving to the next development phase, and security is a main challenge in this. Cybersecurity, or rather the lack of security and trust in the internet, has implications for everyone involved, governments, businesses and users, and all countries are trying to figure out how best to raise cybersecurity awareness in order to create a safe cyberspace for all. With 200,000 internet subscribers, five out of ten businesses connected to the internet, and five out of ten banks using electronic transactions and bank cards, Mr. Kazad noted that there is currently no cybersecurity-related legislation in place in DRC. However, some crimes have been classified according to the classical offenses and are in this way to some extent covered by existing legislation. He mentioned Law 013 from 16 October 2002 which deals with Telecommunications in the DRC, highlighting that this law does not deal with ICTs and the internet and is in dire need of thorough revision.

37. Mr. Kazad also went into some of the challenges that DRC is facing when developing its national cybersecurity response. Here he mentioned the lack of internal synergy and coordination, the lack of legal ICT experts and poor general understanding of ICTs and the problems they may cause amongst policymakers, as well as poor knowledge of the added value of ICT in national economy. Mr. Kazad ended his presentation with some recommendations to the group on how to move forward in this area. He emphasized the need to clarify what the region would want from regional and international cooperation in this area, and what would be expected from COMESA in this regard. He specifically asked COMESA to lead the work on the development of cybersecurity directives for the countries in region, and also that countries should be asked to include these in their national legislation. Mr. Kazad also shared with the meeting participants the idea of establishing a cybersecurity

[22] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/mukelabai-caz-zambia-lusaka-aug-08.pdf

[23] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/kazad-case-study-dem-rep-of-congo-lusaka-aug-08.pdf

commission in COMESA and that resources be made available to countries that need assistance in developing their national cybersecurity frameworks in order to build much needed cybersecurity capacity in COMESA Member States.

38. Andrew Kisaka, Rwanda Utilities Regulatory Agency, Rwanda, in his presentation on "Cybersecurity and CIIP Country Case Study: Rwanda"[24] shared the experience of Rwanda with regards to what has been done to date when it comes to addressing cybersecurity issues. It is a process, he noted, where a dedicated policy is needed to guide the creation of related laws and legislation. In Rwanda, RURA, the Rwanda Utilities Regulatory Agency, is the agency which is responsible for coordinating all activities related to cybersecurity. Rwanda has its National Information and Communication Infrastructure Policy (NICI) plan which is intended to provide an action plan and guideline on how to move Rwanda from an agricultural society to a knowledge-based society by 2020. The 2006 "Solution Building" phase of the plan introduces "ICT applications" and the need to deal with "cybersecurity"-related issues. However, the lack of policy for ICT applications and an appropriate regulatory framework together low awareness of cybersecurity issues were some of the challenges Mr. Kisaka mentioned that Rwanda is facing in accomplishing the goals of the NICI plan. As security is one of the main concerns, Mr. Kisaka mentioned that RURA is currently in the process of identifying the best way to move forward to ensure the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of the national critical information infrastructure.

39. In conclusion the session moderator, Lucky Waindi-Kulecho, Legal Officer, Communications Commission of Kenya, Kenya, shared some insights from her country in "Country Case Study: Towards Development of Cyber Laws in Kenya"[25].

Session 5: Organizing National Cybersecurity/CIIP Efforts and Country Case Studies: Incident Management Capabilities

40. Session 5 looked closer at the different building blocks needed to develop effective Incident Management Capabilities, with examples from countries in the region and the African continent overall. A key activity for addressing cybersecurity at the national level requires preparing for, detecting, managing, and responding to cyber incidents through establishment of watch, warning and incident response capabilities. Effective incident management requires consideration of funding, human resources, training, technological capability, government and private sector relationships, and legal requirements. Collaboration at all levels of government and with the private sector, academia, regional and international organizations, is necessary to raise awareness of potential attacks and steps toward remediation. The moderator of this session was Charles Munamie, Head, Department of Information Systems and Technology Management Services, Ministry of Information and Civic Education, Malawi.

41. Helmi Rais, Manager, CERT-TCC Tunisia, National Agency for Computer Security, Tunisia, in "Country Case Study on Incident Management Capabilities: CERT-TCC, Tunisia"[26] provided an overview of CERT-TCC's mandate, structure and activities, and how these experiences and lessons learned can be of possible assistance to countries in the region thinking about or in the process of developing their national incident management capabilities. In January 2003, there was a decision by the Council of Ministers, and headed by the President, to create a national agency specialized in IT security in order to facilitate the execution of the 2002 national IT security strategy. As a result, CERT-TCC was launched in September 2005. Activities that CERT-TCC is involved in include; watch, warning, and information dissemination, awareness raising (awareness raising campaigns, developing a culture of cybersecurity, information for judges, etc.), information sharing, analysis and collection, incident handling, coordination, and so on. CERT-TCC also provides specific expertise on IT security. Mr. Rais further noted that Tunisia is the only country that has started to provide this service free of charge to national banks and companies and this has made it a very popular service.

42. When considering the framework upon which CERT-TCC is operating and when it comes to dealing with incident handing and incident management at the national level, the first thing that countries need to consider is the importance of being part of a network of competent partners for advice and support. CERT-TCC is working with partners in very many other countries, is a member of FIRST and is part of a number of mailing lists aimed at sharing information on the national and international level. CERT-TCC has a database of threats and virus and currently publishes the information that is collected and regularly sends out advisories to its mailing list subscribers. The mailing list currently has 8000 voluntary subscribers for information in French. On a daily basis the team monitors the state of security and tries to work with other CERTs to share information on existing vulnerabilities. Mr. Rais also mentioned that CERT-TCC has developed an open source work flow tool, which CERT-TCC is willing to share with other countries on the continent free of charge. Mr. Rais ended his presentation by encouraging countries on to continent to establish national CERTs and mentioned that CERT-TCC would be happy to help countries in establishing these national centers.

[24] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/kisaka-karangwa-rwanda-case-study-lusaka-aug-08.pdf

[25] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/waindi-kenya-case-study-legislation-lusaka-aug-08.pdf

[26] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/rais-cert-tcc-tunisia-case-study-lusaka-aug-08.pdf

43. Akram Hamed, National Telecom Corporation, Sudan, in the "Sudan Country Case Study — Incident Management Capabilities"[27] provided a presentation on what the Sudanese government is doing in the field of cybersecurity . He provided an insight into the situation with regards to internet penetration in the country noting that there are currently two telecom companies that also provide internet services in Sudan. He noted that the country is aware of the importance of security in further enhancing and spreading the use of e-government services throughout the country. In order to build cybersecurity in Sudan, he continued, the government has undertaken a number of measures to strengthen the technical aspects of cybersecurity in order to keep up with international developments in the field. This includes establishing protective measures in all new local networks at the government level and raising the awareness of internet dangers amongst users, business people and decision makers in the country. Legislative efforts to fight cybercrime include the two laws that deal with the growing challenges related to cybercrime. The Electronic Transactions Law (2007) can deal with electronic contracting, transactions, digital signatures and other electronic instruments while the Informatics Crimes Law (2007) deals with crimes related to money, data and blackmail, crimes of public order and morals, intellectual property crimes, etc. Organizational efforts to combat electronic crimes include a program to encourage internet service providers to hold log files for Sudanese internet users as well as programs to manage the work of internet cafés in the country.

44. The session chair, Mr. Munamie ended the session by providing an overview of what is happening in Malawi when it comes to cybersecurity, and noted that Malawi can learn a lot from fellow country-mates to make the Malawi cyberspace more tolerant to threats.

Session 6: Organizing National Cybersecurity/CIIP Efforts and Country Case Studies: A National Cybersecurity Strategy

45. Increasingly, electronic networks are being used for criminal purposes, or for objectives that can harm the integrity of critical infrastructure and create barriers for extending the benefits of ICTs. To address these threats and protect infrastructures, each country needs a comprehensive action plan that addresses technical, legal and policy issues, combined with regional and international cooperation. What issues should be considered in a national strategy for cybersecurity and critical information infrastructure protection? Which actors should be involved? Are there examples of frameworks that can be adopted? Session 6 dedicated to the development of a National Cybersecurity Strategy sought to explore in more detail various approaches, best practices, and the key building blocks that could assist countries in establishing national strategies for cybersecurity and CIIP. Building on the presentations made earlier in Sessions 2, 3, 4, and 5 of the forum that showcased the different elements of a national approach to cybersecurity and CIIP, Patrick Mwesigwa, Technical Manager, Uganda Communications Commission, Uganda moderated this session which described the final element which ties the other components together, namely the overall development of a national cybersecurity strategy.

46. The first presentation in this session was delivered by Nafissatou Diallo, Senior Programme Analyst, Department of Information Communications Technology (ICT), Seychelles, "Country Case Study: Status of Cybersecurity and ICT in Seychelles"[28]. In her presentation, Ms. Diallo provided an overview of the status of cybersecurity in the Seychelles. She mentioned that three pieces of legislation have been passed in the country and the government is now considering revising them: the Electronic Transactions Act (2001), the Computer Misuse Act (1998) and the Data Protection Act (2003). In establishing cyber-related legislation and policies, she mentioned that a large group of stakeholders have participated in the process, and she noted that all the same stakeholders will need to be involved in the cybersecurity aspects of future policies and legislation.

47. Ms. Diallo also mentioned that Seychelles is now in the process of moving all government agency services to one network. It is only recently that the country has realized that the country also needs to be sensitized when it comes to cybersecurity threats, mobile phone use and the protection of personal data. Seychelles has been among the leaders in the region in respect to the deployment of ICT and the publication of the NICTP lays the foundation required for the development of a comprehensive National Strategic Plan for ICT. The plan will serve as the roadmap to guide ICT development in the country for the years ahead, Ms. Diallo said, while noting that a greater emphasis on cybersecurity needs to be taken into account in the plan. Going forward some of the main challenges in the area of cybersecurity at the national level include: limited implementation of existing acts (and the need to review the existing acts), low awareness amongst the general public about ICT generally and cybersecurity specifically, limited cybersecurity expertise and know-how, inadequate cybersecurity training and limited dialogue between concerned parties and stakeholders. As a main takeaway from the forum, based on what she has heard from other country representatives and experts, Ms. Diallo noted that there is not enough focus on cybersecurity in current national policies.

48. Patrick Mwesigwa, Director, Technology and Licensing, Uganda Communications Commission, Uganda, provided an overview of ongoing and planned cybersecurity-related initiatives in Uganda in his presentation "Country Case Study: Formulation of Cybersecurity Legislation in Uganda"[29]. Mr. Mwesigwa focused the progress

[27] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/hamed-sudan-case-study-lusaka-aug-08.pdf

[28] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/diallo-case-study-seychelles-lusaka-aug-08.pdf

[29] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/mwesigwa-uganda-legislation-case-study-lusaka-aug-08.pdf

made in the area of cybersecurity legislation, mentioning the three main instruments currently available in Uganda: the Electronic Transactions Bill (2003), the Computer Misuse Bill (2003), and the Electronic Signatures Bill (2003). He also shared information on what other countries in the East African region are doing in terms of harmonizing cyber-related laws and legislation. Laws in the East African countries are going to be harmonized in two phases, with Phase 1 focusing on legislation for Electronic Transactions, Electronic Signatures and Authentications, Data Protection and Privacy, Consumer Protection and Computer Crime and Phase 2dealing with Intellectual Property Rights, Domain Names, Taxation and Freedom of Information. Under this effort a number of regional meetings have already been held and the legal framework is expected to be adopted by relevant organs of EAC in November 2008, subsequently Partner States are expected to enact the new cyber laws by 2010. Mr. Mwesigwa concluded his presentation by emphasizing the need to sensitize policy makers, network operators and individuals on matters related to cybersecurity and encouraged all countries to put in place robust legal frameworks to combat cybersecurity threats. He also noted that due to the borderless nature of cyberspace, international cooperation is crucial in ensuring a safe online environment.

Session 7: Review and Discussion: Organizing National Cybersecurity/CIIP Efforts

49. Session 7, the final session of the day, sought to review and further discuss the elements that make up the Approach for Organizing National Cybersecurity/CIIP Efforts, identifying some of the main takeaways from the presentations on the different elements and the related country case studies in preparation for the concluding forum session. To help organize the session, the session moderators, Abu Sufian E Dafalla, Telecom Officer, Common Market for Eastern and Southern Africa (COMESA) and Marcelino Tayob, Head, ITU Area Office for Southern Africa in Harare, Zimbabwe, asked four panelists to give their main takeaways from sessions already held and, if possible, provide some proposals and recommendations for practical next steps in the Eastern and Southern Africa.

50. Joseph Richardson, Consultant, United States of America noted in his comments that he had heard some good reasons during the course of the past few days why governments should work with industry for cybersecurity and noted that there are many different ways in which to collaborate with the industry. All countries, he said, face the issue that everyone in industry, all different sectors and enterprises, cannot be engaged. To deal with this, countries need instead to find an approach that gathers these representatives in industry associations that in turn can debate on their behalf. Further work is needed to define the frameworks required for this collaboration. Industry collaboration also needs to be looked at in different ways. In particular one area that needs to be further developed is the role of relationships, not only with industry but also with other elements of government. In the future we need to ensure that other ministries, in addition to the communications ministries, are involved in these cybersecurity forums, workshops and related activities. He noted from the comments he had heard this far that the approach to organizing national cybersecurity efforts and the ITU self-assessment tool are useful to countries in the region and that concrete action could be taken to help raise all countries' cybersecurity readiness using these, and other, tools.

51. Ehab Elsonbaty, Senior Judge, Damanhour Court, Egypt noted in his remarks that we should make use of the momentum and move forward on concrete actions now by using the existing instruments in the legal area and accommodate them according to the national systems. With regards to the discussion whether there should be one act or separate acts, he noted that when it comes to cybercrime, more than one act will be needed. Mentioning here that cybersecurity, data and privacy, freedom and information, should be in three different acts. Mr. Elsonbaty also noted the need for a social dialog on cybersecurity and that this discussion cannot only deal with the need for awareness amongst users. With regards to a possible COMESA task force dedicated to cybersecurity issues, he noted that the work on acts from the EAC and other countries in the region should be considered. A good first step would be the creation of and overview of the legal situation in the countries in the region.

52. John Carr, Secretary, Children's Charities' Coalition on Internet Safety (CHIS), United Kingdom, in his remarks highlighted that the protection of children in the online space is important for three main reasons. 1) In its own right, as protecting children, the most precious and the most vulnerable, is something that all countries should do. 2) Governments and politicians can also relate to the needs to protect children. 3) Child protection on the internet is also a good way to allow government to collaborate with the private sector.

53. Helmi Rais, Manager, CERT-TCC Tunisia, National Agency for Computer Security, Tunisia emphasized that any national cybersecurity strategy needs to include some kind of CERT/CSIRT activity. He also noted that the protection of the information infrastructure is important for the overall continuity of the activities of the government and the nation. Mr. Rais mentioned that while laws are important in this respect, they are not the only important things when it comes to cybersecurity. Collaboration between nations and contact points is more important than any laws and legislation when something really happens. As Tunisia has some experience in establishing CERTs, CERT-TCC would be happy to share their experiences in this regard and also contribute to the overall African approach for developing an African center for information security.

Sessions 8 & 9: ITU National Cybersecurity/CIIP Self-Assessment Tool: An Exercise

54. Sessions 8 and 9 of the forum aimed to provide more information on and discuss in further detail the ITU National Cybersecurity/CIIP Self-Assessment Tool. The sessions took the countries through the self-assessment

process to help governments understand their existing efforts, identify gaps that require attention, and prioritize national efforts. The ITU National Cybersecurity/CIIP Self-Assessment Tool is intended to assist national governments in examining their existing national policies, procedures, norms, institutions, and relationships in light of national needs to enhance cybersecurity and address critical information infrastructure protection. The tool is directed to leadership at the policy and management levels of government, and addresses the policies, institutional framework, and relationships for cybersecurity. It seeks to produce a snapshot of the current state of national policy and capability, of institutions and institutional relationships, of personnel and expertise, of relationships among government entities and relationships among government, industry and other private sector entities. Joseph Richardson, Consultant, United States of America acted as the moderator for the two sessions.

Session 10: Regional and International Cooperation

55. Regional and international cooperation is extremely important in fostering national efforts and in facilitating interactions and exchanges. The challenges posed by cyber-attacks and cybercrime are global and far reaching, and can only be addressed through a coherent strategy within a framework of international cooperation, taking into account the roles of different stakeholders and existing initiatives. As facilitator for WSIS Action Line C5 dedicated to building confidence and security in the use of ICTs, ITU is discussing with key stakeholders how to best respond to these growing cybersecurity challenges in a coordinated manner. For instance, the ITU Global Cybersecurity Agenda (GCA) provides a platform for dialogue aimed at leveraging existing initiatives and working with recognized sources of expertise to elaborate global strategies for enhancing confidence and security in the information society. This session facilitated by Abu Sufian E Dafalla, Telecom Officer, Common Market for Eastern and Southern Africa (COMESA), reviewed some of the ongoing initiatives in order to inform meeting participants and to further the discussions in order to identify possible next steps and concrete actions to foster and promote international cooperation for enhanced cybersecurity.

56. Sizo Mhlanga, Regional Adviser, ICT, Science and Technology Division, United Nations Economic Commission for Africa (UNECA), provided a presentation on the "ECA Regional Perspective on e-Security"[30] addressing ECA's response to the growing cybersecurity threats. Limited connectivity and relatively small number of users are factors that currently shield potential African targets from most cyber-related attacks, Mr. Mhlanga said. However, he noted at the same time that African countries are still very vulnerable to most major attacks due to weak underlying technology and vulnerable software. The lack of general cybersecurity awareness amongst users together with uninformed, misguided and malicious users, contribute to the problem, he said. The impact of increased ICT capacity with weak or non-existent legal, regulatory and policy environments and insufficient security technology, therefore makes countries on the African continent a lucrative entry point for cyber-criminals using it as a hub to coordinate and launch attacks, he said. In this regard, Mr. Mhlanga provided an overview of e-government readiness on the African countries and presented some e-government readiness data for different African regional groups (COMESA, SADC, and EAC) and compared this data with that of some European countries. Looking at this data he noted that the main problem is the lack ICT infrastructures.

57. Mr. Mhlanga also shared information on "AISI", which is a vision for ICT development in Africa. Launched in 1996 it also serves as a cooperation framework for partners to support ICT development in Africa. Activities that fall under the AISI initiative include those related to policy development, training and capacity building, sectoral applications and infrastructure development. Within the AISI framework the need for enhanced cybersecurity is reflected in the formulation of national and regional ICT policies and strategies, and in the design of legal frameworks. UNECA is supporting countries in the regional to develop regional and national strategies, including sectoral policies and applications such as those needed for e-applications. In this regard UNECA sees cybersecurity as a sectoral application that should be integrated in overall ICT policies and e-strategies that are being developed and implemented.

58. Mr. Mhlanga also discussed what UNECA has been doing to help countries develop an African cybersecurity framework through the Global ePolicy Resource Network (ePol-NET). This programme which looks at the policy, legislative and infrastructure security requirements involves Burkina Faso, Ghana, Kenya and Mozambique. In this regard there are several projects ongoing in the respective countries. Mr. Mhlanga concluded by encouraging countries in the region to continue participating in initiatives to further strengthen regional and international cooperation noting that UNECA will continue to support governments in establishing cybersecurity policies and in the establishment of the African Public Key Infrastructure Forum.

59. Jacquot Rasemboarimanana, Computer Scientist, Commission de l'Océan Indien (COI)/Indian Ocean Commission (IOC), continued with an overview of "La Communication, la Connectivité et la Sécurité dans la Région COI/Communication, Connectivity and Security in the IOC Region"[31]. In his presentation he provided an insight into the development of ICTs in the Indian Ocean countries and their level of connectivity and security. With regards to the current cybersecurity situation in the region, he noted that under the countries' information security policies when establishing communication centers these needed to be implemented and run with

[30] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/mhlanga-uneca-lusaka-aug-08.ppsm

[31] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/rasemboarimanana-ioc-lusaka-aug-08.pdf

security in mind. With regards to assessment, prevention and training Mr. Rasemboarimanana mentioned that training and outreach programs for acting in a secure manner online were being established. He noted that the problem is often in terms of culture, or the lack of a culture of security at all levels of society. What is needed is the injection of cybersecurity within the everyday use of ICTs, in the establishment of training requirements, education and school curriculums. Mr. Rasemboarimanana noted that as the risks continue to grow, the need for further international cooperation and coordination among different actors will become even more urgent. He encouraged countries in the region to put cybersecurity higher on their national agendas and join in the joint ITU and COMESA efforts for increased cybersecurity.

60. Marco Obiso, Adviser, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Bureau (BDT), as the last speaker in the session presented on the "ITU Global Cybersecurity Agenda (GCA): A Framework for International Cooperation in Cybersecurity"[32]. Through the GCA ITU is paving the way for enhanced global cooperation for a safer and more secure cyberspace. With its 191 Member States and more than 700 Sector Members, including leading industry players, it is well placed to provide the forum for international cooperation on cybersecurity. Because of its long experience in cybersecurity, ITU was entrusted by world leaders at the World Summit on the Information Society to take the lead on action line C5 dedicated to building confidence and security in the use of ICTs. ITU, through its three Sectors, ITU-R, ITU-T and ITU-D, is working towards a global, coordinated and harmonized approach to achieving cybersecurity. Mr. Obiso noted that as the lead facilitator for WSIS action line C5, ITU is working with all key stakeholders on how to best respond in a coordinated manner to the growing cybersecurity challenges. In this regard the ITU Global Cybersecurity Agenda can provide the strategic directions that would foster international cooperation. He also mentioned the leading role played by the ITU Sectors, especially ITU-D, in converting the agreed strategies into actions and projects to be implemented together with partners.

Session 11: Wrap-Up, Recommendations and the Way Forward

61. The final session of the meeting was facilitated by Abu Sufian E Dafalla, Telecom Officer, Common Market for Eastern and Southern Africa (COMESA) and Marcelino Tayob, Head, ITU Area Office for Southern Africa in Harare, Zimbabwe. Together they reported on some of the main findings from the event, and elaborated on a set of recommendations for future activities in order to enhance cybersecurity and increase protection of critical information infrastructures in Eastern and Southern Africa.

62. At the conclusion of the Regional Cybersecurity Forum, the participants agreed on a set of outcomes and recommendations. These can be seen in the **Annexes** to this meeting report. It was also 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)

63. The meeting further 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 recommendations from the regional forum and to provide updates on progress and regional and international cooperation. The meeting also 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.

Meeting Closing

64. In his closing remarks on behalf of ITU, Marcelino Tayob, Head, ITU Area Office for Southern Africa in Harare, Zimbabwe, hoped that the four day long ITU Regional Cybersecurity Forum for Eastern and Southern Africa, including the working sessions dedicated to developing national and regional cybersecurity/CIIP capacity, had proven useful for the forum participants. Mr. Tayob thanked the forum speakers for taking time out of their busy schedules to share their experiences and expertise with the participants. Mr. Tayob thanked everyone who had directly or indirectly contributed to the success of the forum and relayed special thanks to the local hosts and COMESA, for their outstanding work in making this Regional Cybersecurity Forum a successful event. ITU with its long withstanding activities in the standardization and development of telecommunications hopes to continue to provide a forum where the diverse views from governments, the private sector and other stakeholders related to cybersecurity and CIIP can be discussed through its different activities and initiatives.

[32] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/obiso-ITU-GCA-lusaka-aug-08.pdf

This draft meeting report[33] is currently open for the comments for a period of 30 days after reception and publication on the forum website. The email address for comments on this draft report, and for comments on the ITU Cybersecurity Work Programme to Assist Developing Countries (2007-2009)[34], is **cybmail(at)itu.int**[35].

For information sharing purposes, all meeting participants will be added to the **cybersecurity-africa(at)itu.int**[36] for matters concerning ITU-D cybersecurity-related activities. If you have not participated directly in the event, or are not already on the mailing list but interested in participating in these discussions through the relevant mailing list and forum, please send an e-mail to **cybmail(at)itu.int**.

[33] This Forum Report is available online: http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/lusaka-cybersecurity-forum-report-aug-08.pdf

[34] http://www.itu.int/ITU-D/cyb/cybersecurity/index.html#workprogramme

[35] Please send any comments you may have on the workshop report to cybmail@itu.int

[36] Regional ITU cybersecurity mailing list: cybersecurity-africa@itu.int. Please send an e-mail to cybmail@itu.int, to be added to the mailing list.

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[37]

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/.

[37] 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[38]

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:

4. Develop a national cybersecurity strategy (See Annex 1);
5. 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;
6. 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 recommendations from the regional forum and to provide updates on progress and regional and international cooperation.

[38] 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

- 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.

AD HOC WORKING GROUP ANNEX 1

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[39]

Document RFL/2008/WG01-E

28 August 2008

Original: English

Working Group 1: Regional Approach for the Development of a National Cybersecurity Strategy

Recommendations from the Ad Hoc Forum Working Group on a Regional Approach for the Development of a National Cybersecurity Strategy

There is a need for the development of a model national cybersecurity strategy for addressing cybersecurity at the national level. Such a strategy can serve as a coordinating mechanism for the region. Because existing national capabilities vary and threats constantly evolve, the strategy should provide a flexible approach that can assist the nations of the region to review and improve their existing institutions, policies, relationships, and capabilities for addressing cybersecurity. The strategy should support national and regional cybersecurity efforts, the national IT policy, other national and regional policy goals, and the principles of freedom of speech, free flow of information and due process of law.

The strategy should support a comprehensive national approach to cybersecurity and address actions required in key elements, including;

- Promoting a National Culture of Cybersecurity;
- Deterring Cybercrime;
- Creating National Incident Management Capabilities; and
- Establishing National Government-Industry Collaboration.

The strategy should be flexible and able to respond to the dynamic risk environment. It should be developed cooperatively through consultation with representatives of all relevant participant groups including government agencies, industry, academia, and relevant associations. And, it should contain a statement of purpose and operational and implementation provisions. Such provisions are outlined below:

65. Recognize the importance of information and communication technologies to the nation,

66. Recognize the necessity for cybersecurity and that security is a continuing process not a destination.

67. Create awareness at the national policy level and among all national stakeholders of the issues of cybersecurity and the need for national action and regional and international cooperation.

68. Justify the need for national action to address threats to and vulnerabilities of the national cyber infrastructure and call for policy-level discussions and actions to achieve the stated goals in this cybersecurity policy statement.

69. Highlight the need to participate in regional and international cybersecurity efforts.

70. Identify the risks faced, establish the cybersecurity policy goals, and identify how these goals can be implemented.

71. Delineate roles and responsibilities, identify priorities, and establish timeframes and metrics for implementation.

72. Identify a lead person and institution to coordinate the overall national effort as well as lead institutions and cooperating partners, for each element of the national strategy.

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

73. Determine the location, function and role of a national watch, warning and response coordinating operation.

74. Identify cooperative arrangements and establish mechanisms for cooperation among all participants and between government and the private sector.

75. Identify international and regional counterparts and foster international and regional efforts to address cybersecurity, including information sharing and assistance.

76. Call for the development of an integrated risk management process for identifying and prioritizing protective efforts regarding cybersecurity.

77. Call for periodic reassessments of the national strategy and its implementation.

78. Establish or call for the establishment of priorities in national cybersecurity efforts.

79. Identify training requirements and how to achieve them.

80. Identify available resources, expertise and budget and funding requirements.

81. Call for an initial broad review of the adequacy of current national practices and consideration of the role of all stakeholders (government authorities, industry, and citizens) in the process.

82. Be promulgated at the level of head of government to encourage the cooperation of all participants.

83. Be adaptive and integrate state, local, and community-based approaches to national needs and contexts.

****

AD HOC WORKING GROUP ANNEX 2

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[40]

Document RFL/2008/WG02-E

28 August 2008

Original: English

Working Group 2: Legal Foundation and Enforcement

Recommendations from the Ad Hoc Forum Working Group on Legal Foundation and Enforcement

1.0 Legal Foundation and Enforcement Introduction

As modern society's dependence on information and communication technologies (ICTs) grows, so too have cyber crimes. The need to develop and enforce legislation on cyber crimes is, therefore, underscored.

The ad hoc forum working group makes general proposals for inclusion in the COMESA model law on cyber security. These proposals address the following four areas:

- Substantive law criminalizing certain conduct
- Procedural law
- International cooperation
- The treatment of evidence

2.0 Substantive Law

The ad hoc forum working group proposes criminalization of the under listed acts. It is proposed that the working group give a clear description of these crimes:

1. Illegal access to a computer

2. Illegal interception of electronic communication

3. Interference with computer data

4. Interference with a computer system [it is proposed that the working group considers providing for greater penalties for interference with government systems]

5. Misuse of devices [note to have a clear definition of misuse so that legal use is not criminalized]

6. Computer related forgery

7. Computer related fraud

8. Creation, possession or distribution of child pornography [it is proposed that the working group considers penalizing pornography in general, especially for member states already penalizing physical creation, possession and distribution of such material]

9. Identity theft

10. Phishing [the description of the offence should be wide enough to cater for commission of a similar offence through the use of other technology e.g. smishing]

11. Data espionage

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

12. Spamming

13. Harassment

14. Sending of hate speech and commission of other religious offences [Members States should be allowed to exercise discretion in adopting this]

15. Attempt and aiding or abetting of the above offenses [penalties for these should be lighter than those for the actual offences]

16. Corporate liability for the above offences [the working group should determine whether to impose civil or criminal liability]

17. Data protection [to cater for countries that do not have a data protection legislation in place]

3.0 Provisions on procedure

There should be enabling provisions on:

1. Expedited preservation of stored computer data
2. Expedited preservation and partial disclosure of traffic data
3. Investigative authority to compel computer network providers to disclose content and non content information stored on the network
4. Search and seizure of stored computer data by law enforcement authorities
5. Real time collection of traffic data relating to electronic communications
6. Interception of the content of electronic communications
7. Retention of data

4.0 International co-operation

Insert provisions for international co-operation in accordance with relevant international instruments on international co-operation in criminal matters.

New standards should be adopted for mutual assistance, along the 24/7 network point of contact arrangements.

5.0 Evidence

The model law makes provisions addressing admissibility of electronic evidence in court.

****

AD HOC WORKING GROUP ANNEX 3

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[41]

Document RFL/2008/WG03-E

28 August 2008

Original: English

Working Group 3: Watch, Warning, and Incident Response

Recommendations from the Ad Hoc Forum Working Group on Watch, Warning, and Incident Response

This document aims to provide guidelines and recommendations for the establishment of the necessary national and regional organizational structures to initiate Watch, Warning, and Incident Management activities.

1. Establishment of a National Cybersecurity Center that would serve as national point of contact for Cybersecurity. The Center would constitute the basic building block, to evolve in a more consolidated and structured incident management capability (e.g CERT, CSIRT)

- Related Action:
    a. Development of the action plan according to the guidelines provided in the Annex
- Timing: 1 year (3Q 2009)
- Budget: 100.000 USD per Cybersecurity Center (a more detailed breakdown of costs would be provided later on)

2. Definition and implementation of an awareness campaign, in order to share the national experiences at the regional and international level, involving the relevant organizations including AU, ITU, COMESA, IOC, UNECA, EAC, RIOs etc. The process would lead to obtaining the necessary buy-in from key decision makers and to mobilize the necessary financial and human resources.

- Related Action:
    a. Identification of relevant regional meetings in which the Cybersecurity can be addressed.
    b. Organization of at least an annual international event (at regional or continental level), to review the national activities implemented and build the necessary actions to be implemented at regional and international Level
- Timing: Within 2009 (possibly beginning of 2010). NOTE: The timing would depend on the financial capacity available to initiate national activities. Raising awareness activities would be used for fund raising to establish the National Cybersecurity Center
- Budget: To be defined

3. Establishment of a Regional CERT involving COMESA and any other interested African countries. AU, ITU, COMESA, IOC, UNECA, EAC, RIOs and other international organizations would facilitate the coordination and provide all necessary support to the implementation of the related operational activities. The Regional CERT would link to the National Cybersecurity Centers and would facilitate their evolution to national/government CERT, CSIRT. The implementation of this recommendation would be subsequent to the establishment of the National Cybersecurity Centers.

- Related Action:

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

a. ITU, COMESA, UNECA and other interested stakeholders to coordinate and perform the assessment of the operational requirements.

b. Establishment of the implementation plan

c. Deployment

- Timing: 1 year (4Q 2010, 1Q 2011)
- Budget: To be defined

Annex 1:
Operational Guideline for the Establishment of a National Cybersecurity Center

Critical Success Factors

The guideline aims at providing initial indications, including where possible concrete actions to be taken, on the establishment of a National Cybersecurity Center.

To achieve the expected results, some key critical success factors (CSFs) have to be taken in consideration, and compliancy to these would enable the effective implementation of the concerned activity.

CSFs for the establishment and deployment of a National Cybersecurity Center may include:

- Political Commitment – At the highest level possible
- Awareness – Thorough understanding of the needs and the objectives to be achieved
- Ownership – Clear understanding of concepts such us responsibility and accountability
- Management – Operations, sustainability and business continuity
- Budget – The required financial capacity
- “Start small” approach – To be able to build on existing resources minimizing the initial investment.

Phase 1 – Initial Framework – Establishment of the Security Centre

Objective: Establishment of a full operational cell, able to provide a set of well specified services

Requirements:

Human Resources – (3-4 people):

- IT Engineer – Network/Systems administration
- Security Manager – security measures implementation
- Application specialist - Software solutions deployment
- **Note:** For the initial setup, consideration should be given to appropriate personnel already engaged in government and/or government entities.

Equipment and Facilities:

- Client/Server Configuration (standard server, desktop, etc.)
- LAN
- Printing facilities
- Solid and good broadband internet connectivity - 1MB recommended: Lobby for internet connection sponsorship from local ISP
- Facilities - Physical location etc. Consider autonomous government entities like regulators to house the CERT.

Phase 2 – Scope, Coverage, Roles & Responsibilities

Identify focal point responsible for Cybersecurity

- Specific contact person
- Contingency considerations for focal point contacts
    - Automated e-mail responses for example for confidence assurance purposes
- Services to be provided
    - Simple Incident management
        - Stakeholders incident reporting
        - Data gathering and storing
    - Service support & assistance
        - First level support
    - Capacity Building & Awareness

        - Coordination initiation with the relevant stakeholders (IT Managers, Policy Makers, Regulators, ISPs etc)
        - Website establishment for information sharing
        - Training and workshops
        - Regional awareness campaigns
        - Continental awareness campaigns
- Coverage
    - Government Ministries and Agencies
    - Institutional based type clients – NGOs, Civil Society etc
    - Long term cliental coverage to entire citizenry

Phase 3 – Collaborative Network

- National Coordination
    - ISPs, Data Centers
    - Lobby locally available vendors for sponsorship
    - Mailing lists and contact details for institutional clients
- International coordination
    - Coordination with other IT security centers – CERTS
    - Regional Organizations – COMESA, ITU, UNECA, AU, AFRISPA, EAC, RIOs etc

****