ITU Regional Cybersecurity Forum 2009
Tunis, Tunisia

Document RFT/2009/01-E

8 June 2009

Original: English

Draft Meeting Report :

ITU Regional Cybersecurity Forum for Africa and Arab States held in Tunis, Tunisia (4-5 June 2009)[1]

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

Purpose of this Report

1. The 2009 ITU Regional Cybersecurity Forum for Africa and Arab States was held in Tunis, Tunisia from 4 to 5 June 2009. The forum, which was hosted by the National Agency for Computer Security (ANSI), Ministry of Communication Technologies, Tunisia, and dedicated to "Connecting the World Responsibly" aimed to identify some of the main challenges faced by countries in the region in enhancing cybersecurity and securing critical information infrastructures. It considered best practices, information sharing mechanisms and concrete actions for cybersecurity development, taking into consideration the key principles of matching the borderless and transnational nature of cyber-threats and meeting specific national and regional requirements. The forum also looked at actions that are being undertaken or planned by the countries in the region to enhance cooperation and collaboration with other stakeholders at the national, regional, and international levels.

2. The forum, one in a series of regional cybersecurity events organized by the ITU Telecommunication Development Sector (ITU-D), 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), 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*, and for implementing the goals of the ITU Global Cybersecurity Agenda. Experts in specific cybersecurity-related areas from United Nations agencies, international and regional organizations, financial institutions, private industry, non-governmental organizations and representatives from government agencies from 25 countries in Africa and Arab States discussed and elaborated on concrete steps forward to build cybersecurity capacity and competency by sharing information and experiences, exploring partnerships and learning together. Full documentation of the forum, including the final agenda and all presentations made, is available on the event website at www.itu.int/itu-d/cyb/events/2009/tunis/. This meeting report[2] summarizes the discussions throughout the two days of the ITU Regional Cybersecurity Forum for Africa and Arab States, provides a high-level overview of the sessions and presentations, and highlights some of the common understandings noted at the event. Simultaneous interpretation in Arabic, English and French was provided for the participants throughout the forum.

Regional Cybersecurity Forum for Africa and Arab States held in Tunis, Tunisia, 4-5 June 2009

3. As background information, it is commonly agreed that information and communication technologies (ICTs) can play a decisive role in a country's development process. However, the rapid growth in the use of ICTs has also opened up new opportunities for criminals to exploit online vulnerabilities and attack countries' critical infrastructures. As a result, building confidence and security in the use of ICTs is one of the most important and complex challenges connected countries face today. As cyberspace is to large extent without distinct national borders and cyber-threats can arise anywhere and at any time, causing immense damage in a very short space of time before they are tackled, current attempts to address these challenges only at the national and regional

[1] ITU Regional Cybersecurity Forum website: http://www.itu.int/ITU-D/cyb/events/2009/tunis/

[2] This Forum Report is available online: http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/tunis-cybersecurity-forum-report-june-09.pdf

levels are inadequate. A global approach is therefore needed. For this reason, ITU, through its Global Cybersecurity Agenda (GCA), has put in place a framework for international cooperation in cybersecurity. Furthermore, cybersecurity and the protection of critical information infrastructures are a shared responsibility of government, business, other organizations, and individual users who develop, own, provide, manage, service and use information and communication technologies, systems and networks. Promoting cybersecurity, and implementing related measures, needs to be a high priority in order for countries to reap the full benefits of the digital revolution and the new and evolving communication technologies. 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 in the two regions.

Meeting Opening and Welcome

4. Belhassen Zouari, Chief Executive Officer, National Agency for Computer Security and Cert-TCC, Tunisia welcomed the forum participants to the event and highlighted why this event is an important step towards building cybersecurity capacity in Africa and the Arab States. The Regional Cybersecurity Forum for Africa and Arab States was opened with a welcoming address[3] by H.E. Lamia Sghair Chaffai, Secretary of State for Informatics, Internet and Open Source, Tunisia. On behalf of the Government of Tunisia as host for the event, Ms. Chaffai brought the participants' attention to the World Summit on the Information Society (WSIS) Tunis Commitment and Tunis Agenda for the Information Society[4] that emphasized the necessity to set building confidence and security in the use of ICTs high on countries' national ICT development agendas. She further noted the need to foster the development of different kinds of partnerships between countries in the region, other countries present at the event, and beyond. Ms. Chaffai said that Tunisia is a pioneer in the field of ICT and notably cybersecurity. In addition to the Tunisian national cybersecurity strategy and the services provided by the National Agency for Computer Security (ANSI), she also mentioned the need for a supporting legal environment to protect investors.

5. Ms. Chaffai said that for example cyber-auditing has been made compulsory through legislation in Tunisia and that the country also has specific legislation for electronic identification. In the area of capacity building, training and education, Tunisia has been able to create the first national security institute on the African continent, the Tunisian Computer Emergency Response Team Coordination Center (CERT-TCC) that is a member of the global Forum for Incident Response and Security Teams (FIRST). Tunisia also has 7 professional master degrees that aim to build competencies related to network and information security and the country has established a network of national auditors. Ms. Chaffai concluded her opening remarks by highlighting that with an ambitious agenda reflecting many aspects of cybersecurity, this Regional Cybersecurity Forum provides an opportunity for organizations and countries in the region to come together to share experiences. She encouraged further collaboration between African and Arabic stakeholders to work towards common cybersecurity objectives that will foster an inclusive and secure information society.

6. Khedija Gheriani, Secretary-General, Arab ICT Organization (AICTO) also honored the meeting with her presence in the opening session. AICTO is an Arab governmental organization working under the aegis of the League of Arab States, based in Tunisia. Within the scope of the General Arab Strategy for ICTs dedicated to building the Information Society 2007-2012, AICTO and its working groups have activities in a variety of areas, ranging from e-government, e-commerce, e-learning, as well as information and computer security, etc.

7. Miloud Ameziane, Head, ITU Regional Office for Arab States followed with some opening remarks[5] on behalf Sami Al Basheer Al Morshid, Director, ITU Telecommunication Development Bureau. He welcomed the participants to the forum and highlighted that cybersecurity issues constitute a complex mix of technological, political, and cultural challenges. With the number of mobile cellular subscribers having reached 4 billion and the mobile penetration rate estimated at 61 per cent by the end of, Mr. Ameziane reminded the participants of the key role that ICTs play in people's lives. As new technologies are developed and access to ICTs expands, threats to their security are also developing and expanding, he noted. These threats are global in nature, with attacks in one country having an impact on another, while the individual generating the attack could be sitting physically in a third country. Therefore, to safeguard our cybersecurity we have to take a global approach and come to a common understanding on how we can address the needs of all countries, including least developed, developing and developed countries. Only by working together to elaborate strategies and identify best practices, can we address these global challenges, he continued.

8. Mr. Ameziane further reminded the participants that the event serves to follow up on the activities initiated at last year's ITU Regional Cybersecurity Forum for Eastern and Southern Africa held in Lusaka, Zambia (25-28 August 2008) and the associated ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP) for Arab States held in Doha, Qatar (18-21 February 2008). He continued by explaining how the outcomes of the event related to the activities that are being implemented under the global umbrella of the ITU Global Cybersecurity Agenda (GCA). ITU was entrusted by world leaders at

[3] Transcript not available.

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

[5] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/itu-opening-remarks-june-09.pdf

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 and as a response to this developed the GCA. He noted further that ITU launched the Global Cybersecurity Agenda in 2007 as a mechanism and framework for international cooperation and response. As such, the GCA focuses on fostering synergies and building partnerships and collaboration between all relevant parties in the fight against cyber-threats within five main work areas, which are the following: 1. Legal Measures; 2. Technical and Procedural Measures; 3. Organizational Structures, and cross-cutting 4. Capacity Building and 5. International Cooperation. Mr. Ameziane further encouraged the forum participants to engage in rich dialogue and debate during the two days of the event and to come up with a concrete work plan for building cybersecurity capacity in Africa and the Arab States.

Session 1: Towards an Integrated Approach for Cybersecurity and Critical Information Infrastructure Protection

9. Confidence and security in using information and communication technologies are vital for building an inclusive, secure and global Information Society. The continuing changes in the use of ICTs, systems and networks offer significant advantages but also require a much greater emphasis on cybersecurity and critical information infrastructure protection by governments, businesses, other organizations and individual users, who develop, own, provide, manage service and use these networks. Given the interconnected features of ICTs, genuine cybersecurity can only be promoted when all connected stakeholders are aware of the existing dangers and threats and how they can protect themselves online. Government must play a leading role in bringing about a culture of cybersecurity and in supporting the efforts of other participants in this regard. In addition, regional and international cooperation is critical in fostering a global culture of cybersecurity.

10. The first forum session, chaired by Mongi Hamdi, Head of Science, Technology and ICT Branch, (UNCTAD)/(CNUCED), and Head of the Secretariat of the United Nations Commission on Science and Technology for Development, shared an overview of the current cyber-threat landscape and provided an insight into the challenges faced by countries, businesses and citizens in managing their every-day lives in this new and constantly changing environment. Mr. Hamdi noted that the purpose of this event is to help countries better understand the different responsibilities that all stakeholders have when it comes to information security, and to assist countries in developing national approaches for cybersecurity. Cybersecurity issues are critical to all stakeholders and with approximately 1.4 billion internet users worldwide, as users continue to increase, so does also the need to ensure cybersecurity. Mr. Hamdi emphasized the role governments play in taking the lead in fostering a culture of cybersecurity as mentioned in UN Resolutions 57/239 (2002)[6] and 58/199 (2004)[7] on the creation of a global culture of cybersecurity and the protection of critical information infrastructures. He noted the urgency in taking action on cybersecurity as users will not make the full use of the internet unless it is secure.

11. Mohd Shamir Hashim, Head, Strategic Policy and Cyber Media Research Department, CyberSecurity Malaysia, Malaysia, and Representative for the Organisation of The Islamic Conference-Computer Emergency Response Team (OIC-CERT), shared in his presentation an overview of "Malaysia's National Cybersecurity Policy"[8]. Mr. Hashim noted, as like many other countries, Malaysia is plagued by all kinds of online threats, and it was in recognition of the increase in these cyber-threats that the Malaysian Ministry of Science, Technology and Innovation Malaysia in 2005 conducted a study on the development of a National Cyber Security Policy (NCSP). The vision of the policy is to ensure that "Malaysia's Critical National Information Infrastructure shall be secure, resilient and self-reliant. Infused with a culture of security, it will promote stability, social well being and wealth creation". This outcome of the NCSP study was accepted for implementation by the government in May 2006. Overall the objective of the policy is to increase the resiliency of the Critical National Information Infrastructure (CNII) in Malaysia which is defined as assets (real and virtual), systems and functions that are vital to the nation that their incapacity or destruction would have a devastating impact on national defense and security, national economic strength, national image, government's ability to function, and public health and safety. Mr. Hashim provided an overview of the cybersecurity policy and the eight different thrusts that make up the policy, and said that all the thrusts have expected outcomes. He further noted that the policy has identified 10 sectors that constitute the Malaysian CNII: national defense & security, banking & finance, information & communication, energy, transportation, water, health services, government, emergency services and food & agriculture.

12. The policy recognizes the critical and highly interdependent nature of the CNII and aims to develop and establish a comprehensive program and a series of frameworks that will ensure the effectiveness of cybersecurity controls over vital assets. Implementing the policy, Mr. Hashim continued, will enable Malaysia to take a proactive position in handling local and global cybersecurity issues. Successfully implemented, Malaysia's CNII will be better placed to meet the challenges and opportunities that technological advancement brings and this will help to achieve the objectives of Vision 2020 and beyond. In the areas that relate to international

[6] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf

[7] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf

[8] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/hashim-cybersecurity-malaysia-june-09.pdf

cooperation, CyberSecurity Malaysia participates actively. One example of this is the creation of the Organisation of The Islamic Conference-Computer Emergency Response Team (OIC-CERT) together with ANSI and the Tunisian CERT-TCC. The first OIC-CERT seminar was held early in 2009 with Tunisia serving as the Secretariat and CyberSecurity Malaysia as its Chair. Mr. Hashim invited all OIC countries to be part of OIC-CERT, which is an organization that encourages and supports the collaboration and cooperation between CERTs amongst OIC member countries.

13. Ian Cook, Security Evangelist, Team Cymru Research, in his presentation "Expect the Unexpected — The Security Implications of Increased Bandwidth"[9] shared an insight into what Team Cymru, a specialized Internet security research firm, is seeing from their situation on the internet when conducting research into the 'who' and 'why' of malicious Internet activity worldwide. Team Cymru, Mr. Cook said, is concentrating their activity mainly on who are conducting the crime and why they are doing it, and it is for this reason they are monitoring the internet. Mr. Cook discussed how the undersea cables that connect the African continent and the Arab States to the rest of the world, and the increased bandwidth that the new African under seas cable will bring, will impact people in the region also when it comes to the probable increase in malicious activity. Using statistics from other parts of the world he tried to show what happens in terms of cyber threats and related activities when people and countries get connected and go online. Mr. Cook also shared details with the meeting participants on how computers and devices are recruited into botnets. He concluded his presentation with some tips on things that can be done to deal with a possible surge in cyber-threats when the bandwidth increases in the region. This included the urgent need to: block botnets (feeds can be subscribed to, to assist with this), block access to infected web servers; monitor malicious internet activity in each country; set up a national computer security incident response team (CSIRT)/Computer incident response team (CIRT); provide training in incident response as well as training for law enforcement and Internet Service Providers (ISPs) and awareness raising for the general public.

14. Salma Abbasi, Chairperson, The e-Worldwide Group, followed with a presentation on "How to Address the Challenges from Living in the information Society for the Young and Vulnerable"[10], highlighting also the ongoing activities as part of ITU's Child Online Protection initiative which she is closely involved in. As technology is being used at every level in our societies, by all age groups, there is a growing challenge with regards to protecting vulnerable users from the dangers and negative effects of technology in cyber space, specifically children and young people. Ms. Abbasi further pointed out that the Middle East and Africa constitute the fastest growing regions when it comes to internet usage. With this, the dangers online that countries in the West are already experiencing will also be entering these countries. While for instance Arabic only makes up about 3.7 per cent of internet content, this is also likely to increase in the coming years as countries are encouraging more localized content for their citizens. Ms. Abbasi went into some of the specific challenges, risks and dangers that are arising from the expansion and penetration of technology in all walks of life.

15. Pedophiles, embarrassing photos, harassment and bullying online, self-harm consisting of children cutting themselves with blades and sharing this online, just to name some of the actors connected and activities taking place online. Children being innocent and curious, she noted, are the most likely to be attacked and exploited by cyber criminals which may cause great damage not only to the child but subsequently to the family, community and the country. In this regard Ms. Abbasi presented a strategy for mitigation and prevention for addressing the challenges, dangers and threats from cyber space. In order to effectively address this challenge, she emphasized the need for a multi-stakeholder approach that takes into consideration multi-sector partnerships at local, national, regional and international levels. "If we use the system in place properly and further develop the contact network for dealing with cases and for providing education to youngsters, we will already be better off", she said. Ms. Abbasi mentioned the guidelines that ITU is developing as part of a global effort to protect children and young people in cyberspace[11]. The guidelines were issued in draft form on the occasion of World Telecommunication and Information Society Day 2009, celebrated under the theme "Protecting children in cyberspace". The draft guidelines address some of the main issues, along with advice on how policy-makers might tackle the origins of abuse and how industry might help prevent its transmission. Threats to children and young people's well-being are a challenge that must be addressed by all stakeholders, including by the children themselves. The aim is to produce finalized guidelines before the end of 2009 under the Child Online Protection (COP) initiative.

16. Moving forward, Ms Abbasi encouraged countries not to only think about policing and enforcement, but instead to include and involve all different stakeholder groups in the country, start assessing where you are today, look into partnership opportunities, pull together existing content and material and leverage of this and develop an implementation road map. ITU and IMPACT are creating a network to make it easier to work together, she said, but we all have to start now, it is never too late. There is already content available in different languages and countries can start working on awareness raising campaigns, dedicated training sessions, the sharing experiences, tips and tricks, etc.

[9] No slides available.

[10] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/abbasi-child-online-protection-june-09.pdf

[11] http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/index.html

Session 2: Mapping the Global Issue with National and Regional Needs

17. ITU, through its Global Cybersecurity Agenda (GCA), has put in place a framework for international cooperation in cybersecurity, to provide a global platform where all relevant stakeholders can discuss and work together in order to best respond in a coordinated manner to the growing cybersecurity challenges. Each country and region, however, has its own requirements and needs that should be addressed taking in consideration the national and regional context. ITU is working with Members States to ensure that specific requirements are taken into account in order to properly assist. Session 2, moderated by Marco Obiso, Advisor, ICT Applications and Cybersecurity Division, ITU Development Sector (ITU-D), explored how a top-down and bottom-up approach can work to harmonize the overall efforts in order to provide an integrated and consistent response and assistance to Member States.

18. Mr. Obiso in his presentation provided an overview of "ITU-D Activities in the Area of Cybersecurity and Critical Information Infrastructure Protection (CIIP)"[12]. He started by sharing 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 Telecommunication 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 response to addressing the challenges involved in WSIS Action Line C5 and building confidence and security in the use of ICTs, is the Global Cybersecurity Agenda (GCA) which 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 the implementation of the GCA recommendations.

19. Mr. Obiso went on to share details on the ITU-D Cybersecurity Work Programme to Assist Developing Countries (2007-2009)[13], with specific examples of the work that ITU is undertaking to help developing countries. Through these activities ITU-D is assisting countries in building their institutional and human cybersecurity capabilities in a number of different ways. Overall, the ITU Global Cybersecurity Agenda provides the framework for international cooperation in cybersecurity, including for the identification of key strategies to coordinate the international response to the growing challenges of cybersecurity and to enhance confidence and security in the Information Society. Together with partners from the public and private sectors, ITU-D has developed cybersecurity tools to assist developing countries raise awareness and conduct national cybersecurity self-assessments, provide training and build capacity, and how to expand watch, warning and incident response capabilities.

20. These tools include ITU's new Cybercrime Legislation Resources[14] aimed at assisting countries to understanding the legal aspects of cybersecurity and harmonizing legal frameworks, namely the ITU Toolkit for Cybercrime Legislation[15] which provides countries with sample legislative language and reference material that can assist in the establishment of harmonized cybercrime laws and procedural rules. As well as an ITU publication named "Understanding Cybercrime: A Guide for Developing Countries"[16] as a resource to help developing countries better understand the national and international implications of growing cyber-threats, assess the requirements against the existing legal instruments, and assist countries in establishing a sound legal foundation. Furthermore, the ITU National Cybersecurity/CIIP Self-Assessment Tool[17] is an initiative to assist ITU Member States who wish to elaborate on their national approach for cybersecurity and critical information infrastructure protection (CIIP). He also mentioned the ITU Botnet Mitigation Toolkit[18]; cybersecurity guideline publications 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. ITU is currently working on making these resources, related training material and other products and services that are being provided through the ITU-IMPACT collaboration available to Member States.

21. Benoit Morel, Professor, Engineering and Public Policy, Carnegie Mellon University, United States of America, in his presentation discussed "The Challenge of Building Cybersecurity Capability in Developing Countries Today"[19]. Mr. Morel noted the complex nature of cyber-threats, the different dimensions of cybersecurity (legal, technical, etc.) and the varying skills and competencies that are required to deal with these on the national level. Given these human, institutional, and financial resources that are required to build national cybersecurity capacity what can be done to assist developing countries in this regard, he asked. Mr. Morel noted that while the

[12] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/obiso-overview-itu-activities-june-09.pdf

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

[14] http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

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

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

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

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

[19] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/morel-capacity-building-june-09.pdf

United States and advanced Western countries may not be good examples, Tunisia and what the country has done in terms of establishing a national computer emergency response team, the Tunisian CERT/TCC and the National Agency for Computer Security (NACS/ANSI) provide an interesting example for developing countries looking to establish its national watch, warning and incident response capabilities. More generally Mr. Morel discussed some of the recent forms of cyber-attacks like the Conficker, noting that the art of conducting cyber-attack is advancing faster than our ability to respond. He also discussed the reasons behind why these examples should encourage countries to cooperate more effectively and efficiently across borders. One purpose of international cooperation is to make cyberspace a place where it is difficult for attackers to hide, he said. Accomplishing this is still far away. Improving cybersecurity in developing countries is not a simple task but nonetheless of critical importance for global cybersecurity. The longer we leave large parts of the global infrastructure unchecked and neglected, the more difficult it will be to correct the related problems afterwards. Capacity building, education and training constitute important elements. The situation is acute worldwide as there is a global need for many more cybersecurity experts than exist today, and developing countries are faced with particularly difficulties in this regard.

22. Abraham Djekou, Technical Advisor, Agence des Télécommunications, Côte d'Ivoire followed with a presentation on "Experiences and Lessons Learned at a Recent Regional Cybersecurity Event in Côte d'Ivoire: An Overview of Country Needs in The Region"[20] that had been prepared together with Didier Kla, Engineer, Côte d'Ivoire Telecom, Côte d'Ivoire. Mr. Djekou said that when it comes to the uptake and use of ICTs in Côte d'Ivoire, as a developing country with over 20 million inhabitants, one can clearly notice that increasing amounts of activities are become dependent on ICTs. The role of the Internet is growing in importance and criminal activities are growing proportionally. The country is currently in the process of developing the different components that would make up the national cybersecurity strategy. A first step was taken when organizing a national cybersecurity forum in June 2008 to raise awareness on matters that relate to cybersecurity amongst the different national stakeholders (government agencies, private sector, civil society and academia). The main result of the forum was the establishment of a working group with representatives from the public and private sectors, and civil society under the auspices of Agence des Telecommunications de Côte d'Ivoire (ATCI). Mr. Djekou said that the group had been tasked to: propose legislation for cybersecurity; identify and define the institutional, judicial and legal structures needed for cybersecurity (including for the establishment of a national security agency, a national CERT, a national certification agency, etc.); as well as put together a proposal for Côte d'Ivoire's contribution to international cooperation in the cybersecurity.

23. With this mandate in mind, Mr. Djekou shared information on some of the activities related to cybersecurity that have been implemented to date and also provided an insight into some that are being planned. A draft cybercrime law has for example been submitted to the government for approval, a formal framework for collaboration between the entities involved in cybersecurity is being established, the identification of mobile subscribers will be put in place starting 1 July 2009 while owners of cybercafés are already required to ask their clients for identification, and an assistance agreement is in the process of being signed between Tunisia's ANSI and Côte d'Ivoire's ATCI to establish a national CERT. Mr. Djekou also mentioned some of the related outcomes of a cybersecurity event which was held in the country in November 2008. As a result of this meeting, the African countries present had agreed to four priority activity areas: the need to develop human capabilities through enhanced education and training; the creation of an enabling environment (including legal, regulatory, policy, and advocacy aspects); the development of awareness (building confidence, security and guidance with regards to cyberspace); and the global aspects of cybersecurity (as this pertains to information sharing and regional and international cooperation initiatives). The countries involved are now working on the implementation of these actions on the national level.

Session 3: Cybersecurity in the National Agenda and Actions to be Considered in Developing a National Cybersecurity Strategy

24. The need to build confidence and security in the use of ICTs, promote cybersecurity and protect critical infrastructures at the national level is generally acknowledged. As national public and private sector actors bring their own perspective to the relevant importance of issues, in order to have a consistent approach, some countries have established cybersecurity/CIIP institutional framework structures while others have used a light-weight and non-institutional approach. What issues should be considered in a national strategy for cybersecurity and critical information infrastructure protection? Which actors should be involved? As such, the session looked at some of the elements required to develop and organize national cybersecurity/CIIP efforts. Belhassen Zouari, Chief Executive Officer, National Agency for Computer Security and CERT-TCC, Tunisia acted as the moderator for Session 3.

25. The first presentation in Session 3 was provided by Taieb Debbagh, Secretary-General, Department of Post, Telecommunications and New Technologies/ Département de la Poste, des Télécommunications et des Technologies de l'Information (DEPTTI), Morocco. In his presentation on "National Cybersecurity Management System: Framework, Maturity Model and Implementation Guide"[21] he shared some of his experiences as a former

[20] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/kla-cote-divoire-overview-june-09.pdf

[21] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/debbagh-morocco-cybersecurity-june-09.pdf

ITU high level expert group (HLEG)[22] member and leader of GCA Work Area 3 dedicated to organizational structures. The framework for a National Cybersecurity Management System (NCSecMS) that he proposed is built around four main components, namely a National Cybersecurity (NCSec) Framework; a Maturity Model; Roles and Responsibilities; and Implementation Guide. In developing the NCSecMS Mr. Debbagh and his team have taken into consideration existing standards and material, including ITU documents, OECD material, ISO 27001, 27002, 27003, COBIT v 4.1, RACI roles and responsibilities chart, etc. For example, the NCSec Framework consist of five main domains: 1) Strategy and Policies (SP); 2) Implementation and Organisation (IO); 3) Awareness and Communication (AC); 4) Compliance and Coordination (CC); 5) Evaluation and Monitoring (EM). He further highlighted the need for information, resources and people/stakeholder awareness to implement the framework. For each of the processes identified 17 different stakeholders groups have been named and for each of the processes there is also a level of maturity which builds on the existing COBOLT 4.1 framework.

26. Cooperation and collaboration is an important component of the framework, he continued, and 6 processes in the framework relate to this. Once the system has been put in place in a country, the nation can use the framework as a means to conduct a self-assessment of the national and regional cybersecurity readiness. He said that the team has closely studied the existing ITU National Cybersecurity/CIIP Self-Assessment Tool[23] in this regard. Mr. Debbagh also shared details on how this approach has been linked to the building of cybersecurity capacity in Morocco. The national policy thus focuses on building information systems security, fighting cybercriminality, and developing trust in the digital economy (public and enterprise). Mr. Debbagh mentioned that the Morocco CERT will be launched later in 2009.

27. Mohammed Umar Maska, Director of Cybersecurity, Office of the National Security Adviser, Directorate of Cybersecurity, in his presentation "Building National Cybersecurity Capacity in Nigeria: The Journey So Far"[24], provided an overview of what is happening in Nigeria in the area of cybersecurity. He noted that cybersecurity issues are affecting many individuals and companies in Nigeria through website cloning, phishing scams, e-commerce fraud, credit card fraud, advance fee fraud (=the 419 scams), etc. Due to this, in 2003 the President of Nigeria established a Committee to investigate the activities of fraudsters in cyberspace as well as the Economic and Financial Crimes Commission (EFCC) to tackle corruption, advance fee fraud and money laundering. With this strong support from the highest level of government, the National Cybersecurity Initiative (NCI) was developed. Mr. Maska elaborated on the six main objectives of the NCI which include; raising awareness; establishing new legislation to combat cybercrime; providing a legal and technical framework for cybersecurity and CIIP; creating a platform for national public-private stakeholder collaboration; developing extended training across national law enforcement agencies; and building law enforcement cooperation with agencies worldwide.

28. In 2004 the Government set up the Nigeria Cybercrime Working Group (NCWG) to realize the objectives of NCI and subsequently in 2006 the Directorate of Cybersecurity, under the Office of the National Security Adviser, was created. One of the activities of the Directorate is the establishment for a CERT for which the team is now in the process of developing a possible framework. Mr. Maska also pointed out that the Directorate is still sponsoring the computer security and critical information infrastructure protection act and waiting for this to go through the National Assembly. Main challenges going forward, he said, also includes the acquiring the necessary modern technology and tools to help prevent, monitor and investigate constantly changing cyber-threats and criminal activities online. The need for dedicated training for all the different national stakeholders involved was brought up as an important component in successfully implementing the activities under the National Cybersecurity Initiative.

29. Sherif Hashem, Executive Vice President, Information Technology Industry Development Agency (ITIDA), Egypt, in his presentation titled "Towards an Egyptian Framework for CyberSecurity"[25] discussed some of the main aspects of Egypt's approach for dealing with cyber-threats. Mr. Hashem noted that with more than 14 million internet users, Egypt has a lot of economic reasons for further developing its infrastructure. Egypt is now also seeing an increase in the amount of applications that are being developed and used and while raising awareness of online theats is critical, it is equally important to ensure that users are not scared off from using the internet. Mr. Hashem brought to the participants' attention to the fact that even systems that are not connected to the internet can be compromised with usb keys and other devices. He also discussed digital identity and privacy and why this is important when discussing cybersecurity related measures and the need to consider also the costs related to the implementation of different solutions. With regards to ICT-related laws and regulations, Egypt currently has a comprehensive Intellectual Property Rights Law and (Law No. 82/2002), Communications Act (Law No. 10/2003), and E-Signatures Law (Law No. 15/2004). As well as drafts available for a Data Protection, Privacy, and Cybersecurity Law, a Cybercrime Law, and Access to Information Law. In this regard Mr. Hashem recommended that all stakeholder groups be involved when developing new cybersecurity and cybercrime legislation.

[22] http://www.itu.int/cybersecurity/gca/hleg/

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

[24] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/maska-nigeria-cybersecurity-june-09.pdf

[25] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/hashem-cybersecurity-framework-egypt-june-09.pdf

30. Given the high priority given to cybersecurity, Egypt has included cybersecurity in the National Security Council and has in 2007 established a Cybersecurity Committee at the Ministry of Communication and Information Technology (MCIT). In April 2009 a computer emergency response team with national responsibility was launched in Egypt. Established initially to take care of assessment and penetration testing for national critical information infrastructure networks, incident handling, providing an awareness and security alerts portal, other responsibilities will also include international coordination across the activities as well as capacity building and training.

Session 4: Concrete Actions to Foster Regional and International Cooperation

31. Regional and international cooperation is key in fostering cybersecurity 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 on how to best respond in a coordinated manner to the growing cybersecurity challenges. The session reviewed some of the ongoing regional initiatives to further the discussions, in order to identify possible next steps and concrete actions to foster and promote regional and international cooperation for enhanced cybersecurity.

32. Ali Drissa Badiel, Senior Advisor/Head a.i. of ITU Area Office for Central Africa opened the session with an overview of ITU's activities in the region when it comes to cybersecurity and regional cooperation activities for a safer cyberspace for all. He noted that through the Global Cybersecurity Agenda (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. Some ITU activities for strengthening regional cooperation in the field of cybersecurity include assistance to countries such as Cameroon, Côte d'Ivoire, Senegal, Zambia and Burkina Faso for the implementation of network security solutions based on the use of public key infrastructure (PKI). The organization of regional forums, seminars and workshops to build cybersecurity capacity and bring together the different regional and national stakeholders is also an important component of ITU's work. Assistance is also being provided to individual countries for the establishment of national CERTs/CSIRTs/CIRTs.

33. Under ITU-European Union project for the Harmonization of ICT Policies in Sub Saharan Africa (HIPSSA), countries in the region are working towards the overall harmonization of regional regulations, telecommunications and ICTs through, among other things, the provision of assistance to countries in Sub Saharan Africa for the implementation of regional guidelines in their national legislation. Mr. Badiel further highlighted the importance of active participation of all administrations in the Regional Preparatory Meetings to be held in Uganda in July 2009 and in Syria in January 2010. These preparatory meetings provide an excellent opportunity for defining the needs of the countries at the regional level, also in field of cybersecurity.

34. Ali Yahyaoui, Chief ICT Officer, OINF Department, African Development Bank (AfDB)/Banque Africaine de Développement (BAD) in his presentation "The African Development Bank Group's ICT Operations Strategy"[26], continued with an overview of what can the African Development Bank can do to help countries with regards to cybersecurity and other aspects of ICT deployment. As a leader in the region in infrastructure development, the AfDB aims to promote access to ICTs by building national and regional infrastructure and addressing the underlying policy and regulatory environment, and promoting private sector participation through partnerships, with the goal of overall supporting countries in applying ICTs as instrument of development. AfDB does not have a specific programme to support cybersecurity, but instead it has resources available to assist all countries in deploying safe ICTs while building infrastructures and creating a favorable environment for the development of ICTs.

35. Mr. Yahyaoui noted that Africa is still behind with regards to access and usage of ICTs and while there are sub marine cables drawn around the continent there is almost nothing inside. There are also many things to improve for the policy and regulatory side of ICTs, which goes beyond solely laying down the fiber optic cables. Cybersecurity, he said, is yet another dimension in this equation. While most African countries now have some kind of e-strategy in place, all countries are not yet included, and for those that have developed a national e-strategy cybersecurity is unfortunately most often not one of the main priorities. Mr. Yahyaoui also noted that many countries still also lack a dedicated telecom regulatory agency. Many countries on the continent are also at war and not stable. Concrete ways in which the AfDB can assist Member States include throughout the funding of studies to better understand specific national circumstances and AfDB can also consider financing detailed pre-investment studies of infrastructure deployment, the establishment of regional ICT centers of excellence, ICT capacity building more generally, etc. Mr. Yahyaoui ended his presentation with an overview of the methodology used by the bank to provide loans to countries and how AfDB works with countries in getting access to these potential sources of funding.

[26] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/yahiaoui-afdb-strategy-june-09.pdf

36. Mohamed Timoulali, Regional Advisor on ICT Policy, Office for North Africa, United Nations Economic Commission for Africa (UNECA), in his presentation "ECA Cooperative Actions on Cybersecurity"[27] discussed what UNECA is doing the area of cybersecurity. ECA, in collaboration with other stakeholders, is working on a number of activities to follow up on the implementation of WSIS action line C5 dedicated to building confidence and security in the use of ICTs. In this regard, Mr. Timoulali said, ECA is working with countries to develop and formulate national and regional ICT policies and strategies and providing assistance on developing supporting legislation. While several countries have put in place some mechanisms for building confidence, trust and security through the e-strategy development process and national guidelines and directives, very few countries have cybersecurity laws in place. Mr. Timoulali noted that the C5 implementation requires a lot of resources in the countries, not only related to the development of the national strategies but increasingly in the implementation of these strategies. A strategy is only as good as the implementation that follows, he emphasized.

37. In developing a harmonized legal framework, ECA has provided assistance to ECOWAS on the formulation of an ICT harmonized legal framework and assistance has been requested from other Regional Economic Commissions (REC) on adapting the framework. There is also ongoing cooperation with the African Union (AU) for a harmonized regional legal framework for the knowledge society, including guidelines on cybercrime, personal data protection, electronic transactions, e-signatures and certification, and cybersecurity overall. With regards to cybersecurity cooperation, ECA has assisted countries (Kenya, Mozambique, Burkina Faso, Ghana) in the formulation of national cybersecurity policies as well as initiated a project for cooperation on cybersecurity in the Maghreb region. Mr. Timoulali said that ECA wants to continue working with partners in providing technical assistance to regional organizations on implementing harmonized ICT policies, and asked for closer collaboration with ITU and other actors on specific activities that relate to cybersecurity.

38. During the evening of the first day of the forum the participants were invited by ANSI to a cocktail at the meeting venue. In addition, all the country delegates present at the event were invited to visit the Tunisian CERT (CERT-TCC). This much appreciated tour of CERT-TCC was hosted by the ANSI/NACS's and CERT-TCC, Chief Executive Officer Belhassen Zouari and his team.

Session 5: Developing a Legal Foundation and Establishing Effective Enforcement

39. Appropriate national 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 laws, 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, taking into consideration existing international frameworks and recommendations. Session 5 looked closer at the need for a sound legal foundation and effective enforcement, reviewed some of the national legal approaches taken and explored potential areas for international legal coordination efforts. The session was moderated by Nébila Mezghani, Professor, Faculty of Political Sciences, University of Tunis, Tunisia who introduced the speakers in the session, and highlighted the need to update existing laws and when required create new legislation to deal with the growing problem related to the misuse of ICTs.

40. Marco Gercke, Lecturer, University of Cologne, Germany, presented an overview of the newly released ITU publication on "Understanding Cybercrime: A Guide for Developing Countries"[28,29]. This Guide aims to help developing countries better understand the national and international implications of growing cyber-threats, assess requirements of existing national, regional and international instruments, and assist countries in establishing a sound legal foundation. Mr. Gercke also highlighted what is currently happening in the international community and with regards to countries' efforts in revising existing laws and developing new legislation to criminalize the misuse of ICTs. He 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 said that a legal foundation provides the framework to investigate, prosecute and deter cybercrime, promote cybersecurity, as well as encourage commerce.

41. While elaborating on national, regional and international cybercrime legislation, Mr. Gercke emphasized the importance of, and the need for, further harmonization of legislation. He noted that there are a number of international initiatives for cybersecurity and the fight against cybercrime, and that all these different

[27] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/timoulali-eca-cooperative-actions-june-09.pdf

[28] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/gercke-undertstanding-cybercrime-june-09.pdf

[29] The ITU Publication on Understanding Cybercrime – A Guide for Developing Countries was released in May 2009 as part of ITU's dedicated cybercrime legislation resources. The Guide is available for FREE DOWNLOAD at: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html

initiatives have a role to play. 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. The adoption by all countries of appropriate legislation against the misuse of ICTs for criminal or other purposes, including activities intended to affect the integrity of national critical information infrastructures, is central to achieving global cybersecurity. The purpose of ITU's dedicated cybercrime legislation resources[30], the Understanding Cybercrime Guide and the ITU Toolkit for Cybercrime Legislation is to assist countries in understanding the legal aspects of cybersecurity and to harmonize legal frameworks in order to combat cybercrime and facilitate international cooperation.

42. Mwende Njiraini, Engineer, New Technologies, Communications Commission of Kenya, Kenya followed with a presentation on "Developing a Legal Foundation and Establishing Effective Enforcement: Kenya Case Study"[31], discussing how Kenya is developing its legal foundation and related mechanisms for enforcing the provisions of the 2009 Kenya Communications Amendment Act. She shared some background information on the reasons for the revised Act, some of the challenges associated with ICT in national development and the specific policy objectives that Kenya is trying to address with the Act. Ms. Njiraini further noted that due to the increase in international connectivity that Kenya will be experiencing with the opening of traffic through new undersea cables at the end of June 2009, the country is placing even more emphasis on cybersecurity. The revised Act expands the mandate of the Communications Commission to include also broadcasting regulation, and electronic transactions, and in addition gives formal recognition to Kenya's Internet domain resources and cybercrimes. While countries take different approaches for these topics, Ms. Njiraini noted that these responsibilities will now fall under the Communications Commission.

43. Specifically in the area of cybersecurity, the Act gives mandate to the Commission to promote public confidence as well as the development of a sound national framework and approach for cybersecurity. The Act does not provide a definition of cybercrime, she said, but deals with a number of topics related to this, including: unauthorized access to computer data; unauthorized access to and interception of computer service; unauthorized modification of computer material, among others. She further mentioned that there are currently two important areas that the Act does not cover. These are international cooperation in the fight against cybercrimes for which a Mutual Legal Assistance Bill is scheduled to be enacted in the coming months, and procedures for fast-tracking investigation and prosecution of cyber-offences. Ms. Njiraini also discussed some of the concrete measures that the country is undertaken to implement the Act. Here she mentioned activities that were the executed under the framework of the EARPTO (East Africa Regulatory, Post and Telecommunications Organization) Cybersecurity Taskforce which included a plan to establish national CERTs in the countries in question (Kenya, Uganda, Tanzania, Burundi, Rwanda) and a possible regional CERT by 2011.

44. David Weitzel, Lead InfoSec & Privacy Engineer, MITRE, United States of America and Vice Chair, American Bar Association (ABA) Privacy & Computer Crime Committee presented on the "ITU Toolkit for Cybercrime Legislation"[32,33]. The Toolkit aims to provide countries with sample legislative language and reference material that can assist in the establishment of harmonized cybercrime laws and procedural rules. The Toolkit is a practical instrument that countries can use for the elaboration of a cybersecurity legal framework and related laws. The sample language provided in the Toolkit was developed after an analysis of the most relevant regional and international legal frameworks currently available, he continued. The Toolkit language is consistent with these laws and is intended to serve as a guide for countries desiring to develop, draft, or modify their own cybercrime laws. Mr. Weitzel noted that the Toolkit is intended to advance the global harmonization of cybercrime laws by serving as a central resource to help legislators, attorneys, government officials, policy experts, and industry representatives around the globe move their countries towards a consistent legal framework that protects against the misuse of ICTs.

45. The Toolkit's sample language may be customized to suit the laws of a particular country. Countries that model their cybercrime laws after the Toolkit's sample language will help advance a harmonized global framework, facilitate international cooperation, resolve jurisdictional and evidentiary issues, and deter cyber criminal behavior. In addition to the sample language, the Toolkit contains three sections of information that serve as practical aids in developing cybercrime legislation: a) Explanatory comments regarding certain provisions or aspects of the sample language; b) a matrix of cybercrime laws that compares the provisions of

[30] More information on ITU's cybercrime legislation resources can be found online at: http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

[31] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/njiraini-kenya-legal-foundation-june-09.pdf

[32] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/weitzel-cybercrime-legislation-toolkit-june-09.pdf

[33] The ITU Toolkit for Cybercrime Legislation was released in May 2009 as part of ITU's dedicated cybercrime legislation resources. The Toolkit is available for FREE DOWNLOAD at: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html

various countries' laws; and, c) a listing of useful reference materials of various works, laws, books, and articles that discuss cybercrime laws and issues. Mr. Weitzel noted that ITU welcomes feedback and comments on the cybercrime legislation resources to allow ITU to ensure that the materials produced are useful to ITU Member States in pursuing important national cybersecurity efforts.

Session 6: Elaborating on Technical Solutions for Resiliency of Information and Communication Networks

46. The expansion and evolution of telecommunications brings new opportunities, as well as new challenges. Convergence and the move towards networks based on internet protocol (IP) or next generation networks (NGNs) are redefining the industry and business strategies. New services and applications, such as voice over internet protocol (VoIP), are disrupting business models and calling regulatory frameworks into question. Faced with this transition, governments, regulators, operators and manufacturers are struggling to anticipate and adapt to tomorrow's emerging issues. The purpose of the session was to help countries better understand how they can mitigate the impact of security threats and ensure that communications over public telecommunication networks remain reliable, secure, interoperable and user-friendly. Session 6, moderated by Ali Drissa Badiel, Senior Advisor/Head a.i. of ITU Area Office for Central Africa, provided an overview of the threats to networks and discussed technical measures and standards that can be adopted to foster improved network resiliency.

47. Mr. Drissa opened the session with an overview of some of the associated activities that have been taking place over the past few years in the region and specific initiatives that ITU has been involved in and supported in different ways. Along with the new opportunities that the development of telecommunications and ICTs offer, they also bring with them new challenges such as the redefinition of industrial strategies and business models, the impact of the convergence of technologies making more room for IP, the growth of VoIP and especially the migration of networks around the world to the IP next generation networks, he said. These changes require governments, regulators, operators and manufacturers to anticipate prepare themselves for the challenges at hand. In this regard a Forum on Telecommunication Regulation on the theme "IP Networks and Their Challenges for African Regulators" was held in Cameroon in 2006, a Regional Development Forum focusing on "Bridging the ICT Standardization Gap in Developing Countries" with sessions on NGN was held in Ghana in 2008, and a Regional Development Forum on "NGN and Broadband Networks, Opportunities and Challenges" was held in Zambia in May 2009.

48. Patrick Mwesigwa, Director, Technology and Licensing, Uganda Communication Commission, Uganda, and also Vice-Chair, ITU-T Study Group 17 dedicated to security provided an "Overview on Work of ITU-T Study Group 17"[34] and gave an insight into some of the ongoing cybersecurity-related activities in Uganda in his presentation "Cybersecurity Legal and Policy Initiatives — Uganda Case"[35]. The ITU's Standardization Sector (ITU-T) works to bring together the private sector and governments to coordinate work and promote the harmonization of security policy and security standards on an international scale. Standards development bodies have a vital role to play in addressing security vulnerabilities in protocols, he said. In addition to many key security Recommendations, ITU has developed an overview of security requirements, security guidelines for protocol authors, security specifications for IP-based systems, guidance on how to identify cyber-threats and countermeasures to mitigate risks. Mr. Mwesigwa mentioned some of the relevant resolutions that guide ITU-T's security work and some of the ongoing initiatives, like the ICT Security Standards Roadmap[36] which aims to promote closer collaboration between international standards bodies. The Roadmap promotes the development of security standards by highlighting existing standards, current work and future standards among key organizations. When discussing the initiatives undertaken by ITU-T Study Group 17, he emphasized the need for close collaboration with other countries in the region and encouraged developing countries to participate in the activities of ITU-T Study Group 17.

49. In describing some of the ongoing activities in Uganda, Mr. Mwesigwa discussed the progress made in the area of cybersecurity legislation. Since 2003 the country's National Task Force, led by the Uganda Law Reform Commission, has been working on drafting cyber laws. The National Task Force includes representatives from different stakeholder groups, including the Ugandan Ministries of Justice, Trade and Industry, Water, Lands & Environment, the Ministry of Finance, the Ministry of Works Housing & Communications, the Ministry of ICT, as well as the Uganda Communications Commission, Uganda Law Society, National Bureau of Standards, Bank of Uganda, Uganda Investment Authority, Makerere University, Uganda Insurance Commission, etc. Three main instruments are currently available in Uganda: the Electronic Transactions Bill (2003), the Computer Misuse Bill (2003), and the Electronic Signatures Bill (2003). The bills have already been approved by Cabinet and currently under consideration by Parliament. They are expected to be approved by Parliament by the end of 2009.

50. Mr. Mwesigwa also shared information on what other countries in the East African region (Burundi, Kenya, Rwanda, Tanzania, and Uganda) 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

[34] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/mwesigwa-itu-sg-17-overview-june-09.pdf

[35] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/mwesigwa-uganda-case-study-june-09.pdf

[36] http://www.itu.int/ITU-T/studygroups/com17/ict/index.html

Electronic Transactions, Electronic Signatures and Authentications, Data Protection and Privacy, Consumer Protection and Computer Crime and Phase 2 dealing with Intellectual Property Rights, Domain Names, Taxation and Freedom of Information. Under this effort a number of regional meetings have been held and 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.

51. Garry Mukelabai, Information Systems Manager, Communications Authority of Zambia, Zambia, presented on some of the "Cybersecurity Efforts in Zambia"[37]. As a result of the ITU Regional Cybersecurity Forum for Eastern and Southern Africa held Lusaka, Zambia in August 2008[38], a National Cybersecurity Working Group was created. The Working Group, which has full support from the government, is made up of 14 members from various organizations with skills in different areas under the auspices of the telecoms regulator the Communications Authority of Zambia (CAZ). Mr. Mukelabai is currently the chairman of this National Cybersecurity Working Group. Capacity building workshops and training sessions for all members of the National Cybersecurity Working Group are now under planning. Awareness programs to date include: a workshop on e-Payment organized together with the Computer Society of Zambia, a workshop on information system auditing organized by KPMG that the Working Group members were invited to participate in, a Cybersecurity Workshop organized together with the e-Brain Forum and the celebration of the World Telecommunication and Information Society Day (WTISD) dedicated to Child Online Protection on 18 May 2009[39] together with CAZ, in addition to various radio and TV discussion and phone-in programs.

52. In the area of building national incident management capability, Zambia is working on establishing a national Computer Emergency Response Team (CERT), as well as sector specific CERTS reporting to the national CERT. The purpose of this national CERT is to establish a central, trusted organization that can coordinate the national response to cybersecurity incidents. The CERT should be equipped to assist with proactive measures to reduce risk, provide watch, warning, information alerts, and resources to analyze, investigate and respond effectively to incidents. In addition, three different bills are currently being considered by the Parliamentary Review Committee. The ICT Bill introduces a new technology neutral licensing regime, repeals the Telecommunications Act and enhances the Radiocommunications Act. The Electronic Communications and Transaction Bill, based on the based on the UNCITRAL model law, repeals and improves the Computer Misuse Act (2004), introduces and regulates cryptography and authentication service providers, and creates an enabling environment for e-Commerce, e-Health, e-Banking, e-Government and other related e-applications, and empowers CAZ to administer the .zm ccTLD. Furthermore, the Postal Services Bill brings regulation in the postal industry, fosters competition in postal and unreserved services and enables the creation of the Postal Bank. As the use of computers and the internet increases, cyber incidents will also continue to increase. In this regard, Mr. Mukelabai noted that countries and nations have a better chance to mitigate the related effects if they create and sustain a coordinated, trustful alliance.

Session 7: Defining Sound Organizational Structures and Developing Incident Management Capabilities

53. A key activity for addressing cybersecurity requires the establishment of watch, warning and incident response capabilities to prepare for, detect, manage, and responding to cyber incidents. Effective incident management requires consideration of funding, human resources, training, technological capability, government and private sector collaboration, 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 take steps toward remediation. In this regard, Session 7 discussed best practices, organizational structures and related standards in the technical, managerial and financial aspects of establishing national, regional and international watch, warning, and incident response capabilities. The session was moderated by Nabil Sahli, Professor, Tunisia.

54. Haythem El Mir, Technical Manager, National Agency for Computer Security (NACS)(ANSI) and Representative from CERT-TCC, Tunisia, presented on "Developing National CSIRT Capabilities – Tunisia Case Study"[40]. In his presentation, Mr. El Mir shared information on the Tunisian experience in establishing a national CERT, focusing on some of the practical and technical aspects of the Tunisian CERT. He noted that all incident management services are offered free of charge to the different stakeholder groups (government, public and private sector users, home users, professionals, banks, etc.) as a public service. In this regard CERT-TCC tries to ensure a national coordinated approach by providing centralized coordination for IT security issues (trusted point of

[37] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/mukelabai-cybersecurity-efforts-zambia-june-09.pdf

[38] See the website for the ITU Regional Cybersecurity Forum for Eastern and Southern Africa held in Lusaka, Zambia (25-28 August 2008) at: www.itu.int/ITU-D/cyb/events/2008/lusaka/

[39] http://www.itu.int/wtisd/index.html

[40] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/elmir-ansi-csirt-june-09.pdf

contact), a centralized and specialized unit for incident response, awareness raising for all categories of users, technology and security watch, cyberspace monitoring and expertise to support and assist to quickly recover from security incidents. Mr. El Mir said that when the Tunisian CERT started its work its main activity was security awareness, and the CERT still sees awareness raising as one of its most important responsibilities. Representing the only FIRST-recognized Computer Emergence Response Team (CERT) on the African continent, the Tunisian CERT-TCC, Mr. El Mir encouraged countries in Africa and the Arab States to establish their national centers for coordinating watch, warning and incident response activities.

55. Mr. El Mir noted that there is still an overall lack of security awareness and understanding of what ICT security is in the region. 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 funds. In this regard CERT-TCC has been linking cybersecurity to some of the main projects and events going on in the country and assisting other countries in the region and beyond with specific capacity building, awareness raising and training initiatives. Some of these include the assistance provided and experiences shared with Rwanda (2007, sharing experiences), Senegal (2008, training), South Africa (2009, ECS-CSIRT), joining UNCTAD's Centers of Excellence (2008, sharing information), establishing OIC-CERT, CERT-AFRICA, etc. Mr. El Mir concluded his presentation by sharing some concrete lessons learned based on what Tunisia has experienced. These included: the need to define a strategy with clear objectives, ensure that the country has the power of law and high level support, ensure the best possible use of limited resources (adopting a low cost approach through the use of open source), set awareness as one of the primary priorities, improve training and education, rely as much as possible on local capabilities, ensure collaboration with national partners (involving all sectors and building public private partnerships), and provide free technical support in order to build incident management capabilities across the different stakeholder groups.

56. Mohamed Shihab, Technical Advisor, IMPACT and Anuj Singh, Director, Global Response Center (GRC), IMPACT continued with a presentation on the "The Global Response Center (GRC)" and assistance for building national watch, warning and incident response capabilities. They shared information on some of the new opportunities offered by the ITU-IMPACT collaboration through the resources of the Global Response Center (GRC) and related capacity building and training. ITU and IMPACT have signed a Memorandum of Understanding in which IMPACT's state-of-the-art global headquarters in Cyberjaya, Malaysia, will effectively become the physical home of the ITU's Global Cybersecurity Agenda. One of the first services to be shared with Member States is the Global Response Center (GRC), which is designed to be the foremost cyber-threat resource center in the world. Working with leading partners including academia and governments, the GRC provides the global community with a real-time aggregated early warning system. This 'Network Early Warning System' (NEWS) can help Member States identify cyber-threats early on and provide critical guidance on what measures to take to mitigate them. Through the GRC members can gain access to specialized tools and systems, including the recently-developed 'Electronically Secure Collaborative Application Platform for Experts' (ESCAPE).

57. ESCAPE is an electronic tool that enables authorized cyber-experts across different countries to pool resources and collaborate with each other remotely within a secure and trusted environment. By pooling resources and expertise from many different countries on short notice, ESCAPE enables individual nations and the global community to respond immediately to cyber-threats, especially during crisis situations. In addition to the GRC offerings, IMPACT offers scholarship grants to eligible developing country Member States for training courses delivered through the SANS Institute. The aim of the training is to build a pool of resources that can later share the knowledge acquired with others to build national capacity and expertise in the field of cybersecurity. Anuj Singh continued with an overview of some of the operational activities required to set up a functional national computer incident response team (CIRT). He briefly discussed the importance of national CIRTs, what different types of CIRTs exist, and what some of the benefits behind establishing a national CIRT are. Given the global threat landscape a national CIRT is a necessity and a concerted effort is required to help countries that do not already have a CIRT to establish one, Mr. Singh said.

58. In order to initiate a creative dialog among countries to drive a comprehensive CIRT offering, IMPACT has studied various successful CIRT models and has distilled a basic set of elements that are required. Based on this, a basic set of required activities are proposed: the initial CIRT structure planning, technical solution sets, manpower planning and capacity building, and a constant cycle of improvement. He highlighted that the IMPACT-ITU collaboration does not want the countries to make the same mistakes that countries have done in the past and have therefore identified four main components proposed for the national CIRT, including 1) a technical solution, 2) organisation structure and manpower planning, 3) policies and procedures, and 4) training for CIRT staff. The CIRT solution will be set up within the GRC and includes a public portal, an incident management portal, advisories, mailing list solutions for different stakeholders, to name just a few of the different components. It is important to note that all the solutions are integrated back into the GRC. Overall when rolling out these IMPACT-ITU services, Phase 1 consists of setting up an infrastructure, taking the feeds, and learning how to deal with the incidents, Phase 2 and Phase 3 involved helping countries set up fully functional CIRTs. The participants were encouraged to contact ITU and IMPACT at cybmail@itu.int for more information.

Session 8: Promoting a Culture of Cybersecurity through Innovative Partnerships

59. The realities of cyberspace make it clear that everyone has to work together. Responding effectively to cyber-threats requires resources, know-how and strong investments on capacity developments, and these efforts cannot be undertaken by only one entity. The key element is bringing the public and the private sectors together in trusted forums and joint activities, to address the common cybersecurity challenges and develop solid capacity building plans. These collaborative efforts should involve every cyber-user; from citizens to corporations, law enforcement, and critical infrastructure providers. The basis of a successful partnership is trust, which is necessary for establishing, developing and maintaining sharing relationships between the different parties. Session 8, moderated by Ahmed Elsheikh, Director, Department of Information and Communication Arab League Educational, Cultural and Scientific Organization (ALECSO), looked closer at the benefits as well as challenges associated with innovative and sustainable partnerships for enhanced cybersecurity, and how joint efforts generate concrete steps forward.

60. Mohamed Shihab, Technical Advisor, IMPACT, to show how innovative partnerships can work in practice when partners contribute with their core competences, provided a general "Overview of IMPACT – The International Multilateral Partnership Against Cyber Threats"[41]. Mr. Shihab noted that the previous presentation showcased a subset of the products and services that IMPACT currently offers while this presentation discussed what IMPACT is and how it is trying to help countries around the world build cybersecurity capacity. Launched in March 2009, IMPACT is an international platform for governments, industry and academia to collaborate in cybersecurity. In this regard IMPACT is a non-profit organization which is international and multilateral in nature. It is also a public-private partnership, with the private sector and academia partnering up to assist member countries to secure their IT infrastructure. Countries interested in joining and benefiting from the services offered through the IMPACT-ITU partnership are advised to contact the ITU Telecommunication Development Bureau at cybmail@itu.int, highlighting the specific area and services that the country is interested in.

61. Angus Goldfinch, Public Safety and National Security Consultant, Intercai Mondiale, in his presentation "Partnerships for Consumer Online Safety for the Internet (COSI)"[42] continued with an overview of what constitutes successful partnership models to improve users' online safety. The basis of a successful partnership is trust, which is necessary for establishing, developing and maintaining sharing relationships between the different parties, he said. Emphasizing the need to leverage of existing partnerships in order not to have to start from scratch every time. As an example Mr. Goldfinch used the Consumer On-line Safety for the Internet (COSI) partnership which requires stakeholders in the public and private sectors to address the challenges against various threats to consumers, including but not limited to: content and child protection; unsolicited commercial messaging (spam); scams (phishing and pharming); illegal downloading of music and film, etc. He further noted that the partnership needs to be clear in its purpose, operations model and its way forward. Having the aims of the association, its obligations under law, obligations under regulations, obligations implied under possible licenses clear when developing the specific principles and executive regulations, reference model, code of practice and overall framework for its operation. The partnership then has to deliver against its aims. Mr. Goldfinch also elaborated on ways to further promote these partnership activities nationally and internationally, engaging with existing activities and organizations.

62. In the last presentation, Naoufel Frikha, Engineer, National Agency for Computer Security (NACS)(ANSI), Tunisia, presented on "Cybersecurity Awareness Raising – The Tunisian Experience/L'Éxpérience Tunisienne en Matière de Sensibilisation dans le Domaine de la Cybersécurité"[43]. Mr. Frikha noted that there is not a lot of knowledge amongst stakeholders and users about the risks that people are exposed to on the internet. As there are both cultural risks and technical risks when it comes to cybersecurity, Mr. Frikha continued, how should countries go about raising awareness amongst the population? When it comes to cybersecurity threats, he said, countries are not solely dealing with a technical problem, above anything else it is a human problem and the individual is the weak link in the equation. First of all, he said, the country needs to define the actor, the entity responsible that will be responsible for managing the programmes and initiatives. Then identify the receivers of the communication and determine what the message should be. It is important to choose the appropriate words and think about how the message will be perceived, for example with regards to pedophilia in Arab and Muslim states. Finally, decide and develop the approach and means of which the message will be shared with the receivers. In doing so, Mr. Frikha said, the main agency behind the campaign needs to make sure that partner organizations, private sector collaborators and specialists in the area are closely involved in the different stages. 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. Frikha noted.

63. Mr. Frikha concluded his presentation with an overview of some of the cybersecurity awareness raising material that has been developed by ANSI and Tunisian partners and shared with different target groups. This included dedicating personnel to prepare material targeted for journalists, radio and television, cartoons for children, a CD-ROM for parental control, creating and distributing IT security awareness raising posters, just to

[41] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/impact-overview-june-09.pdf

[42] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/goldfinch-partnerships-consumer-safety-june-09.pdf

[43] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/frikha-ansi-awareness-june-09.pdf

mention a few examples. He 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. These constituted some interesting examples of material that can be developed by countries in different regions of the world to engage with the users and target groups in innovative ways.

Session 9: Wrap-Up, Recommendations and the Way Forward

64. The final session of the forum was co-facilitated by Belhassen Zouari, Chief Executive Officer, National Agency for Computer Security (ANSI/NACS), Tunisia, Miloud Ameziane, Head, ITU Regional Office for Arab States and Marco Obiso, Advisor, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Bureau (BDT). 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 the protection of critical information infrastructures in Africa and the Arab States.

65. The purpose of the Regional Cybersecurity Forum was to serve as an open platform for interested stakeholders in the Arab States and on the African continent, and it also aimed to follow up on the activities that had been initiated and committed to by countries at last year's ITU Regional Cybersecurity Forum for Eastern and Southern Africa held in Lusaka, Zambia (25-28 August 2008)[44] and the associated ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP) for Arab States held in Doha, Qatar (18-21 February 2008)[45]. These two events had asked for countries in the regions to develop a national cybersecurity strategy, review and revise current cyber-legislation, draft new legislation to criminalize the misuse of ICTs, taking into account the rapidly evolving cybersecurity threats, as well as develop incident management capabilities with national responsibility, or computer incident response teams (CIRTs), and use examples of existing national CIRTs/CSIRTs/CERTs when developing these.

66. At the 2009 ITU Regional Cybersecurity Forum for Africa and Arab States, country representatives focused their discussions and brain-storming around concrete next steps in these three main areas. They identified requirements for specific cybersecurity capacity building and training needs that the countries in the regions have and ways in which to achieve these. Mechanisms to finance such activities were also discussed. Some recommendations for concrete actions that need to be taken by countries in the regions were identified by the participants and speakers, these included the following:

- In the area of **developing a legal framework and establishing effective enforcement,** countries encouraged the involvement of governments in the region in international efforts and in coordination/cooperation with regional and international efforts. They noted that more direct assistance to countries is needed and with the help of existing tools, such as the newly released ITU Toolkit for Cybercrime Legislation, and Understanding Cybercrime Guide, countries in the region are ready to take action in this area. It was decided to feed in contributions on necessary cybersecurity activities from the countries to the ITU Regional Preparatory Meeting for the WTDC for Africa to be held in Uganda in July 2009 and in Syria in January 2010.

- As a result of the meeting and discussions that have been taking place over the past few weeks, countries expressed their need for direct assistance in the **development of watch, warning and incident management capabilities** and for the establishment of the necessary organizational structures with national responsibility, including national computer incident response teams (CIRTs). These national efforts can at the same time initiate cooperative activities at the regional and international levels, with the possible establishment of regional centers. Some countries in the region, namely Burkina Faso, Burundi, Cote D'Ivoire, Egypt, Iraq, Kenya, Mauritius, Morocco, Nigeria, Rwanda, Saudi Arabia, South Africa, Tanzania, Tunisia, Uganda, United Arab Emirates, and Zambia, are now working with ITU, in collaboration with key partners, such as the International Multilateral Partnership Against Cyber Threats (IMPACT), to facilitate the development of cybersecurity capabilities, including the establishment of national CIRTs.

- Furthermore, countries committed to concrete actions to be taken in **developing a national cybersecurity strategy** and ensuring harmonization within the key principles of international cooperation. The development of national strategies with the commitment of key national decision makers facilitate the process towards implementation of the necessary measures, legislation and capabilities required by the countries to respond effectively to cyber-threats. In this regard, countries can make use of the expertise and resources that the ITU and other regional and international organizations as well as private parties can provide, in order to receive the proper assistance for establishing national cybersecurity policies. It was also highlighted that this needs to be done within an established international cooperation framework and building on work already initiated in the countries through regional and international organizations.

[44] See the website for the ITU Regional Cybersecurity Forum for Eastern and Southern Africa held in Lusaka, Zambia (25-28 August 2008) at: www.itu.int/ITU-D/cyb/events/2008/lusaka/

[45] See the website for the ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP) for Arab States held in Doha, Qatar (18-21 February 2008) at: www.itu.int/ITU-D/cyb/events/2008/doha/

- The countries noted the need for **enhanced capacity building** in all cybersecurity-related areas, focusing also on stakeholders with specific needs. Activities need to be initiated that help Member States identify risks to children and young people online and develop their national child online protection (COP) activities.

67. Cybersecurity issues are a complex mix of technological, political, and cultural challenges. Countries in Africa and the Arab States are surely at different stages in their development of effective responses, institutional and human capacity to deal with issues pertaining to cybersecurity, however, clear progress is being made and countries are positive with regards to how their levels of preparedness are evolving and the support they are receiving. The Forum participants shared the understanding that in order to safeguard national cybersecurity a global approach is needed. ITU is working on understanding to specific needs of countries in the region to be able to provide a platform to come to a common understanding on how ITU can, together with partners, address the needs of all countries.

Meeting Closing

68. In closing the event Mr. Zouari shared some closing remarks on behalf of the National Agency for Computer Security, Tunisia, as the host for the ITU Regional Cybersecurity Forum for Africa and Arab.

69. In his closing remarks on behalf of ITU and the Director of the ITU Telecommunication Development Bureau ITU, Miloud Ameziane, Head, ITU Regional Office for Arab States said that he hoped that the two day long had been informative and useful for the participants. Mr. Ameziane thanked everyone who had directly or indirectly contributed to the success of the forum and relayed special thanks to the local hosts, for their outstanding work in making this Regional Cybersecurity Forum possible. He also thanked the forum speakers for taking time to prepare the presentations and share their experiences and expertise with the forum participants. ITU, he said, 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 the different activities, initiatives and events.

The email address for comments on this meeting report[46] is **cybmail(at)itu.int**[47].

For information sharing purposes, all forum participants will be added to the: cybersecurity-arab-states(at)itu.int and cybersecurity-africa(at)itu.int**[48]** mailing lists for matters concerning ITU-D cybersecurity-related activities. If you have not participated directly in the event, or are not already on the mailing lists but interested in participating in these discussions through the relevant mailing list and forum, please send an e-mail to **cybmail(at)itu.int**.

[46] This Forum Report is available online: http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/tunis-cybersecurity-forum-report-june-09.pdf

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

[48] Regional ITU cybersecurity mailing lists: cybersecurity-arab-states@itu.int and cybersecurity-africa@itu.int. Please send an e-mail to cybmail@itu.int, to be added to the mailing lists.