ITU Regional Cybersecurity Forum 2008
Sofia, Bulgaria

Document RFS/2008/01-E
10 October 2008
Original: English

Meeting Report :

ITU Regional Cybersecurity Forum for Europe and CIS held in Sofia, Bulgaria, 7-9 October 2008[1]

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

Purpose of this Report

1. The ITU Regional Cybersecurity Forum for Europe and the Commonwealth of Independent States (CIS) was held in Sofia, Bulgaria from 7 to 9 October 2008. The forum, which was hosted by the State Agency for Information Technology and Communications (SAITC) of the Republic of Bulgaria, aimed to identify some of the main challenges faced by countries in Europe and CIS in developing frameworks for cybersecurity and CIIP, to consider best practices, share information on cybersecurity development activities being undertaken by ITU as well as other entities, and review the role of various actors in promoting a culture of cybersecurity. The forum also considered initiatives on the regional and international level to increase cooperation and coordination amongst the different stakeholders.

2. The forum, 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) and the 2006 World Telecommunication Development Conference Doha Action Plan establishing ITU-D Study Group Question 22/1: *Securing information and communication networks: Best practices for developing a culture of cybersecurity*. Approximately 130 people from 25 countries participated in the event from Europe and CIS, as well as from other parts of the world. 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/2008/sofia/. This meeting report[2] summarizes the discussions throughout the three days of the ITU Regional Cybersecurity Forum for Europe and CIS, provides a high-level overview of the sessions and speaker presentations, and presents some of the common understandings reached at the event. Simultaneous interpretation in Russian and English was provided for the participants throughout the forum.

ITU Regional Cybersecurity Forum for Europe and CIS held in Sofia, Bulgaria, 7-9 October 2008

3. As background information, considering that modern societies have a growing dependency on information and communication technologies (ICTs) that are globally interconnected, countries are increasingly aware that this creates interdependencies and risks that need to be managed at national, regional and international levels. Therefore, enhancing cybersecurity and protecting critical information infrastructures are essential to each nation's security, social and economic well-being. At the national level, this is a shared responsibility requiring coordinated action related to the prevention, preparation, response, and recovery from incidents on the part of government authorities, the private sector and citizens. At the regional and international level, this necessitates cooperation and coordination with relevant partners. The formulation and implementation of a national framework for cybersecurity and critical information infrastructure protection therefore requires a comprehensive, multi-disciplinary and multi-stakeholder approach. The Regional Cybersecurity Forum discussed some of the key elements in developing such policy and regulatory frameworks and proposed some concrete actions that can be taken in implementing these in the region.

---

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

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

Meeting Opening and Welcome

4. The Regional Cybersecurity Forum for Europe and CIS was opened with a welcoming address[3] by Plamen Vatchkov, Chairman, State Agency for Information Technology and Communications (SAITC), Bulgaria. On behalf of SAITC, Mr. Vatchkov welcomed the forum participants to the event and highlighted why this event is an important step towards building cybersecurity capacity in Europe and CIS. Mr. Vatchkov noted that hosting the forum is an expression of the commitment of SAITC to apply more efforts in the field of network and information security. In this regard, he shared some of the agency's activities in the area. Mr. Vatchkov also mentioned SAITC's ongoing involvement in the activities of ENISA, highlighting that as a result of this active cooperation with ENISA and the Hungarian CERT, the establishment of a Government-CERT in Bulgaria is underway. SAITC is taking measures to consolidate its institutional capacity in terms of information security and is also in the process of developing a national cybersecurity strategy, he continued.

5. How best to deal with cybersecurity, Mr. Vatchkov asked. Because most of us spend a lot of time online, and since the online virtual world is a reflection of the real world, just like criminals are an inevitable part of our social structure, not surprisingly, they have also populated the virtual world. However, while initially the results of these cybercrimes were felt mainly within the virtual world, now the victims of cybercrimes are in the real world and they suffer heavy financial losses or lose credibility, he said. The logic is simple, Mr. Vatchkov continued, since there are cybercrimes, fighting these calls for cybersecurity. That is the reason we are here for this Regional Cybersecurity Forum, he said, to find the ways and means to raise the level of cybersecurity.Mr. Vatchkov concluded his 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, and work towards common cybersecurity objectives that will foster an inclusive and secure information society.

6. Sami Al Basheer Al Morshid, Director, Telecommunication Development Bureau, International Telecommunication Union (ITU)[4] followed with some opening remarks[5] on behalf of the ITU. 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 about to reach 4 billion and the mobile penetration rate estimated to reach 61 per cent by the end of this year, Mr. Al Basheer reminded the participants of the key role that ICTs play in people's lives. Access to ICTs has become essential for social and economic development and ICTs have provided solutions to a wide range of everyday problems, sometimes in unexpected ways, Mr. Al Basheer said. However, as new technologies are developed and access to ICTs expands threats to their security are also growing fast. 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, he continued, to safeguard cyberspace 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 said.

7. ITU is paving the way for this global cooperation, Mr. Al Basheer continued. ITU was entrusted by world leaders at the World Summit on the Information Society to take the lead on action line C5, dedicated to building confidence and security in the use of ICTs. ITU, through its three Sectors, is working towards a global, coordinated and harmonized approach to achieving cybersecurity through the ITU Global Cybersecurity Agenda, a mechanism to cooperate internationally, building synergies and coordinating ITU's efforts. As part of these efforts, the ITU Telecommunication Development Bureau is providing expertise through a specific work programme with initiatives and projects designed to respond to the needs of Member States for assuring safer ICTs. This work programme includes the organization of regional forums, such as this one in Bulgaria, to build the necessary capacity for countries to tackle cyberthreats efficiently. Mr. Al Basheer concluded his opening remarks by expressing how happy he was to see all the delegates present at the forum, highlighting that this was a good opportunity to bring together representatives from Europe and CIS, regional and international organizations to exchange experiences and share best practices to assure the security that is needed in cyberspace for everyone to be able to benefit from the information society. With its long scientific tradition, with a political experience established during the various eras of its history, with an extremely rich culture, he continued, Bulgaria has all the ingredients to inspire delegates' work during this forum.

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

8. The necessity of building confidence and security in the use of ICTs, promoting cybersecurity and protecting critical infrastructures at national levels is generally acknowledged. As national public and private actors bring their own perspective to the relevant importance of issues, in order to have a consistent approach, some countries have established institutional frameworks while other countries have used a light-weight, non-

[3] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/saitc-opening-remarks-sofia-oct-08.pdf

[4] http://www.itu.int/ITU-D/dir/

[5] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/itu-opening-remarks-sofia-oct-08.pdf

institutional approach. Many countries have not yet established a national strategy for cybersecurity and CIIP. The first forum session, chaired by Valérie Andrianavaly, Officer, Network and Information Security, DG Information Society and Media, European Commission, introduced the concept of a national framework for cybersecurity and CIIP, discussed what has been done to date in Europe and CIS in this regard, and presented some of the ongoing cybersecurity efforts in the ITU, in order to provide meeting participants with a broad overview of the issues and challenges involved. Ms. Andrianavaly 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.

9. Mark Sunner, Chief Security Analyst, MessageLabs, in his presentation titled "Setting the Stage — The Changing Cybersecurity Threat Environment"[6], shared an observation of what MessageLabs, as a provider of managed IT security services, are seeing in their own situation on the internet. Mr. Sunner mentioned that MessageLabs has a datacenter processing information on the internet and based on the 1.5 billion daily web requests he gave an insight into what they are seeing in this data on a day to day, month to month, year to year basis. Mr. Sunner noted that the threat landscape has evolved dramatically with viruses giving way to targeted trojans and highly socially engineered phishing attacks. The trend shows that while spam as a percentage of all e-mails sent is still high, spam volumes overall have dropped in the past few weeks and the reason for this being that one ISP in the United States that has long been a problem has been shut down. With this he wanted to show that there are ways to take out the command and control and reduce the amount of spam delivered to end users. He further noted that 1 in 131 e-mail messages still contain a virus of some kind and in August 2008, 1 in 288 e-mail messages contained phishing. Towards the end of 2007 the volume of phishing messages passed malware and this data, Mr. Sunner said, can be seen as an indication of where things may be going in the future. By the end of 2008, he continued, the number of viruses will come down, but this will instead mean that bad guys will be using more urls and hyperlinks than executables. Compared with viruses and spam though, botnets are growing at a faster rate.

10. Mr. Sunner showed an indication of what specifically is being seen with regards to botnet activity, and mentioned that the botnet activity in China and India is increasing and that this is linked directly to the rollout of broadband in the region. The change in the middle class in India and China and the rollout of broadband has clear implications for all of us. "History is repeating itself", he said, as there is almost a one to one correlation between broadband connections and spam. This was also noted in the past for Western Europe and the United States and is most likely going to happen in India and China in the coming year. By the midpoint of next year (2009) there will be a lot more broadband access in this region and everyone will be feeling this with increased spam, especially countries like Japan that feel the majority of the spam coming from China, he said. Mr. Sunner also shared information on some specific botnets that make up a large majority of the spam in the world, CAPTCHA, or Completely Automated Public Turing Test to tell Computers and Humans Apart, was also mentioned and discussed. With regards to the observed increase in the frequency of targeted attacks, Mr. Sunner noted that while most mainstream attacks are for anyone and everyone, there were still only 1 or 2 targeted attacks per week in 2005 and now around 80 per day. In June 2008 there were 540 attacks in two hours, all in documents, and all targeted towards job titles, individuals with interesting secrets, CEO's, etc. What is fueling this, he said, is the black economy that is selling DDOS attacks and the like. The barrier to entry is very low in some regions of the world with some "providers" even offering service level agreements, which mirrors very well the real world and the real economy. Tightening of legislation is key, he continued, to avoid safe havens for this type of activity.

11. Alexander Zolotnikov, Chief of Information Security, TransTeleCom, Russian Federation, provided a presentation on "Cybercrime on Global Information Networks. Countering Cyber Terrorism"[7]. TransTeleCom, whose main shareholder is the Russian Railways, operates and maintains the largest fiber-optic network in the Russian Federation with more than 53 000 km of cable laid along the country's railway lines and over 1,000 access nodes in all regions of the country. Given the widespread adoption of information technology in all areas of society, including critical infrastructures that form the basis of all government institutions, be it for finance and banking, transportation, energy, or public security, ensuring information security has become one of the government's main tasks, he said. The protection of critical information infrastructure facilities is a major challenge for both the government and private businesses, who are the owners of these infrastructures on both the national and international level.

12. The problems that exist in the networks, he said, are the company's problems as it is the operator who is directly providing this service to the customer. Hence the role and related responsibilities of the telecom operator in the area of cybersecurity are very important and should not be ignored. In this intervention Mr. Zolotnikov shared some of the specific responsibilities of the operator in creating secure information and telecommunications networks. He emphasized the need for each operator to introduce systems to effectively monitor the networks and actively take measures to counter fraud. He further explained the need for the operator to interact and share experiences with other operators, to regularly interact with law enforcement

[6] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/sunner-threat-overview-sofia-oct-08.pdf

[7] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/zolotnikov-cyberfighting-sofia-oct-08.pdf

agencies and special services, and highlighted the need for operators to actively participate in both national and international forums to discuss and learn what other people are doing in this domain.

13. The session chairperson, Valérie Andrianavaly, Officer, Network and Information Security, DG Information Society and Media, European Commission, provided an insight into "Security and Resilience in the Information Society: Towards a CIIP Policy in the EU"[8]. Ms. Andrianavaly started her presentation by providing an overview of the existing policies and legislation in the European Union and the role of the European Commission in proposing policy and legislation for CIIP. Measures presented included the 2006 Strategy for a Secure Information Society; policy initiatives on the fight against spam, spyware and malware, promoting data protection, and the fight against cybercrime; the proposed package to reform the regulatory framework for e-communications; the establishment of the European Network and Information Security Agency (ENISA); and a policy initiative on CIIP to be adopted in early 2009 under the general framework of the European Programme on Critical Infrastructure Protection. The purpose of the new CIIP policy initiative is to enhance the level of CIIP preparedness and response across the EU and ensure that adequate and consistent levels of preventive, detection, emergency and recovery measures are put in operation. In order to do meet these goals a better understanding of and clarity on the guiding policy principles must be achieved, she said. The approach that will be followed to meet the objectives of the policy include building better on existing national and private sector initiatives, engaging relevant public and private stakeholders, and collaborating closely with regional and international initiatives in the area.

14. Ms. Andrianavaly further stressed the need to bridge the gaps with regards to national CIIP policies across Europe and assist countries that are less developed in this area to bring all countries up to the same level and to reinforce the cooperation and information exchange between countries. The international dimension of CIIP and the need to reinforce cooperation on related global issues such as the security and the robustness of the internet, was also noted as important. Successfully implementing the new policy initiative will be a significant step forward in the realization of the European Commission's strategy for a Secure Information Society, she said. Ms. Andrianavaly concluded her presentation by elaborating on some of the planned next steps for CIIP in the European Union. A number of studies have already been prepared and initiated to work toward the Q1 2009 deadline for the new policy initiative. This includes studies to better understand how dependent the different industry sectors are on ICTs. A study is already underway which will look at the finance, energy and transport sectors and the findings of this study will be released at the end of 2009. A stocktaking exercise to analyze existing initiatives in the region has also been started. Ms. Andrianavaly further highlighted the aim of the European Commission not to duplicate work already done in Member States but instead build synergies and assist those countries that are less developed in this area, to bring everyone to the same level of readiness. The goal is to adopt a detailed action plan for CIIP by Q1 2009.

15. Marco Obiso, Advisor, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Bureau (BDT), in his presentation provided an overview of "ITU-D Activities in the Area of Cybersecurity and Critical Information Infrastructure Protection (CIIP)"[9]. He started by providing an insight into ITU's overall activities in the area of cybersecurity, noting that there are cybersecurity-related activities ongoing in all three ITU Sectors. The 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), a tool that the ITU is using to aggregate and harmonize internal ITU activities on cybersecurity conducted in all three ITU Sectors and to work with the external stakeholders, organizations and experts, ensuring also the implementation of the recommendations that have come out of the GCA.

16. Mr. Obiso went on to share details on the ITU-D Cybersecurity Work Programme to Assist Developing Countries (2007-2009)[10], with specific examples of the work that ITU is undertaking to help developing countries in the domain of cybersecurity and CIIP. Some of the ongoing and planned ITU cybersecurity initiatives mentioned in his presentation included: activities dealing with the identification of best practices in the establishment of a national approach for cybersecurity and CIIP; a national cybersecurity/CIIP readiness self-assessment tool; a botnet mitigation toolkit; cybersecurity guideline publications for developing countries; an international survey of national cybersecurity/CSIRT capabilities; a toolkit for model cybercrime legislation for developing countries; a toolkit for promoting a culture of cybersecurity as well as a number of planned regional events for awareness-raising and capacity building on cybersecurity and CIIP. He further noted that the *Work Programme* describes how ITU in a practical way can and plans to assist countries in developing cybersecurity capacity, through providing Member States with useful resources, reference material, and toolkits on related subjects and implementing a variety of projects in the different countries and regions. As the related toolkits

[8] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/andrianavaly-CIIP-in-EU-sofia-oct-08.pdf

[9] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/obiso-overview-of-activities-sofia-oct-08.pdf

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

and reference material become more stable, the ITU-D is looking to disseminate them widely through multiple channels to ITU's 191 Member States.

17. Joseph Richardson, Consultant, United States of America, followed with his presentation providing a more detailed insight into the "ITU Approach for Organizing National Cybersecurity/CIIP Efforts and the ITU Cybersecurity Self-Assessment Tool"[11]. Mr. Richardson described the approach for organizing national cybersecurity/CIIP efforts, which includes policy statements, identifies goals and specific steps to reach these goals, and references and material related to each specific step. Highlighting that the protection of cyberspace is essential to national security and economic well-being, Mr. Richardson continued by provided some concrete ideas and examples on how countries can get started on developing a national cybersecurity strategy. An important tool in this effort is the ongoing ITU work to develop a comprehensive National Cybersecurity/CIIP Self-Assessment Tool[12]. The tool can assist governments in examining existing national policies, procedures, norms, institutions and other elements necessary for formulating security strategies in an ever-changing ICT environment. It can help governments better understand existing systems, identify gaps that require special attention and prioritize national cybersecurity response efforts.

18. Mr. Richardson highlighted that the tool identifies issues and poses a number of questions that might be worth considering; what actions have been taken to date, what actions are planned, what actions are to be considered, and what is the status of these actions? Mr. Richardson also noted that no country is starting at zero when it comes to initiatives for cybersecurity and there is no one right answer or approach to be taken as all countries have unique national requirements and circumstances. Continual review and revision is also needed of any approach taken, and it is equally important to involve all stakeholders, appropriate to their roles, in developing a national strategy. Countries interested in undertaking a facilitated national cybersecurity/CIIP self-assessment together with the ITU can contact the ITU Telecommunication Development Bureau at cybmail@itu.int.

Session 2: Promoting a Culture of Cybersecurity

19. Trust, 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. Session 2, moderated by Janice Richardson, Representative, European Schoolnet and Coordinator, Safer Internet Initiative, looked closer at the building blocks needed to successfully Promote a Culture of Cybersecurity.

20. Christine Sund, Cybersecurity Coordinator, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Sector (ITU-D), in her presentation on "Promoting a Culture of Cybersecurity – Fundamentals"[13] provided an overview of what a culture of cybersecurity means and some of the possible roles of different stakeholders in the information society in creating a global culture of cybersecurity. She highlighted the nine elements for creating a culture of cybersecurity outlined in UN Resolution 57/239 (2002): "Creation of a global culture of cybersecurity", and UN Resolution 58/199 (2004): "Promotion of a global culture of cybersecurity and protection of critical information infrastructures". These nine elements include: a) awareness, b) responsibility, c) response, d) ethics, e) democracy, f) risk assessment, g) security design and implementation, h) security management, and i) reassessment. Through these Resolutions, UN Member States and relevant international organizations were asked to take action to promote, develop and implement a global culture of cybersecurity in cooperation and further take these elements into account in preparation for the two phases on the World Summit on the Information Society (WSIS)[14] in 2003 and 2005. The outcome documents from the two WSIS phases further emphasized the importance of building confidence and security in the use of ICTs and reaffirmed countries' commitment to promoting a culture of security.

21. Ms. Sund's presentation mentioned some possible roles for governments in promoting a culture of cybersecurity, including: playing a central role in coordinating and implementing a national cybersecurity strategy; ensuring that the national policy is flexible and adaptive; coordinating responsibilities across authorities and government departments; creating new (or adapting existing) legislation to criminalize the misuse of ICTs; protecting consumer rights; ensuring that a nation's citizens are protected; and leading national, regional, and international cybersecurity cooperation activities. With regards to the private sector's involvement

---

[11] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/richardson-overview-of-approach-sofia-oct-08.pdf

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

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

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

in establishing a national approach for cybersecurity, Ms. Sund further noted that as the ICT infrastructures are in many countries owned and operated by the private sector, their involvement in promoting a national and global culture of cybersecurity is critical. Effective cybersecurity measures need an in-depth understanding of all aspects of ICT networks, and the private sector's expertise and involvement is therefore paramount in the development and implementation of national cybersecurity strategies. Furthermore, Ms. Sund highlighted that governments and businesses need to assist citizens in obtaining information on how to protect themselves online. While cybersecurity at its core is a shared responsibility, with the right tools readily accessible, each participant in the information society is responsible for being alert and protecting themselves.

22. Ilari Patrick Lindy, Senior Expert, Relations to Industry and International Organisations, ENISA, provided an overview of ENISA's mission to foster a culture of information security in Europe in his presentation on "Awareness Raising in Promoting a Culture of Cybersecurity: Recent Work by ENISA"[15]. Mr. Lindy focused on some of the work already undertaken and ongoing initiatives in the area of security awareness raising, with awareness raising amongst all stakeholders in the Member States being one of ENISA's main goals in order to enhance security capabilities of EU bodies and Member States. In this regard, Mr. Lindy continued, ENISA aims to be a stimulator, catalyst, promoter, advisor and facilitator when it comes to cybersecurity matters. Awareness raising, and ensuring that the constituents are aware of the risks involved and what tools they can use to safeguard against the threats, is the first line of defense for the security of information systems and networks, he said.

23. ENISA's work in the area of awareness raising involves helping to monitor the progress on the national level, provide an inventory of good practices that have been run or planned in public and private organizations, develop dissemination plans to share these good practices as well as provide material that can be customized to facilitate the different entities' work and awareness raising initiatives. ENISA also contributes to the implementation of an information security culture in Member States by encouraging users to act responsibly and thus operate more securely. Mr. Lindy went further into describing what the Awareness Raising Community initiative was all about. The Awareness Raising Community is a network of information security experts from public as well as private organizations in 38 countries who exchange information on EU good practices and awareness raising initiatives. The parties communicate mainly through using bulletins, participating in monthly conference calls and taking part in events organized for the Community.

24. Janice Richardson, Representative, European Schoolnet and Coordinator, Safer Internet Initiative, in her presentation discussed "Educating about Online Safety in a Multi-Stakeholder Approach"[16]. She presented some of the activities that are currently taking place under the Insafe umbrella of activities and also looked closer at Insafe's objectives in raising cybersecurity awareness in Europe and beyond. Insafe is a European-wide network of awareness raising centers set up by the European Commission in 2004 within the framework of the European Commission's Safer Internet Programme to promote safe, responsible use of online technology, especially amongst children and young people. Ms. Richardson shared the approach adopted by Insafe to promote a culture of cybersecurity which includes three main steps: 1) provide information, 2) take action and integrate into existing practices, and 3) advocate. Over the past four years the network has earned itself a leading role in internet safety actions across Europe, and worldwide, through among other things, the initiatives organized around Safer Internet Day which is celebrated by more than 50 countries in February each year, she said. The next Safer Internet Day will be held on 10 February 2009.

25. Insafe also serves as an expert and observer to the Media and Information Society Division of the Council of Europe, and has largely contributed to its multi-lingual Internet Literacy Handbook. This has been distributed in 8 languages and hundreds of thousands of copies across the world, and is the basis for a new recently developed online safety game called "Through the Wild Web Woods"[17]. Furthermore, in 2008, in collaboration with the cable operator Liberty Global Inc., Insafe launched an eSafety toolkit containing stories and activities for 6-12 year olds and a guidebook for parents. The toolkit has already been published in 10 languages. Ms. Richardson noted that one of the more recent actions of Insafe has been its work with a consortium of 14 major companies ranging from google to Vodafone to launch a new website for teachers called TeachToday[18]. This site especially caters to the widely diverse needs of teachers striving to ensure that their pupils get the most out of technology, but keenly aware of the traps it tenders for the unwary.

26. Solange Ghernaouti-Hélie, Professor, Faculty of Business and Economics, University of Lausanne, Switzerland, followed with her presentation on "A Culture of Cybersecurity: from Policies to Practice"[19] providing an insight into the importance of education when it comes to promoting a culture of cybersecurity and building a safe and inclusive information society. The lack of know-how and understanding of all the dimensions of cybersecurity, i.e. the technical, legal, organizational and human dimensions, constitute a serious infrastructure deficiency

---

[15] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/lindy-enisa-awareness-sofia-oct-08.pdf

[16] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/richardson-insafe-sofia-oct-08.pdf

[17] http://www.wildwebwoods.org

[18] http://www.TeachToday.eu

[19] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/ghernaouti-helie-education-sofia-oct-08.pdf

that is widening the digital divide, she said, emphasizing further that developing and least developed countries face significant challenges in meeting the requirements of the global market place without adequate cybersecurity. The culture of cybersecurity should be an integral part of any national and a global response to cyber-threats dealing with the key economic, legal, and social issues in the information society. As such it is an important component required for countries preparing to deal with the challenges that are linked to the deployment of ICTs, its uses and misuses. Currently, Ms. Ghernaouti-Hélie noted, most of these efforts focus on awareness, which is appropriate but not sufficient. In order for education and awareness raising initiatives to be effective, they need to be made available and targeted towards each stakeholder group. Educational efforts and related investments should be made to educate and train all members of the information society, from decision makers, policy makers, justice and police professionals, to citizens, end-users, children and elderly.

27. In order to deal with the national and international cybersecurity issues, specific actions should be taken at the national level to increase the cybersecurity capacity of the various actors, she said. At present in developing countries most ICT end-users, individuals and organizations, do not understand security issues and do not have the skills or the tools to correctly protect their assets. They do not have the means to build confidence in ICT infrastructures and services and are therefore forced to rely on products and mechanisms they do not master, and on solutions that have been imposed on them for commercial reasons. Hence, Ms. Ghernaouti-Hélie said, security is based on obscurity. In concluding her presentation, Ms. Ghernaouti-Hélie noted some basic recommendations to effectively promote a culture of cybersecurity. These included, the need to further educate end-users; increase public security awareness in order change users' online behavior; provide end-users with the tools and means required to be responsible online; and overall focus on designing an end-user-centric security model within a given technical and legal framework whereby the user can decide what is sensible behavior based on his/her own resources.

Session 3: Public — Private Partnerships

28. With privatization, the vast majority of each country's ICT networks are now owned and operated by the private sector. A key element of a national framework for cybersecurity and CIIP is bringing the private sector and government together in trusted forums to address common national security challenges. The basis of successful public–private partnerships is trust which is necessary for establishing, developing and maintaining sharing relationships between the private sector and government. Session 3, which looked closer at the benefits as well as challenges associated with public–private partnerships, was moderated by Krasimir Simonski, Deputy Chairman, State Agency for Information Technology and Communications (SAITC), Bulgaria. Mr. Simonski noted the importance of public-private partnerships in the development of ICTs and the role these can play in building national cybersecurity capacity.

29. The first presentation in Session 3 was conducted using remote access and online training software by Vladimir Radunovic, DiploFoundation, Malta. In his presentation "Case Study on Cybersecurity and Education: Development of National Capacity"[20] discussed some of the main components that need to be considered with regards to elaborative cybersecurity education and training. In order to address the educational challenges in this area, Mr. Radunovic emphasized the need to introduce inter-professional communication in the cybersecurity curriculum, including academic courses and professional training, and a multi-stakeholder composition of student and participant groups with opening trainings to other professional and institutional groups. He also highlighted the need to increase the use of online tools for cybersecurity training and community building for a culture of cybersecurity. Mr. Radunovic also noted that based on what DiploFoundation has seen when training on other internet-related topics, when communities are encouraged to engage in peer-to-peer collaboration, involving experienced peers as intermediaries between senior experts and new trainees, participants are more likely to come away with additional learning experiences. This coupled with the concept of learning-by-doing, where training and practice are combined, has proven quite successful in other areas, and could work very well also for cybersecurity.

30. In his presentation Mr. Radunovic further highlighted the need for dedicated National Cybersecurity Capacity Development. With this he referred to using existing tools and material, like the ITU National Cybersecurity/CIIP Self-Assessment Tool, to further develop the training material based on this documentation with related courses, policy research and immersion serving as a basis for practical follow-up on initiatives and activities planned in a country. In this context he also provided an overview of what a possible training program and related courses could look like, as well as additional details on what online collaborative research for national cybersecurity capacity development could consist of and how it could be undertaken.

31. Cheri McGuire, Principal Security Strategist, Trustworthy Computing, Critical Infrastructure Protection Program, Microsoft, in her presentation provided an overview of some "Case Studies in Public-Private Partnership"[21]. Ms. McGuire started her presentation by sharing information on Microsoft's Critical Infrastructure Protection Program, which aims to build trust and alignment of actions between governments and critical infrastructure providers. Typically a public-private partnership require that all parties embrace the core aspects

[20] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/radunovic-diplofoundation-education-sofia-oct-08.pdf

[21] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/mcguire-case-studies-sofia-oct-08.pdf

of the terms "public-private" and "partnership" in order to provide the structure, processes, and environment required for trusted collaboration. The partnership needs to align industry and government requirements, priorities, goals and objectives, be flexible and adaptable to address the changing risk landscape, provide value for both government and industry members, and focus on continual improvement and assessment of lessons learned. After a more general overview of the main requirements for a successful public-private partnership, Ms. McGuire provided examples of cybersecurity and CIIP initiatives that she has been involved in both at the national and international levels.

32. Some of the national-level partnerships mentioned included Japan's Computer Emergency Response Team Coordination Center (JP-CERT) and the Japanese National Infrastructure Security Center, the Australian Infrastructure Assurance Advisory Group, the United Kingdom's Centre for the Protection of National Infrastructure and the Vendor Security Information Exchange, as well as United States' Critical Infrastructure Partnership Advisory Council, Network Security and Information Exchange, and National Security Telecommunications Advisory Committee. Ms. McGuire also shared information on two private sector partnerships, namely ICASI and SafeCode. The Industry Consortium for Advancement of Security on the Internet (ICASI)[22] was formed by a group of global IT vendors to create a trusted forum to address international, multi-product security challenges. The forum extends the ability of IT vendors to address complex security issues in order to better protect enterprises, governments, citizens and the critical IT infrastructures that support them. The Software Assurance Forum for Excellence in Code (SafeCode)[23] initiative is dedicated to increasing trust in ICT products and services through the advancement of proven software assurance methods by working to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services.

33. Victor Minin, Representative, Information Security Association, Russian Federation, in his presentation titled "Mission of NGOs in Cooperation between the Governmental Bodies and the Cybersecurity Sector"[24], discussed some of the activities which the Information Security Association (ISA) based in the Russian Federation is involved in. The organizations represented in ISA can, as per the license granted to ISA by the Federal Agency for Government Communication and Information and the State Technical Commission, provide information security services especially to safeguard sensitive and confidential data, carry out information security research and related projects, deliver projects involving the use of secret state data; research, develop and market cryptographic products and provide after-sales technical support.

34. Mr. Minin in his presentation emphasized the importance of educational activities when it comes to information security, and noted that ISA also engages in a number of awareness raising initiatives. He highlighted the need for responsible online behaviour by saying that "if you do not brush your teeth every day, you get caries, similarly if you use ICTs every day there are also some basic things you need to pay attention to". Furthermore, when people travel to other countries passports are used to identify these travellers, however when users of ICTs enter cyberspace they enter it anonymously and internet users need to be made better aware of the possible threats that this exposes them to. Who are the bad guys and bad girls on the internet?, he then asked. What ISA is doing in this regard is not only creating tools to track cyber-criminals, but establishing profiles of the criminals that could lead to the development of preventive actions and mitigation of these crimes.

35. Jody Westby, CEO, Global Cyber Risk, United States of America, in her presentation "The Culture of Public-Private Partnerships"[25] discussed how public-private partnerships can and should involve every cyber-user, from citizens to corporations, law enforcement, and critical infrastructure providers. Computers can be involved in criminal cyber-related activities in three main ways, she said: 1) as the target of offense, when confidentiality, integrity, and availability of data, applications, networks are compromised; 2) as a tool to commit a crime, including for fraud, child pornography, conspiracy; and 3) as incidental to a crime but have significant importance to law enforcement, especially for evidentiary purposes. The realities of cyberspace make it clear that everyone has to work together, she said. In this regard, public-private partnerships need to be part of the culture of cybersecurity and an integral part of every security program and incident response plan. Cybersecurity activities and responses to cyber-threats, she continued, require more resources than what one specific entity has available. Overall, PPPs need to be much more inclusive than they are today, she said. Public and private sector cooperation is also important for a global response for cybersecurity. "No attack is an island", Ms. Westby continued, highlighting the fact that each incident is instead a global issue, which require PPPs, which in turn require collaboration across national borders.

36. Ms. Westby also drew the participants' attention to some of the public-private partnership models that have been tried in other sectors of the economy, especially when privatizing state-owned enterprises. She highlighted some advantages and disadvantages with of these models that could be interesting to consider also for PPPs in cybersecurity. The sustainability of PPPs is a real issue, she said, noting the usefulness of Information Sharing

---

[22] http://www.icasi.org

[23] http://www.safecode.org

[24] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/minin-ngo-cooperation-sofia-oct-08.pdf

[25] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/westby-culture-public-private-sofia-oct-08.pdf

and Analysis Centers (ISACs) while highlighting some of the challenges that these ISACs have faced. The general purpose of an ISAC, and why they were established in the first place, is to gather and analyze information about information security threats, vulnerabilities, incidents, countermeasures, and best practices, and share these findings with the members. She noted that there might be a need to revisit the structure and the incentives that bring the different actors together to share information in ISACs to ensure that their sustainability is not impacted. With many industries becoming increasingly dependent on one and other, electricity and telecoms, etc., there is a growing need for to start looking at how stakeholders can move towards a more harmonized approach for cybersecurity, she concluded.

37. During the evening of the first full day of the forum the participants were invited by the Chairman of the State Agency for Information Technology and Communications to a reception at the Central Military Club.

Session 4: Legal Foundation and Enforcement

38. 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, in accordance with international conventions and recommendations. Session 4 looked closer at the need for a sound legal foundation and effective enforcement, reviewed some of the national legal approaches taken to date and explored potential areas for international legal coordination efforts. The session was moderated by Ehab Elsonbaty, Senior Judge, Damanhour Court, Egypt 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.

39. Henrik Kaspersen, Professor, University of Amsterdam, The Netherlands, Member and Former Chair, Cybercrime Convention Committee, provided the first presentation in the session with an overview of the "Council of Europe Convention on Cybercrime"[26]. He noted that from the very beginning when work was started on the text in the Convention, the ambition was to have a global Convention. To date 47 countries have signed and 23 have ratified the Convention and that, he said, is enough to move forward with the instrument at this point in time. The signatories of the Convention include the European Union Member States and the G7 countries. He also noted that countries outside the European Union have in addition taken on board the Convention as a model law when revising and updating their legislation and drafting new legislation. The Cybercrime Convention aims towards: a) harmonization of substantive criminal law to ensure that there are no data havens and approach dual criminality and cybercrime in both the narrow and broader sense; b) harmonization of investigative powers to provide capacity to collect electronic evidence, preservation power, production of data, including traffic data, internet surveillance, etc.; and c) international cooperation on the basis of the Convention, with existing bi- and multilateral instruments and expedited assistance through the 24/7 High Tech Crime Network and other means.

40. Mr. Kaspersen mentioned that the Convention on Cybercrime is one of the best performing conventions in the Council of Europe portfolio of conventions. Is the Convention perfect?, he then asked, and noted that there are some problem areas which include extraterritorial jurisdiction (referring to Art. 22 CCC), executive jurisdiction (referring to Art. 32 CCC) and the possible lack of a sense of urgency with a relatively low rate of solved cases to showcase and an emphasis on domestic cases. Mr. Kaspersen also introduced the Council of Europe Cybercrime Project. The Cybercrime Project encompasses a number of cybercrime coordination activities including: consultations with industry with regards to possible codes of practice; cooperation with law enforcement agencies; exchange of experiences, methods and tools; provision of training and legal advice; and, the development of new forums, like the Convention Committee on Cybercrime (TC-CY) where cybercrime-related issues are discussed and debated.

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

42. 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

[26] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/kaspersen-cybercrime-convention-sofia-oct-08.pdf

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

43. Matthew Lamberti, Intellectual Property Law Enforcement Coordinator for Eastern Europe, United States Department of Justice, United States Embassy in Bulgaria, followed with his presentation on "Legal Foundation and Enforcement: Country Case Studies"[27] providing an insight into some of the lessons learned based on the work he is doing in 20 of the Central and Eastern European countries. Mr. Lamberti noted that countries in the region generally have laws that cover cybercrime and that many countries have already designated dedicated agents to deal with specialized computer crime, but that there is a lack of enforcement capability in most of the countries. If laws are not enforced in this important area, business and investment will go elsewhere, he said. He further noted that many of the cybersecurity and cybercrime-related cases and investigations cross borders and because of this any investigation needs to be global in its outreach.

44. Mr. Lamberti emphasized the importance of revising and updating laws to deal with the new and emerging technologies. He noted that the Council of Europe's Convention on Cybercrime is an important tool and that people in the countries in the region are aware of the Convention but that the countries are not necessarily using it directly to guide their work on criminalizing the misuse of ICTs. Mr. Lamberti gave some examples of collaborative investigations across borders and mentioned an investigation where law enforcement officials from the United States and Romania had been involved, noting that the only way this successful collaboration was possible was due to the fact that it was done under the auspice of the Convention on Cybercrime and the 24/7 High Tech Crime Network. In this regard he also shared insights into some of the investigations and prosecutions that he has been working on together with industry and how this approach can in many ways save money for country governments.

45. Yavor Kolev, Chief Inspector, Head of Cybercrime Unit, National Police Service, Bulgaria, in his presentation titled "Bulgarian Law Enforcement Counter Cybercrime Authorities: Structure and Legal Framework"[28] shared information on the structure, legislation and enforcement that Bulgaria has put in place to fight the growing cyber-related crimes. He noted that even though this is quite new area in Bulgaria, there are already 50 people working in this area in the country, and more people will be recruited to work in this area in the coming months. Mr. Kolev mentioned that each Directorate belonging to the Ministry of Interior has at least one person who is trained to work in the area of cybercrime.

46. Mr. Kolev also mentioned that the existing 24/7 High Tech Crime Network has been a very useful tool and resource in their everyday work and with regards to this Mr. Kolev gave some examples of how Bulgaria is using the network to conduct their investigations. He noted that the assistance provided through the network is an effective way to ensure that data is being preserved correctly and in a timely fashion in order to support the ongoing investigations. On the receiving side of the network, Mr. Kolev mentioned that the cybercrim unit that he head is receiving many requests to investigate computer related crimes. The Bulgarian penal code is the main legal text that the investigators are relying on when investigating and bringing forward these crimes. Especially some articles are more relevant than others, he said giving an example of Art. 159 on pornography, especially the text related to child pornography, and the penalties for these and associated crimes.

47. Ehab Elsonbaty, Senior Judge, Damanhour Court, Egypt, with his presentation "An Overview of Legal Challenges"[29] provided an insight into some of the legal tools that are currently being used to address cybercrime in Egypt. He noted that as cybercrime is growing much more that physical crime, and critical infrastructures are increasingly run on and managed by computers and networks, the rules in the Egyptian legal system for cybercrime are currently being revised. All countries, he said, need to ensure that their criminal laws are revised to accommodate for the particular nature of cybercrime. This revising and updating may be done by modifying some articles regarding the classical crimes done via new media, abolishing some others which are not adequate or by creating new rules for completely new issues.

48. Mr. Elsonbaty also noted that the levels of punishment, be it imprisonment or fines, should also be reviewed. The importance of developing training programmes for law enforcement officers, prosecutors as well as for judges and legislators was furthermore emphasized by Mr. Elsonbaty. The international nature of cybercrime, he continued, creates the need for an international solution which covers substantive, procedural and international

---

[27] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/lamberti-united-states-case-study-sofia-oct-08.pdf

[28] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/kolev-bulgaria-enforcement-sofia-oct-08.pdf

[29] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/elsonbaty-legal-challenges-sofia-oct-08.pdf

cooperation rules. In this regard he mentioned the work done in Egypt and that he was looking forward to a modern Egyptian cybercrime act. Finally Mr. Elsonbaty mentioned the G8 24/7 High Tech Crime Network as a useful contact network for dealing with cases that involve collecting electronic evidence across borders.

Session 5: Organizational Structures and Incident Management Capabilities

49. A key activity for addressing cybersecurity at the national level requires preparing for, detecting, managing, and responding to cyber incidents through the establishment of watch, warning and incident response capabilities. Effective incident management requires consideration of funding, human resources, training, technological capability, government and private sector relationships, and legal requirements. Collaboration at all levels of government and with the private sector, academia, regional and international organizations, is necessary to raise awareness of potential attacks and steps toward remediation. Session 5, moderated by Jaroslaw Ponder, Focal Point for Europe, ITU Development Sector (ITU-D), discussed best practices, organizational structures and related standards, and the technical, managerial and financial aspects of establishing national, regional and international watch, warning, and incident response capabilities.

50. Jacek Gajewski, Secretary-General, Central and Eastern European Networking Association (CEENet), Poland and Representative, ENISA Permanent Stakeholder Group, opened the session with a presentation on "ENISA's Step-by-Step Guide to Setting up a National CERT/CSIRT"[30]. Released in 2006, the ENISA Step-by-Step Guide for Setting up Computer Security Incident Response Teams (CSIRTs)/Computer Emergency Response Teams (CERTs) aims to cover all aspects of the services CERTs can provide and the necessary steps to get started with regards to business management, process management, and the technical aspective of establishing a CERT. The guide includes case studies, exercises and a practical project plan for putting everything into practice. CERTs constitute a crucial building block for safeguarding network and information systems, Mr. Gajewski noted. A wider geographical distribution of CERTs, with more CERTs in all different sectors of society, meaning in academia, government as well as in business are needed, he said. CEENet is an association of national organizations which focus on academic, research and educational networking and currently comprises of 23 national research and education networks in Central and Eastern Europe. As such CEENet is in a good position to support the creation of CERTs/CSIRTs in the region. In 2007 CEENet started a project to encourage the creation of additional academic network CERTs in these countries. As a result, CEENet currently has three ongoing projects in the region and are planning to launch a fourth project for the Magreb countries.

51. To date 1-3 officers in each CEENet country have been trained, using the training material available through ENISA's Step-by-Step Guide and TRANSIT material distributed by TERENA. Mr. Gajewski mentioned that when CEENet has been in the process of establishing academic CERTs together with the countries, these academic CERTs have often served as a first step in establishing a country's national CERTs. Mr. Gajewski concluded his presentation by providing an overview of the establishment of CERTs in some of the CIS countries. He noted that while some CERTs have been highly successful others have suffered and have had difficulty to run their operations in a sustainable manner. He also noted that starting a new CERT in a country requires close to a two year long incubation period. A parent organization willing to help monitor and support the activities of the new organization is also required. Still, he said, there are many countries without CERTs/CSIRTs and he encouraged countries in the region to expand this network and establish their own CERTs.

52. Alexander Zolotnikov, Chief of Information Security, TransTeleCom, Russian Federation, presented on "Cybercrime Counteraction a Practical Activity of the Backbone Telecommunication Operator"[31]. In his presentation he addressed cybercriminality in global information networks, the combating of unsuitable online content and the role of a telecommunication operator in this regard. Mr. Zolotnikov noted that the information that can currently be found on the internet, in terms of its objectivity, integrity, reliability, truthfulness and decency, has a fundamental bearing on the individual's personal development and on the active role he or she pursues in life. The appearance of content on the internet can have a very negative impact on the development of people and society, and can also ultimately constitute a threat to a country's national security. This state of affairs, Mr. Zolotnikov said, calls for the implementation of active and timely measures designed to combat such internet-borne threats. Mr. Zolotnikov further discussed what measures a telecommunication operator can take in order to combat the related problems and highlighted the need to urgently elaborate on means to deal with unsuitable content on the internet especially when it comes to the spreading of child pornography.

53. In countering the spread of child pornography he shared some statistics on how the Russian Federation is dealing with this issue. Some ways to counteract the problem were assessed and Mr. Zolotnikov proposed a mechanism that from the telecommunication operator's point of view could be considered the most effective for combating unsuitable and undesirable content, this included the need to take action and address this at the carrier level allowing for the maximum competence and flexibility in shaping services.

54. Mauro Vignati, Analyst, MELANI, Federal Office of Police, Switzerland, in his presentation on "Public-Private Partnerships: Switzerland Case Study"[32] discussed why there is an urgent need to protect the national critical

[30] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/gajewski-enisa-cert-toolkit-sofia-oct-08.pdf

[31] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/zolotnikov-content-sofia-oct-08.pdf

[32] No slides available.

information infrastructure and how Switzerland has organized itself to deal with the growing challenges related to CIIP. He started his presentation by discussing the difference between CIIP and CIP and the strong link between the two, and introduced MELANI which is the Swiss reporting and analysis center for information assurance. MELANI has been operational since October 2004 and forms the core of the Swiss early-warning system as it plays an integral role in all four pillars of the Swiss information assurance policy (i.e. prevention, early warning, crisis management, and technical problem solutions). Since early 2008, MELANI has also run the Swiss government's CERT, GovCERT.ch, which serves as a technical competence center responsible for dealing with related technical incidents.

55. Mr. Vignati mentioned the growing threats to countries' Supervisory Control and Data Acquisition or SCADA systems, noting that also these systems can be manipulated and controlled remotely with possible attacks having severe consequences for society. In this regard he also shared with the participants insights into some possible test attacks done through computer systems. For discussions and activities related to the national information infrastructure, Mr. Vignati highlighted the importance of including every relevant industry stakeholder in these discussions. In Switzerland the importance of including representatives from the financial and banking sector in the CIIP debates was mentioned as an example.

Session 6: A National Cybersecurity Strategy

56. Increasingly, electronic networks are being used for criminal purposes, or for objectives that can harm the integrity of critical infrastructure and create barriers for extending the benefits of ICTs. To address these threats and protect infrastructures, each country needs a comprehensive action plan that addresses technical, legal and policy issues, combined with regional and international cooperation. What issues should be considered in a national strategy for cybersecurity and critical information infrastructure protection? Which actors should be involved? Are there examples of frameworks and approaches that can be adopted? Session 6, moderated by Roumen Trifonov, Secretary, Coordination Council on Information Society, Council of Ministers, Bulgaria, sought to explore in more detail various approaches, best practices, and the key building blocks that could assist countries in establishing national strategies for cybersecurity and CIIP. Building on the presentations made in earlier sessions, Session 6 discussed the final element for organizing national cybersecurity/CIIP efforts which ties the other components together, namely the overall development of a national cybersecurity strategy.

57. The first presentation in this session was delivered by Alexander Donos, Director, State Enterprise, Center for Special Telecommunications, Moldova, who presented the "Moldova Country Case Study – A National Information Security Strategy"[33]. In his presentation he noted some of the risks to information security and threats to the information society overall, namely, unauthorized access to state information system and resources; unauthorized substitution and deleting of information of state importance; blocking of governmental websites and information systems, as well as attacks by hackers, computer viruses and spam. Measures undertaken in Moldova to deal with these threats include the implementation of digital signatures and the creation of the necessary conditions for its application, the development of a secure telecommunication system for public authorities in the city of Chisinau city, and the creation of a main Government Data Center to secure critical state databases and information.

58. As priorities in the country's security measures, Mr. Donos highlighted the need to move forward on creating of intra-departamental systems for information, expanding the public authorities' telecommunication systems in the country and integrate the information system of both central and local authorities. He also mentioned the need to create a security gateway for the governmental portal and proceed with the creation of the national center for ensuring information security and for the related administration of the public authorities' telecommunication system. The purpose of this situation center, which will be situated within the premises of the state enterprise special telecommunications center, Mr. Donos said, is the prevention and detection of computer intrusions and hacker attacks, the development of protection against viruses and spam, and the overall control and monitoring of the state of information security on the national level. These activities all fall under an initiative, lead by the President, to further the development of an e-management system for the state. The planned project is built up around three main phases: 1) development of the e-Government infrastructure, which has already been completed; 2) implementation of e-government services, which is currently being undertaking through among other things the development of e-services for citizens; and 3) the further development of e-Government services. In moving forward on these initiatives to provide a secure online environment in Moldova, Mr. Donos highlighted the need to work together with neighbours.

59. Valery Konyavskiy, Director, All-Russia Research-and-Development Institute for the Problems of Computing Equipment and Information (VNII PVTI), Russian Federation, discussed some "New Approaches to Ensure Cybersecurity"[34]. PVTI is a network of research organizations under the Ministry of Telecom and Mass Communications dedicated to scientific research, addressing problems of lawmaking in the telecommunication field, information security, certification, computer systems and networks, etc. The institute has been involved in the development and implementation of large-scale national projects such as the state network of computer

[33] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/donos-moldova-case-study-sofia-oct-08.pdf

[34] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/konyavsky-new-approaches-sofia-oct-08.pdf

centers, the centers of collective use, among others. Mr. Konyavskiy noted that there is too much statistics out there on all aspects of information and communication technologies and the dependency on these statistics is leading the different stakeholders to build their responses inaccurately. When the response to the threats and the emerging threats is not the right one, "the strawberries will get stolen no matter how high the fence", he said. Furthermore, if stakeholders do not know exactly what it is that is being protecting the defences and responses will most likely continue to be inaccurate. Mr. Konyavskiy thus encouraged the meeting participants to make a conscious change in the approaches they are currently adopting and stop looking at the computer world as a natural phenomenon but instead as something that was created by people.

60. Slavcho Manolov, Advisor to the Chairman of SAITS, Bulgaria, and Alternate Member of the ENISA Management Board, in his presentation discussed "The Policy of the Bulgarian Government in the Field of Network and Information Security"[35]. The Law on Electronic Governance adopted in June 2007 regulates the requirements for achieving network and information security in public information systems in the country and has assigned SAITC as the government authority responsible for this. With regards to the Bulgarian overall response to building network and information security, Mr. Manolov mentioned that the adopted policy contains well defined information security measures which can be realized at two levels: those that relate to the central level of response and those at the level of an administrative body. At the central level, measures include such as: a) the establishment and centralized management of the national electronic communications network (NESM); b) the establishment of a national computer security incident response team; the creation of a unified environment for secure exchange of electronic documents (ESOD); the implementation of a national e-governance data model for the public administration through centrally managed registers; a unified policy for disaster recovery centers; the establishment of central unit for monitoring of network and information security under SAITC, etc. The level of an administrative body is in turn based on the following policies: a) internal rules and guidelines in accordance with the systems of information security management specifications under ISO 27001:2005; specific certification of administrative information systems and networks by the Chairman of SAITC, etc.

61. Mr. Manolov also discussed the establishment of the Bulgarian government CSIRT, the requirement in the regulation to establish the CSIRT and how the government had gone about creating the foundation for the entity with the support of the Hungarian CERT and ENISA. He noted that the CSIRT will also play part of the role of a national CERT. The approach and policy of the Bulgarian government in the field of network and information security, in municipalities and in the government, is more decentralized compared to the Moldovan approach presented earlier, Mr. Manolov noted. The Electronic Governance Act and the six related regulations make up a consistent and functionally complete environment with regards to the requirements for network and information security of administrative information systems. These requirements, Mr. Manolov said, are primarily aimed at ensuring the smooth exchange of internal electronic administrative services between administrations.

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

62. Session 7, aimed to review and further discuss the different elements required to develop and organize national cybersecurity/CIIP efforts and the related ITU National Cybersecurity/CIIP Self-Assessment Tool, identifying some of the main takeaways from the presentations in the different sessions and the country case studies in preparation for the concluding meeting discussions. These discussions were integrated into the final discussions that took place in Session 10 dedicated to Regional and International Cooperation and Session 11 wrapping up the meeting and identifying some concrete steps forward for cybersecurity activities in Europe and the Commonwealth of Independent States.

Sessions 8: Cybersecurity Forensics

63. Session 8 provided an overview of work done in the region in the area of cybersecurity forensics, incident analysis, and best practices for engagement with law enforcement. The session moderator, Andrea Ghirardini, Consultant and Expert on Computer Forensics, United Nations Interregional Crime and Justice Research Institute (UNICRI), opened the session by noting that cyberforensics in a new area and that it is here to stay.

64. Eugene Nickolov, Doctor of Mathematical Sciences, Director, National Laboratory of Computer Virology, Bulgaria in his presentation titled "Modern Trends in the Attacks Against Critical Information Infrastructure"[36] examined some of the definitions used in the field of cybersecurity and cyber-forensics. He also provided an overview of some of the attacking instruments that are being used and the changes observed during the past few years in this area. Mr. Nickolov discussed the scale of these attacks in the global networks and how viruses and worms have evolved to what they are today. He ended his presentation with some security trends and a set of information security tools and practices that have proven to be useful to protect against attacks on the information infrastructure. Here he mentioned the need to apply proactive software assurance and safely support authorized users, how to block network and host based attacks and eliminate security vulnerabilities, and listed some tools to use to manage security and maximize effectiveness.

---

[35] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/manolov-bulgaria-strategy-sofia-oct-08.pdf

[36] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/nickolov-modern-trends-sofia-oct-08.pdf

65. Ales Zavrsnik, Research Associate, Institute of Criminology, Faculty of Law, Slovenia, shared with the meeting participants the discussion surrounding the "Criminal Justice System's Intervention to Cybersecurity Threats: Panacea or Pandora's Box?"[37]. In his presentation he noted that societies today are relying on a number of methods to respond to cybersecurity threats, including public cybersecurity raising awareness, building safe technologies by enhancing protocol security, protecting the networks in a variety of way, and so on. Yet, he said, non-repressive technological methods used by the private sector and technology-savvy people, cannot alone provide a sufficient level of information and network security and safety. Because of this, he noted, the fight against cyber-threats need to be backed and executed by a central system of crime control, i.e. by the criminal justice system. This system is only one link in the cybersecurity chain that can help to enhance cybersecurity but simultaneously this response can also provoke undesirable effects, like the violation of civil liberties and the possible impact this may have on the free use of the internet and related public policy concerns.

66. With his presentation Mr. Zavrsnik wanted to make the case why cyberforensics should have a place in the criminal justice system framework but also highlight some of the challenges that the cyberforensic profession is currently faced with due to the ambiguities prevalent in the field. With regards to the electronic footprint he asked for decisions and agreements to be made on how to collect intangible and transient data, how to analyze and make sense of this information, and how to preserve digital information? He further asked for clarity on how to identify suspects going back from the available data, to a virtual identity, to a real person. He also brought to the participants' attention the question about how to obtain the data and information, as transmitted or residing on a resource. By asking the participants to think creatively about the issue of what is a bigger threat: the growing problem of cybercrime or the actual reactions to the problem of cybercrime in the justice system's response, he discussed some of the very real problems in this regard. With regards to the deregulation of expertise: who can conduct cyberforensic analysis, who can provide guidance on handling of digital evidence, who should be providing training for law enforcement personnel, should training be provided by the manufacturers of the forensic tools available? Mr. Zavrsnik highlighted that we are witnessing an over-extension of the reach of criminal law which in turn can have severe consequences.

67. Fredesvinda Insa, Manager, Strategic Development, CYBEX, Spain, in her presentation titled "The Need for A European Legal Framework and Training Concerning Electronic Evidence"[38] she elaborated on the need of a European legal framework and training programs for handling e-evidence. New technologies have exponentially increased the creation of electronic documents in organizations all over the world, she noted, and more than 3 trillion of emails are sent in the world every year. Research shows that in many European organizations more than 90 per cent of the documents are electronic and less than 30 per cent of these are printed. The use of the digital means and the virtual environment is not exempt from dishonest use and traditional evidence is moving from paper and print to a virtual environment. In the context of electronic evidence, management procedures and admissibility criteria are changing. E-evidence is gaining increased relevance in legal procedures because it is the best mean to prove that certain types of crime have been committed through these new technologies, she stated. Nonetheless, existing legislation available in the European countries studied does not establish any specific definition on e-evidence and does not regulate e-evidence handling.

68. Ms. Insa noted that the results of a related study that Cybex, a Spanish organization which focuses on seizing, analyzing and presenting electronic evidence in courts, conducted amongst European judges, lawyers, prosecutors, and law enforcement bodies, showed that a European legal framework and specific training programs on e-evidence is necessary. Given the transnational character of e-evidence this would help countries develop their national legislation in the area while ensuring a standardized regional and international approach to handling e-evidence. Specific procedures for obtaining, analyzing and presentation of e-evidence are therefore now being discussed, Ms. Insa continued. In the European countries examined, general proceedings are applied to the e-evidence, while other times the proceeding established for traditional evidence is applied. Furthermore, the legal requirements in the individual countries occasionally overlookthings such as: fundamental rights, data protection issues, existing telecommunications laws, the chain of custody, measures related to the authenticity of evidence, etc. Ms. Insa concluded her presentation by sharing information on some of the ongoing projects on the European level which concern e-evidence. When it comes to training on e-evidence she shared information on the new "European Certificate on Cybercrime and Electronic Evidence" program which aims to train judges, prosecutors and lawyers. The program will be launched with the participation of 13 European countries as well as Argentina, Brazil and Venezuela in academic programs and later extended into seminars and courses. Ms. Insa also noted that the first electronic library on e-evidence and cybercrime, containing legislative texts, case laws, expert articles will soon be launched, and the development of an electronic newsletter for e-evidence and the fight against cybercrime is underway.

69. Andrea Ghirardini, Consultant and Expert on Computer Forensics, United Nations Interregional Crime and Justice Research Institute (UNICRI) in his presentation on "Open Source Applied to Computer Forensics"[39] discussed computer forensics and open source software focusing on GNU/Linux. Open source, Mr. Ghirardini said,

---

[37] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/zavrsnik-criminal-justice-system-sofia-oct-08.pdf

[38] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/insa-cyber-forensics-sofia-oct-08.pdf

[39] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/ghirardini-open-software-sofia-oct-08.pdf

should be used in computer forensics for several different reasons. Some compelling reasons include the need to keep costs down which is highly desirable for emerging economies and countries with low dedicated budget, and to allow for the use of technologies that may perform better than commercial solutions. Open source software is often also updated faster than other commercial software which is useful for an area that is forced to develop quickly with the changing technology. Mr. Ghirardini also noted some additional benefits of using open source software for forensics analysis in terms of availability (the software is available online and old version can always be found), open format (files can easily be converted from one file format to another), possibility to double check analysis conducted (other parties can check every step of the analysis), and transparency (open source software can easily be checked).

Session 9: The Economics of Cybersecurity

70. Security flaws are often due to perverse incentives rather than the lack of suitable technical protection mechanisms. Since individuals and companies do not bear the entire costs of cyber incidents, they do not tend to protect their system in the most efficient way. If they did support all the financial consequences, they would have stronger incentives to make their network more secure for the good of all interconnected networks. Session 9 of the forum reviewed some of the current leading thinking and research on the economics of cybersecurity and presented a recent ITU study dedicated to the Financial Aspects of Network Security: Malware and Spam[40]. Roumen Trifonov, Secretary, Coordination Council on Information Society, Council of Ministers, Bulgaria, served as the moderator for Session 9 and provided an introduction to the session and managed the discussions that followed.

71. Michel van Eeten, Associate Professor, School of Technology, Policy and Management, Delft University of Technology, The Netherlands, provided an overview of the "ITU Study on the Financial Aspects of Network Security: Malware and Spam"[41]. The study is a survey of existing resources and data available when it comes to the economics and financial aspects of cybersecurity. Measures to improve information security enhance trust in online activities and contribute directly and indirectly to the welfare gains associated with the use of information and communication technologies (ICTs), Mr. van Eeten explained. However, some expenditure on security is only necessary because of relentless attacks by fraudsters and cybercriminals that undermine and threaten trust in online transactions. Such costs are not welfare-enhancing but instead a burden on society. Two vectors through which such attacks are carried out are malware and spam. During the past two decades, the production and dissemination of malware has grown into a multibillion dollar business. Damages created by fraudulent and criminal activities using malware and the costs of preventative measures are likely to exceed that number significantly. Malware puts the private and the public sector at risk because both increasingly rely on the value net of information services, he said.

72. Spam and malware have multifaceted financial implications on the costs and the revenues of participants in the ICT value chain. The costs carried by all stakeholders across the value network of information services are affected directly and indirectly by this. But most of the financial flows between the legal and illegal players in the underground cybercrime economy are only partially known. The background study prepared by Mr. van Eeten and his team develops a framework within which these financial impacts can be assessed and brings together the many disparate sources of financial data on malware and spam. Some of the findings of report include: a) Estimates of the financial effects of malware differ widely, figures for overall effects range from USD 13.2 billion of direct damages for the global economy (in 2006) to USD 67.2 billion in direct and indirect effects on businesses in the United States alone (in 2005). b) Numbers documenting the magnitude of the underground internet economy and transactions between it and the formal economy also vary widely. One source estimates the worldwide underground economy at USD 105 billion. c) No reliable numbers exist as to the potential opportunity costs to society at large due to reduced trust, however, a considerable number of users have indicated that it reduces their willingness to perform online transactions. d) Although the financial aspects of malware and spam are increasingly documented, serious gaps and inconsistencies exist in the available information. This complicates finding meaningful and effective responses, and for this reason, more systematic efforts to gather more reliable information would be highly desirable, Mr. van Eeten explained.

Session 10: Regional and International Cooperation

73. Regional and international cooperation is extremely important in fostering national efforts and in facilitating interactions and exchanges. The challenges posed by cyber-attacks and cybercrime are global and far reaching, and can only be addressed through a coherent strategy within a framework of international cooperation, taking into account the roles of different stakeholders and existing initiatives. As facilitator for WSIS Action Line C5 dedicated to building confidence and security in the use of ICTs, ITU is discussing with key stakeholders how to best respond to these growing cybersecurity challenges in a coordinated manner. For instance, the ITU Global Cybersecurity Agenda (GCA) provides a platform for dialogue aimed at leveraging existing initiatives and working with recognized sources of expertise to elaborate global strategies for enhancing confidence and security in the information society. The session reviewed some of the ongoing initiatives in order to inform forum participants

[40] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf

[41] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/eeten-financial-aspects-sofia-oct-08.pdf

and to further the discussions in order to identify possible next steps and concrete actions to foster and promote international cooperation for enhanced cybersecurity.

74. Marco Obiso, Adviser, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Sector (ITU-D) opened the session with a presentation on the ITU's activities when it comes to international cooperation for a safer cyberspace in an "Overview of the ITU Global Cybersecurity Agenda"[42]. He noted that through the GCA ITU is paving the way for enhanced global cooperation for a safer and more secure cyberspace. With its 191 Member States and more than 700 Sector Members, including leading industry players, it is well placed to provide the forum for international cooperation on cybersecurity. Because of its long experience in cybersecurity, Mr. Obiso continued, ITU was entrusted by world leaders at the World Summit on the Information Society to take the lead on action line C5 dedicated to building confidence and security in the use of ICTs. ITU, through its three Sectors, ITU-R, ITU-T and ITU-D, is thus working towards a global, coordinated and harmonized approach to achieving cybersecurity. Mr. Obiso noted that as the lead facilitator for WSIS action line C5, ITU is working with all key stakeholders on how to best respond in a coordinated manner to the growing cybersecurity challenges. In this regard the ITU Global Cybersecurity Agenda can provide the strategic directions that would foster international cooperation. He also mentioned the leading role played by the ITU Sectors, especially ITU-D, in converting the agreed strategies into actions and projects to be implemented together with partners in Europe and CIS as well as in the other regions.

75. Ilari Patrick Lindy, Senior Expert, Relations to Industry and International Organisations, ENISA, followed with an overview of what ENISA is doing in the area of regional and international cooperation in "ENISA and Regional Cooperation"[43]. ENISA was created to be a stimulator and catalyst by its regulation to work on the elements that allow for the smooth functioning of the market, not to execute a European defense policy or coordinate police cooperation. With its 30 operational people ENISA also works to raise the general level of European Member States for network and information security and overall as a facilitator for building a stronger European cooperation area. To better engage stakeholders, he continued, we need to know what the stakeholders are in need of, what the barriers in the market are and what some of the incentives out there could be. ENISA aims to act as a broker between the Member States in the network and information security area and works to bring the different stakeholders and stakeholder groups in the region together using different outreach and communication tools to make sure that the stakeholders are aware of the activities that are taking place.

76. Mr. Lindy further mentioned that there is a lot of interest in the work of ENISA also amongst stakeholders in countries outside the European Union. Today, ENISA is looking mainly towards these countries where some kind of collaborative initiatives in the research area could be undertaken, he said. ENISA can also be studied as an organizational model, he said, bringing together many different countries, representatives from a variety of backgrounds, to work together on elaborated network and information security initiatives. ENISA, Mr. Lindy continued, does not want to create papers but see how the different approaches are implemented in practice, in the countries.

77. Alexander Donos, Director, State Enterprise, Center for Special Telecommunications, Moldova and Chairman of the Commission on Information Security under the Coordinating Council, Regional Commonwealth in the Field of Communication (RCC) followed with an overview of the "Activities of the Commission on Information Security under the Coordinating Council of the CIS Member States on Informatization Attached to RCC"[44]. The main goals and functions of the Commission, he noted, include: elaborating recommendations in the field of the information security; exchanging information and experiences in creating systems and means to ensure information security of information and telecommunication systems and networks; preparing joint proposals and establishment of priority of issues for CIS countries; preparing joint recommendations on the elaboration of interstate programs in the field of information security; elaborating on proposals on the harmonization of national legislation in CIS Member States; and, preparing proposals on further development of the market, among other things. Mr. Donos also shared details on a pilot project for trans-boundary legally significant information exchange applying the digital signature in 2009-2011, which is organized following the results of the joint R&D RCC "Research of the possibility of applying the digital signature at trans-boundary information exchange".

78. Matthew Lamberti, Intellectual Property Law Enforcement Coordinator for Eastern Europe, United States Department of Justice, United States Embassy in Bulgaria presented on "Promoting Regional and International Cooperation On Cybersecurity Issues"[45] and the 24/7 High Tech Crime Network, originally a G8 initiative, which provides a contact network for online crime issues. The network is intended to provide a simple cooperation mechanism that can be used by countries to report on incidents and allow follow-up. The network is made up of law enforcement people who among other things share information and advice related to data preservation, ISP contacts, and how to start mutual legal assistance processes. The network is open to all countries and is easy to

---

[42] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/obiso-GCA-overview-sofia-oct-08.pdf

[43] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/lindy-regional-cooperation-sofia-oct-08.pdf

[44] http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/donos-RCC-overview-sofia-oct-08.pdf

[45] No slides available.

join. The only requirements being that the country identifies a contact point, a person on call who has sufficient technical knowledge when it comes to dealing with cyber-related crimes, as one of the main issues with these cybercrime cases is the handling digital forensic evidence. The person also needs to know domestic laws and procedures with regards to electronic evidence. When used, this instrument has been very useful, Mr. Lamberti continued, and mentioned some examples where the network had made available information that have made it possible to identify and arrest cybercriminals.

79. Eduard Djanserikov, Head, Information Security Sector, JSC Kyrgyztelecom, Kyrgyz Republic, in his intervention discussed the "Cooperation of Telecom Operators of RCC Participant Countries in the Field of Cybersecurity"[46]. Mr. Djansetikov noted that coordination on cybersecurity-related in RCC countries currently also involves relevant private sector actors. He shared with the participants examples of some of the activities undertaken by private sector entities of RCC to facilitate international cooperation. Mr. Djansetikov further highlighted the importance of the private sector to liaise with the relevant government entities and with international organizations.

80. Jaroslaw Ponder, Focal Point for Europe, ITU Telecommunication Development Sector (ITU-D) followed, drawing the participants' attention to the regular programming of ITU-D's activities related to the cybersecurity and the process for responding to the needs of countries in the region in this respect. He also mentioned the upcoming World Telecommunication Development Conference (WTDC)[47] to be held in 2010 and how Member States can actively participate in the Conference itself and the preparatory process. Mr. Ponder highlighted the importance of active participation of all administrations in the Regional Preparatory Meetings to be held in 2009. These preparatory meetings provide an excellent opportunity for defining the needs of the countries at the regional level, also in field of cybersecurity.

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

81. The final session of the meeting was co-facilitated by Krasimir Simonski, Deputy Chairman, State Agency for Information Technology and Communications (SAITC), Bulgaria 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 protection of critical information infrastructures in the region. Some recommendations for concrete action that need to be taken by countries in the region were identified.

82. Mr. Obiso noted the need for countries to undertake action to:

- Review and, if necessary, revise or draft new legislation, to criminalize the misuse of ICTs, taking into account the rapidly evolving cybersecurity threats. This process would need to take into account: 1) requirements related to attacks and threats generated from country to country; 2) requirements related to attacks or threats generated from outside and pose a threat to a country. The two requirements can be converted into effective mechanisms if international frameworks are taken in consideration. The country legislation should develop or adapt the cyber-legislation according to existing international instruments.
- Develop the necessary organizational structures aimed at properly addressing cybersecurity-related issues. This process would allow for the creation of a structure that would be accountable for cybersecurity issues in the country. This structure can be affiliated directly with the Government or operating in close coordination with the Government. Some possible components of such a structure can include:
    - A national cybersecurity coordinator (an individual or an office) to organize the work and coordinate the efforts, interacting with Government, business, and academia.
    - Incident management capabilities with national responsibility. This activity would involve the possible creation of a National Cybersecurity Center with the medium/long-term objective of establishing a CERT/CSIRT.
- Inject measures that enhance the protection of children into the country's ongoing cybersecurity-related activities. This would involve technical mechanisms aimed at mitigating the risks for young people and children online, including:
    - Development of a framework for authentication and authorization to ensure that children are protected from inappropriate material.
    - Development of an internationally recognized database for law enforcement agencies.
- Ensure coordinated efforts on several areas related to cybersecurity forensics and analysis, including:
    - Training and capacity building.

[46] No slides available.

[47] http://www.itu.int/ITU-D/wtdc/

- Cost effective technical solutions to perform forensics related activities.

83. Mr Simonski further noted the need for the countries to:

- Build competence and expertise as these are essential components for developing cybersecurity capabilities and sharing knowledge. Awareness raising and training were noted as main elements of countries' cybersecurity capacity building efforts.
- Bring the different cybersecurity stakeholder together and provide a platform for fostering partnerships for enhanced cybersecurity. The importance of identifying the relevant players in the cybersecurity arena and establish a dialogue in order to define possible partnerships and effective cooperation mechanisms is critical going forward. Close collaboration and exchange of experiences with will improve the understanding of each party's activities, role, and competencies.
- Develop the right foundation for a multi-stakeholder approach. The presence of the various players and actors should be guaranteed to ensure that the multitudes of views are taken in consideration. The work should be undertaken following the perspectives and dimensions characterizing the operational cybersecurity environment, noting the roles of the stakeholder groups:
    - Business – in order to ensure that the latest technical developments are injected in the process;
    - Government – to ensure overall accountability and responsibility. It is important that public sector is active in order to ensure stability and continuity in the protection of a country's critical information infrastructure;
    - International and inter-governmental organizations – to ensure that international cooperation and the global aspect of cybersecurity-related related responses are taken into consideration. Only IGOs can address international public policy issues and define the frameworks that can be driving the process toward global cybersecurity. In particular ITU, with its GCA and its role as lead facilitator on WSIS action line C5, represent a key actor that the government can work with in this respect.

84. Mr. Simonski highlighted that Bulgaria will make use of the expertise of the ITU to receive the proper assistance in the process of establishing national policies for cybersecurity within a well established international cooperation framework.

Meeting Closing

85. In his closing remarks on behalf of ITU, Marco Obiso, Advisor, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Bureau (BDT) said that he hoped that the three day ITU Regional Cybersecurity Forum for Europe and CIS had proven useful for the event participants. Mr. Obiso 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 a highly successful event. Mr. Obiso also thanked the forum speakers for taking time out of their busy schedules to share their experiences and expertise with the forum participants. ITU with its long standing activities in the standardization and development of telecommunications hopes to continue to provide a forum where the diverse views from governments, the private sector and other stakeholders related to cybersecurity and CIIP can be discussed through its different activities and initiatives.

The email address for comments on this meeting report[48] and for comments on the ITU Cybersecurity Work Programme to Assist Developing Countries (2007-2009)[49], is **cybmail(at)itu.int**[50].

For information sharing purposes, all meeting participants will be added to the **cybersecurity-europe-cis(at)itu.int**[51] for matters concerning ITU-D cybersecurity-related activities. If you have not participated directly in the event, or are not already on the mailing list but interested in participating in these discussions through the relevant mailing list and forum, please send an e-mail to **cybmail(at)itu.int**.

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

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

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

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