ITU Regional Cybersecurity Forum 2008
Sofia, Bulgaria

Document RFS/2008/OUT01-E
10 October 2008
Original: English

Summary of Forum Outputs and Possible Ways Forward[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. 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/.

At the conclusion of the Regional Cybersecurity Event some outcomes and recommendations for concrete action to be taken by countries in the region were identified. This included the need 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.
  - Cost effective technical solutions to perform forensics related activities.

[1] Available online at http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/sofia-cybersecurity-outputs-oct-08.pdf

- 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.