ITU Regional Cybersecurity Forum for Americas

- Connecting the World Responsibly -

Santo Domingo, Dominican Republic
23-25 November 2009

FORUM WRAP-UP

In concluding the **ITU Regional Cybersecurity Forum for Americas**, the participants highlighted the following. They:

- Recognized that **cybersecurity is a global issue** that requires cooperation across national borders. As such, measures at the national, regional as well as global levels are required to deal with the various aspects of cyber-threats to protect critical infrastructures.
- Emphasized that cybersecurity is increasingly important for countries in the Americas region, and governments need to be well informed and coordinated on this topic.
- Recognized the usefulness of the **ITU Global Cybersecurity Agenda (GCA)** as a mechanism and framework for international cooperation for cybersecurity and encouraged countries to undertake activities that relate to the five work areas of the GCA: 1. Legal Measures; 2. Technical and Procedural Measures; 3. Organizational Structures, 4. Capacity Building, and 5. International Cooperation, and share their experiences in implementing these initiatives on the national level with other countries in the region.
- Acknowledged the usefulness of the **Regional Cybersecurity Forum** as a platform for representatives from countries, regional and international organizations, to come together to discuss and elaborate on concrete steps to build cybersecurity capacity and competency in the region.
- Acknowledged that a **coordinated national response in cybersecurity** requires the participation of all relevant stakeholders and includes awareness and engagement at all levels. All different stakeholders have a role to play and government leadership in coordinating the national response is critical. In this regard, they encouraged countries in the region to actively share information and experiences, good practices and explore partnership opportunities for effective cybersecurity responses, and that the use of international standards should be promoted as a way to ensure interoperability between the diverse cybersecurity solutions being deployed. Only by working together to elaborate strategies, identify best practices, develop standards and implement concrete solutions, can the global challenges be addressed.
- Highlighted the need for **capacity building** across all different areas of cybersecurity and encouraged countries to incorporate initiatives on how to protect children online in their national cybersecurity efforts, and contribute to regional and global activities and initiatives, such as the ITU's Child Online Protection (COP) initiative.
- Noted that conducting a **national cybersecurity self-assessment** using existing tools and material such as the ITU National Cybersecurity/CIIP Self-Assessment Tool can be useful for countries to help identify where the different national parties are at with regards to cybersecurity **readiness** and preparedness, what they are doing, what they could do next and as a result identify practical steps forward on developing a national cybersecurity strategy.

- Committed to take action on **developing a national cybersecurity strategy** and ensure that international cooperation is taken into consideration in the development of the different national cybersecurity building blocks.
- Noted the need to share information and best practices amongst the countries in the area of **developing a legal framework and establishing effective enforcement.** Existing resources and tools like the ITU Understanding Cybercrime Guide and Toolkit for Cybercrime Legislation were mentioned as useful resources in this regard.
- Expressed the need to share information and assist one and other in **developing national watch and warning and incident management capabilities** and noted that in order to facilitate the development of cybersecurity capabilities, including the establishment of national CIRTs, the resources and services made available by the ITU in collaboration with key partners, such as the **International Multilateral Partnership Against Cyber Threats (IMPACT)**, governments and other stakeholders in the region such as existing national CSIRTs/CERTs/CIRTs, is useful. The work on security standards is an integral part of these efforts.
- Noted the **usefulness of the training provided at the Forum on three main topics**: developing a national cybersecurity strategy; building national watch, warning and incident response capabilities; and, developing legislation to criminalize the misuse of ICTs.

More details on the ITU Regional Cybersecurity Forum for Americas can be found on the website at: www.itu.int/ITU-D/cyb/events/2009/santo-domingo/