2009 ITU Regional Cybersecurity Forum for Americas

"Connecting the World Responsibly"

23-25 November 2009
Santo Domingo, Dominican Republic[1]

Draft Forum Agenda

Description: Information and communication technologies (ICTs) can play a decisive role in a country's development process. However, the rapid growth in the use of ICTs has also opened up new opportunities for criminals to exploit online vulnerabilities and attack countries' critical infrastructures. A fundamental role of ITU, following the World Summit on the Information Society (WSIS) and the 2006 ITU Plenipotentiary Conference, is to build confidence and security in the use of ICTs. Heads of states and government, and other global leaders participating in the WSIS as well as ITU Member States entrusted ITU to take concrete steps towards curbing the threats and insecurities related to the information society. For this reason, and in response to its role as facilitator for WSIS Action Line C5, on 17 May 2007, ITU launched the ITU Global Cybersecurity Agenda (GCA) to provide a framework within which the international response to the growing challenges to cybersecurity can be coordinated and addressed. More recently, the 2009 ITU Council endorsed ITU's activities related to building confidence and security in the use of ICTs .

Under the overall GCA framework, the 2009 ITU Regional Cybersecurity Forum for Americas dedicated to "Connecting the World Responsibly", aims to identify the main challenges faced by countries in the region in enhancing cybersecurity and securing critical information infrastructures, to consider best practices, and share information on cybersecurity development activities being undertaken by ITU as well as other entities to build cybersecurity capacity. The forum will also consider initiatives on the regional and international levels to increase cooperation and coordination amongst the different stakeholders.

MONDAY 23 NOVEMBER 2009	
08:30–09:30	**Meeting Registration and Badging (Online pre-registration required)**
09:30–10:00	**Meeting Opening and Welcoming Address**
	Welcome: Dario Cordero, Instituto Dominicano de las Telecomunicaciones (INDOTEL), Dominican Republic *Opening Remarks:* Dr. José Rafael Vargas, Secretary of State and President of Instituto Dominicano de las Telecomunicaciones (INDOTEL), Dominican Republic *Opening Remarks:* Juan Zavattiero, Head, ITU Americas Regional Office, International Telecommunication Union (ITU)
10:00–11:45	**Session 1: Setting The Stage — Towards an Integrated Approach for Cybersecurity and Critical Information Infrastructure Protection (CIIP)**
	Session Description: 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. The need to build confidence and security in the use of ICTs, promote

[1] See the ITU Regional Cybersecurity Forum for Americas website at: www.itu.int/ITU-D/cyb/events/2009/santo-domingo/

	cybersecurity and protect critical infrastructures at the national, regional and international level is generally acknowledged. The ITU Global Cybersecurity Agenda (GCA), provides a global approach to cybersecurity, where all relevant stakeholders can discuss and work together in order to best respond in a coordinated manner to the growing cybersecurity challenges. This session shares an overview of the current cyber-threat landscape and provides an insight into the challenges faced by countries, businesses and citizens in managing their every-day lives in this new and constantly changing environment. *Session Moderator:* Souheil Marine, Head, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Sector (ITU-D) *Presentation:* Souheil Marine, Head, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Sector (ITU-D), "An Overview of ITU Activities in the Area of Cybersecurity" *Presentation:* Graciela Piedras, Senior Telecommunications Specialist, Inter-American Telecommunication Commission (CITEL), Organization of American States (OAS) *Presentation:* Alberto Bolaña Wittenberger, Senior Consultant, Regional Programme Office in Panama (ROPAN), United Nations Organization for Drugs and Crime (UNODC), "Fortalecimiento de los equipos de investigación en las actividades de los Ministerios Públicos/ The strengthening of the investigation teams in the activities of the Public Ministries". *Presentation:* Jaime Ansieta, Criminal Intelligence Officer, Financial and High Tech Crime Sub-Directorate, Interpol
11:45–12:00	**Coffee/Tea Break**
12:00–13:30	**Session 2: Cybersecurity in the National Agenda and Actions to be Considered in Developing a National Cybersecurity Strategy**
	Session Description: Each country and region has its own requirements and needs that need to be addressed taking in consideration given the national and regional context. As national public and private sector actors bring their own perspective to the relevant importance of issues, in order to have a consistent approach, some countries have established cybersecurity/CIIP strategies while others have used a light-weight and non-institutional approach. What issues should be considered in a national strategy for cybersecurity and critical information infrastructure protection? Which actors should be involved? Considering the global nature of the challenges faced, how do these national initiatives and approaches fit into a global framework? This session will discuss some of the elements required to develop and organize national cybersecurity/CIIP efforts. The session will also introduce the ITU National Cybersecurity/CIIP Self Assessment Tool which is intended to assist national governments in elaborating a national approach for cybersecurity. *Session Moderator:* José A. Rizek, Telecommunications Advisor to the Executive Branch, Office of the President, Dominican Republic *Presentation:* Cesar Augusto Torres López, Director de Acceso y Desarrollo Social, Ministerio de Tecnologías de la Información y las Comunicaciones, Colombia *Presentation:* César Moliné Rodríguez, Asesor Legal en las áreas de Comercio Electrónico, Firma Digital, y Sociedad de la Información, Legal Counsel for Electronic Commerce, Digital Signature, and the Information Society, Instituto Dominicano de las Telecomunicaciones (INDOTEL), Dominican Republic *Presentation:* Belisario Contreras, Assistant Project Manager - Cyber Security, Inter-American Committee against Terrorism (CICTE), Organization of American States (OAS) *Presentation:* Joseph Richardson, Consultant to ITU, "Developing a National Cybersecurity/CIIP Strategy and ITU National Cybersecurity/CIIP Self-Assessment Tool"
13:30–14:30	**Lunch**
14:30–15:45	**Session 3: Defining Sound Organizational Structures and Developing Incident Management Capabilities**
	Session Description: A key activity for addressing cybersecurity requires the establishment of watch, warning and incident response capabilities to prepare for, detect, manage, and responding to cyber incidents. Effective incident management requires consideration of funding, human resources, training, technological capability, government and private sector collaboration, and legal requirements. This session discusses best practices, organizational structures and related standards in the technical, managerial and financial aspects of establishing national, regional and international watch, warning, and incident response capabilities. *Session Moderator:* Juan Antonio Delgado, Member of the Board of Directors, Instituto Dominicano

	de las Telecomunicaciones (INDOTEL), Dominican Republic *Presentation:* Michael Lewis, Consultant to ITU *Presentation:* Georges Sebek, Counsellor for ITU-T Study Group 17, ITU Telecommunication Standardization Sector (ITU-T) "Cybersecurity, ITU-T Standards and Initiatives: Implementation of ITU WTSA-08 Resolution 58 on the Creation of National Computer Incident Response Teams for Developing Countries" *Presentation:* Anuj Singh, Director, Global Response Center (GRC), International Multilateral Partnership for Cyber Threats (IMPACT)
15:45–16:00	**Coffee/Tea Break**
16:00–17:15	**Session 4: Capacity Building and International Cooperation**
	Session Description: The realities of cyberspace make it clear that everyone has to work together. Responding effectively to cyber-threats requires resources, know-how and strong investments on capacity developments. A key element is bringing together all relevant stakeholders to address the common cybersecurity challenges and develop solid capacity building plans. 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. World leaders at WSIS stressed the importance of security as a key pillar for a global information society and entrusted ITU to coordinate a global response to cybersecurity issues. With such a large number of relevant players and an ever increasing number of threats, how can we be effective in our collaboration towards a global strategy? This session looks closer at the possible mechanisms to build capacity in an effective manner, through collaboration and cooperation among all stakeholders at the national, regional and international level, for enhanced cybersecurity and for protecting children online *Session Moderator:* Souheil Marine, Head, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Sector (ITU-D) *Presentation:* Jorge Navarro, Consultant, Mexico *Presentation:* Souheil Marine, Head, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Sector (ITU-D), "An insight into ITU's Child Online Protection (COP) initiative" *Presentation:* María José Cantarino de Frías, Responsabilidad Corporativa, Corporate Responsibility, Telefónica, S.A. *Presentation:* Anuj Singh, Director, Global Response Center (GRC), International Multilateral Partnership for Cyber Threats (IMPACT) and Elina Noor, Senior Policy Analyst, Centre for Policy and International Cooperation, International Multilateral Partnership Against Cyber Threats (IMPACT)
17:15–17:30	**Daily Wrap-Up and Announcements**
19:00–	**Forum Welcome Cocktail Offered by Indotel**

TUESDAY 24 NOVEMBER 2009	
09:30–10:45	**Working Group Session 1: Developing A National Cybersecurity Strategy**
	Session Description: Each country needs a comprehensive national strategy and 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? Which actors should be involved? This working group session will look closer at the necessary components of such a national strategy and provide insights into what a possible strategy could look like. *Trainer:* Joseph Richardson, Consultant to ITU, "Developing a National Cybersecurity/CIIP Strategy and ITU National Cybersecurity/CIIP Self-Assessment Tool"
10:45–11:00	**Coffee/Tea Break**
11:00–12:45	**Working Group Session 1: Developing A National Cybersecurity Strategy (Continued)**
12:45–14:00	**Lunch**
14:00–15:30	**Working Group Session 2: Legal Measures on Cybersecurity**

	Session Description: Cyber criminals are an ever present menace in every country connected to the Internet. Organized crime has been on the rise because the Internet has proved a low risk, lucrative business. This is due to the fact that loopholes in national and regional legislation still remain, making it difficult to effectively track down criminals. The main problem is the lack of international harmonization regarding cybercrime legislation. Some efforts to address this challenge have been undertaken, and although very valuable, they are still insufficient. The Internet is an international communication tool and consequently, any solution to secure it must be sought at the global level. The purpose of this working group session is to provide countries in the region with a practical in-depth explanation of the different components needed for comprehensive legislation and effective to deter cybercrime and criminalize the misuse of ICTs. ITU has developed a comprehensive set of legal resources that serve to facilitate the discussions and the elaboration of cybersecurity related legislation. *Trainer:* Marco Gercke, Lecturer, University of Cologne, Germany, "ITU Publication on Understanding Cybercrime: A Guide for Developing Countries and the ITU Toolkit of Cybercrime Legislation"
15:30–15:45	**Coffee/Tea Break**
15:45–17:30	**Working Group Session 2: Legal Measures on Cybersecurity (Continued)**
17:30–17:45	**Daily Wrap-Up and Announcements**

WEDNESDAY 25 NOVEMBER 2009	
09:30–10:30	**Working Group Session 3: Implementing Organizational Structures and Incident Management Capabilities**
	Session Description: The purpose of the working group session is to elaborate on the requirements for establishing watch, warning and incident response capabilities to prepare for, detect, manage, and responding to cyber incidents. The working group session will discuss the ITU-IMPACT Global Response Center (GRC) and related assistance for building national watch, warning and incident response capabilities. The GRC can provide the global community with a real-time aggregated early warning system. This 'Network Early Warning System' (NEWS) can help Member States identify cyber-threats early on and provide critical guidance on what measures to take to mitigate them. Through the GRC members can gain access to specialized tools and systems, including the 'Electronically Secure Collaborative Application Platform for Experts' (ESCAPE). *Trainers:* Michael Lewis, Consultant to ITU and Anuj Singh, Director, Global Response Center (GRC), International Multilateral Partnership for Cyber Threats (IMPACT)
10:30–10:45	**Coffee/Tea Break**
10:45–11:45	**Working Group Session 3: Implementing Organizational Structures and Incident Management Capabilities (Continued)**
11:45–12:30	**Forum Wrap-Up, Recommendations and the Way Forward**
	Session Description: The final session of the forum reports some of the main findings from the event and tries to elaborate recommendations for future activities in order to enhance cybersecurity and increase the protection of critical information infrastructures in the region. *Closing Remarks:* Joelle Exarhakos, Executive Director, Instituto Dominicano de las Telecomunicaciones (INDOTEL), Dominican Republic *Closing Remarks:* Souheil Marine, Head, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Sector (ITU-D) *Closing Remarks:* Juan Zavattiero, Head, ITU Americas Regional Office, International Telecommunication Union (ITU)