International Telecommunication Union

Secretaría de COMUNICACIONES
MINISTERIO DE PLANIFICACION FEDERAL, INVERSION PUBLICA Y SERVICIOS

CNC COMISION NACIONAL DE COMUNICACIONES

Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP)

Document RWBA/2007/01-E
1 November 2007 Rev 1.0
Original: English

Meeting Report :
Regional Workshop on Frameworks for Cybersecurity and CIIP
Buenos Aires, Argentina, 16-18 October 2007

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

Purpose of this Report

1. The ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP) was held in Buenos Aires, Argentina, 16-18 October 2007[1]. The workshop is one of a series of regional cybersecurity awareness and capacity-building events jointly organized by the ITU Telecommunication Development Sector (ITU-D) and ITU Telecommunication Standardization Sector (ITU-T). The workshop aimed to identify the main challenges faced by countries in the Americas region in developing frameworks and national strategies for cybersecurity and CIIP, to consider best practices, share information on technical standards and development activities being undertaken by ITU as well as other entities, and review the role of various actors in promoting a culture of cybersecurity.

2. Approximately 60 people participated in the event, from countries in the Americas region as well as from other parts of the world. Full documentation of the workshop, including the final agenda and all presentations made, is available on the event website at www.itu.int/itu-d/cyb/events/2007/buenos-aires/. This meeting report summarizes the discussions throughout the three days, provides a high-level overview of the sessions and speaker presentations, and presents some of the common understandings and positions reached at the event.

Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection held in Buenos Aires, Argentina, 16-18 October 2007

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 requires a comprehensive approach. This event discussed some of the key elements in developing such frameworks.

Meeting Opening and Welcome

4. The Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection was opened with a welcoming address by Gonzalo Heredia, Coordinator for National Information Society Programs, on behalf of Carlos Lisandro Salas, Secretarío de Comunicaciones, from the Secretaría de Comunicaciones, Argentina. In his opening remarks, Mr. Heredia stated that cybersecurity and critical information infrastructure protection are very important challenges to the Information Society that cannot be answered without concrete action. He noted that in Argentina, the use of ICTs is increasing rapidly and therefore more focus should be placed on the issues related to Internet security. Everyone, security experts and users alike, need to better understand what is at stake, and what can be done about it. With this he invited the workshop participants to engage in fruitful and focused discussion during the three day event.

[1] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/

5. This welcoming address by the Secretaría de Comunicaciones was followed by opening remarks[2] [3] made by ITU's Mario Maniewicz, Chief a.i., Policies and Strategies Department, Telecommunication Development Bureau, on behalf of ITU-D Director Sami Al-Basheer and ITU-T Director Malcolm Johnson. In his opening remarks, Mr. Maniewicz noted that this workshop presents an excellent opportunity to share experiences and best practices for addressing the challenges faced by countries in the Americas region when developing related frameworks and strategies. He noted that the workshop also provided an opportunity to increase awareness on relevant ITU-T Recommendations and ongoing cybersecurity-related activities in the ITU Telecommunication Development and Standardization Sectors. Mr. Maniewicz thanked Argentina for their particularly active interest in the activities of ITU on cybersecurity and mentioned that it was Argentina who immediately volunteered to play host to such an event in the Latin American region when plans for such a workshop were first announced.

6. Mr. Maniewicz noted the excellent line up of experts and speakers at the workshop, and invited all participants to take advantage of the presence of these experts as well as counterparts from countries in the Americas and other regions, to actively participate in all sessions of the workshop by sharing views and experiences, and to raise any questions or issues participants may have on the topics discussed. He noted that the active participation and contribution of the workshop participants is what will ultimately contribute to the success of the event.

Session 1: What is a Framework for Cybersecurity and Critical Information Infrastructure Protection?

7. 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 and non-institutional approach. This session discussed the concept of a national framework for cybersecurity and CIIP and ongoing efforts to elaborate such a best practices framework in the ITU.

8. Robert Shaw, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Sector (ITU-D) acted as the moderator for this session which sought to review, from a broad perspective, different approaches to cybersecurity and CIIP frameworks and their often similar components in order to provide meeting participants with an overview of the issues and challenges involved. Mr. Shaw provided an overview of "ITU-D's Activities in the Area of Cybersecurity and CIIP"[4] and shared details on the ITU-D Cybersecurity Work Programme to Assist Developing Countries (2007-2009)[5]. Some of the ongoing and planned ITU cybersecurity initiatives mentioned included: activities dealing with the identification of best practices in the establishment of national frameworks for cybersecurity and CIIP; a national cybersecurity/CIIP readiness self-assessment toolkit; 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 workshops for awareness raising and capacity building on frameworks for cybersecurity and CIIP.

9. Mr. Shaw noted that most countries have not yet formulated or implemented a national strategy for cybersecurity and critical information infrastructure protection and that with limited human, institutional and financial resources, developing countries face particular challenges in elaborating and implementing such policies. He noted that the ITU Telecommunication Development Sector has a Study Group currently developing a best practices document containing a proposed framework for national cybersecurity efforts which is closely tied to the ITU-D's *Cybersecurity Work Programme to Assist Developing Countries*. This *Work Programme* scopes out how ITU plans to assist countries in developing cybersecurity/CIIP capacity, through, *inter alia*, providing Member States with useful resources and toolkits on related subjects. As the toolkits become more stable, the ITU-D is looking to disseminate them widely through multiple channels to ITU 191 Member States. Mr. Shaw mentioned that one challenge in moving forward on discussions relating to cybersecurity was finding appropriate mechanisms for the different actors to better communicate with each other, given that each group of actors often have different and specific requirements as to the levels of trust needed to share specific information.

10. Daniel Hurley, Department of Commerce, National Telecommunications and Information Administration (NTIA), United States of America, followed with an overview of the work on a *Framework for National Cybersecurity Efforts* that is currently being developed in ITU-D Study Group 1 Question 22 with his presentation on "Building Cybersecurity Capacity: Overview of Best Practices for Cybersecurity"[6]. The framework is one of the components of the work conducted in the Study Group which has been proposed in a report on *Best Practices for Organizing National Cybersecurity Efforts* which governments can use as a guideline when undertaking national strategies for cybersecurity and CIIP. The *Framework for National Cybersecurity Efforts* looks at five main components for best practices in cybersecurity, namely: developing a National Strategy for Cybersecurity; Government-Industry Collaboration; Deterring Cybercrime; National Incident Management Capabilities; and, a

[2] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/opening-remarks-itu-buenos-aires-16-oct-07.pdf

[3] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/opening-remarks-itu-buenos-aires-16-oct-07-s.pdf (Español)

[4] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/shaw-itu-d-cybersecurity-overview-buenos-aires-oct-07.pdf

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

[6] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/hurley-building-cybersecurity-capacity-buenos-aires-oct-07.pdf

National Culture of Cybersecurity. The draft report includes a policy statement for each component of the framework, identifies goals and specific steps to reach these goals, and references and material related to each specific step. The *Best Practices for Organizing National Cybersecurity Efforts* report, including the framework, is a living document and it will evolve over time. Mr. Hurley emphasized the importance of having overall coordination of any national cybersecurity program established at the very highest level in national governments in order to be effective. Mr. Hurley closed his presentation by mentioning the useful appendices and annexes available in the *ITU-D Study Group Question 22/1 Draft Report on Best Practices for Cybersecurity*[7] which is available on the ITU-D website.

11. Phil Sodoma, Trustworthy Computing Group, Microsoft Corporation followed with a presentation entitled "Resiliency Rules: 7 Steps for Resiliency in Critical Infrastructure Protection"[8]. The purpose of the Resiliency Rules approach presented is to provide a set of elements of best practices from different regions in the world that governments have adopted. With these guiding principles in mind, government, infrastructure owners/operators can collaboratively pursue a set of core enablers of resiliency and infrastructure.

12. The 7 Steps include: 1) Define goals and roles. Establishing clear goals is central to generate support for cybersecurity by the different stakeholder groups while understanding the different roles of the stakeholders promotes coordination, efficiency and trust. 2) Identify and prioritize critical functions. Close collaboration is needed to understand interdependencies involved. Mr. Sodoma encouraged countries to establish an open dialogue to understand the critical functions, infrastructure elements, and key resources necessary for delivering essential services, maintaining the orderly operations of the economy, and helping to ensure public safety. 3) Continuously assess and manage risks as protection is the continuous application of risk management. 4) Establish and exercise emergency plans and improve operational coordination. Emergency response plans can mitigate damage and promote resiliency. 5) Create public-private partnerships. Mr. Sodoma explained why the importance of public-private partnerships should not be underestimated. The creation of trusted relationships is key to information sharing and developing solutions to difficult problems and leveraging the unique skills of government and private sector organizations are necessary to address today's dynamic threat environment. 6) Build security/resiliency into operations as security is a continuous process 7) Update and innovate technology/processes. While cyber threats are constantly evolving policy makers, enterprise owners, infrastructure operators can still prepare for and mitigate these threats by keeping the technologies they are using current and up-to-date.

13. Mr. Sodoma also shared with the participants what he saw as potential barriers to implementing a national cybersecurity/CIIP strategy and program. These included perceived economic barriers, the natural transition time necessary to secure infrastructures, citing the examples of airplanes and air traffic control, where with experience gained, we eventually learned how to prevent airplanes from falling out of the sky, and the necessity to engage sometimes in what could be called "security theater" to raise political awareness of risks and the necessity to undertake measures to mitigate them. Mr. Sodoma also noted that the lack of cooperation between countries and also within nations, is a major barrier, if not the main barrier, to successfully implementing a national cybersecurity/CIIP strategy and program. He stressed that the only way to get things moving towards enhanced cybersecurity is to break down the barriers and communicate across government agencies.

14. Mr. Sodoma also mentioned that many countries lack the knowledge of what to do, and how to proceed from where they are, given their specific situation, and highlighted that the ITU National Cybersecurity/CIIP Self Assessment toolkit as an excellent way to approach the problem. He furthermore indicated that a role of the government is risk assessment, the role of the public-private partnership is to define what is critical, and the role of infrastructure operators is to prioritize risks. Mr. Sodoma ended his presentation by noting that in the past, security in enterprises was seen as a technology issue, but that this has changed over the past few years, and it is now widely recognized that a more comprehensive, multi-layered security approach is necessary. He also noted that software created 10 years ago was not created for the current threat environment. Therefore, it is important to always use the latest version of available software and hardware.

Session 2: Development of a National Strategy

15. Increasingly, electronic networks are being used for criminal purposes, or for objectives that can harm the integrity of critical infrastructure and create barriers to 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 that countries can adopt? This session, moderated by Gonzalo Heredia, Coordinator for National Information Society Programs, Secretaría de Comunicaciones, Argentina, sought to explore in more detail various approaches and best practices, and identify key building blocks that could assist countries in the Americas region in establishing national strategies for cybersecurity and CIIP.

16. In the first presentation in Session 2, Development of a National Strategy, Carlos Achiary, Director of the Oficina Nacional de Tecnologías de Información (ONTI), Subsecretaría de la Gestión Pública, Argentina, in his

[7] http://www.itu.int/md/D06-SG01-C-0130/en

[8] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/sodoma-resiliency-rules-buenos-aires-oct-07.pdf

presentation on the development of a national strategy "Desarrollo de una Estrategia Nacional",[9] shared some insights into the challenges involved in developing a national strategy for cybersecurity and CIIP, with specific examples from Argentina and the region. He noted that cyberspace today is a field for new actions; some legal while others are not, and that citizens, private companies, organizations, and governments alike are finding new ways to leverage ICTs. Because of this, governments have an increasingly important role to play in making cyberspace a safer and more reliable place. Mr. Achiary talked about some of the main areas that Argentina is focusing on in order to develop a comprehensive national strategy for cybersecurity. He acknowledged the importance of good cooperation and coordination between the national agencies involved, and once the country is well organized internally on the national level, the importance of the international cooperation aspect of dealing with threats, building response capacity, etc. should not be underestimated. This should include communication between public and private sector players and citizens internally in a country, but with the government playing a key coordinating role.

17. In his update on what is currently happening in Argentina, he noted that the country is still at an early stage and is now assessing what further measures need to be taken in both the short and long term. There needs to be a change in legislation at some point, and this is the responsibility of the government. The government is also often the main representative of the country in international fora. He mentioned that Oficina Nacional de Tecnologías de Información (ONTI), the national office for ICTs, has a coordinating role in this effort. He also mentioned that ArCERT is the only computer security incident response team (CSIRT)/computer emergency response team (CERT) in Argentina and was established already in 1999. ArCERT is responsible for the federal public sector, but is often asked to assist other government sectors and the private sector. However, he noted that ArCERT is not officially a national CERT. In addition to engaging in international cooperation activities under the OAS framework and providing representation at ITU cybersecurity efforts, other regional contacts have also been established. He also mentioned that Argentina has developed a model cybersecurity policy, and currently has a cybercrime bill in congress, which, if passed, will lead to a change in the Argentine criminal code. He said Argentina was looking forward to increasing cybersecurity collaboration in all areas and playing an active role in the ITU cybersecurity workshop.

18. Bradford Willke, CERT/CC, Software Engineering Institute (SEI), United States of America, started his presentation on "Engineering National Cybersecurity and Critical Information Infrastructure Protection"[10] by looking at some of the national and multi-national cybersecurity impediments. He mentioned that when it comes to goal orientation, cybersecurity, business continuity, and ICT operations support critical information infrastructure protection (i.e., provide elements of resiliency), but are often performed independently of one another. On the other hand, when looking at problem recognition, the field of cybersecurity and CIIP tends to be focused on technical rather than managerial solutions and therefore a true process-orientated approach remains elusive. Therefore, he believed that nations have a false sense of preparedness, and this preparedness is actually only tested during disruptive events. Furthermore, while codes of practice are numerous, practice effectiveness is rarely measured. Overall, Mr. Willke stated that there are few reliable benchmarks for determining a nation's capability for protecting critical information infrastructures.

19. When countries are getting ready to start developing a national strategy and program for cybersecurity and CIIP, self-assessment against a common framework provides a good place to start. Critical questions at this stage include having a good understanding of the following: "What is the route? (Is there a framework to follow?)", "What is the destination? (How far must the framework be implemented?)", and "Where are we? (How far has the country come in implementing the framework?)". Mr. Willke noted that the "destination" is determined by the capabilities and the maturity of processes that a country must have in place to manage unacceptable risks. In addition, for true process improvement to take place, there needs to be clear procedures to engage with the communities that are experts in this area. In that regard, countries need to have a better understanding of how it might respond under stress and under attack, how mature they are in their response and the culture involved. A repeatable process that the nation can apply, together with the tools to measure how well they are doing against risk management, is also important. Mr. Willke noted that each nation's approach will be different, because countries have different goals, objectives and different sectors which are seen as critical. He said that "Lessons learned" from a negative event is not the best way to learn but if this happens it can result in a good learning experience from both a policy and management perspective. In particular, "What is needed the next time" needs to be considered. He ended his presentation by mentioning that there are all sizes and shapes of frameworks and the best way to start is by identifying the framework that will best suit the country's specific needs.

20. Fred Clark, Superintendencia de Telecomunicaciones, Guatemala, followed with a country case study on "E-Readiness in Guatemala"[11]. In his presentation he shared information with the delegates on the current situation in Guatemala and how the uptake of ICTs in people's everyday lives is gradually transforming society. Mr. Clark gave examples from a recent 2007 e-Readiness study for Guatemala and linked these to the growing

[9] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/achiary-argentina-national-cybersecurity-strategy-buenos-aires-oct-07.pdf

[10] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/willke-ciip-buenos-aires-oct-07.pdf

[11] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/clark-e-Readiness-guatemala-buenos-aires-oct-07.pdf

need for enhanced awareness of the threats to users and businesses online caused by an increasingly insecure cyberspace.

21. Building on the presentations made in the two workshop sessions showcasing frameworks for cybersecurity and CIIP and different national strategies and approaches, Joseph Richardson, United States of America, described the elements of the ongoing ITU work to develop a comprehensive National Cybersecurity/CIIP Readiness Self Assessment Toolkit[12] with his presentation on "Management Framework for Organizing National Cybersecurity Efforts: Self-Assessment Tool"[13]. Representing one of the key synergies between ITU-D Study Group Q22/1 work on "Securing information and communication networks: Best practices for developing a culture of cybersecurity"[14] and the ITU Cybersecurity Work Programme to Assist Developing Countries (2007-2009)[15] activities, the ITU National Cybersecurity/CIIP Self-Assessment Toolkit applies the framework under development in the Study Group with a practical toolkit for consideration at the national level. The toolkit 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 response efforts. The toolkit addresses the management and policy level for each of the five elements of the best practices framework that was presented by Mr. Hurley in Session 1 of the workshop, namely: 1) national strategy; 2) deterring cybercrime; 3) national incident management capabilities; 4) government-private sector collaboration; and, 5) a culture of cybersecurity, the necessary institutions, as well as the relationships among government, industry and other private-sector entities.

22. Mr. Richardson noted that no country is starting at zero when it comes to initiatives for cybersecurity and critical information infrastructure protection. Furthermore, there is no one right answer or approach as all countries have unique national requirements and desires. A continual review and revision is needed of any approach taken, and it is equally important to involve all stakeholders, appropriate to their roles, in developing a national strategy for cybersecurity and CIIP. Mr. Richardson mentioned that updates to the toolkit and related resources are continuously updated through the ITU-D cybersecurity website (www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html), and country pilot projects to test and evaluate the toolkit are being undertaken in conjunction with a number of regional capacity-building workshops organized by ITU in 2007, 2008, and 2009.At the end of the first day of the workshop the workshop participants and local organizers were invited to a cocktail sponsored by CISCO.

Session 3: Technical Standards for Cybersecurity

23. Standards-development bodies are important players in addressing security vulnerabilities in ICTs. Session 3 of the workshop, moderated by Paolo Rosa, Workshops and Promotion Division, ITU Telecommunication Standardization Sector (ITU-T), highlighted some of the main activities of standards development organizations (SDOs), focusing on ITU-T, and considering topics such as security architecture, cybersecurity, security management, identity management, security baseline for network operators, and the ICT Security Standards Roadmap initiated by ITU-T Study Group

24. Mr. Rosa opened the standards discussions with a presentation on "ITU-T: Cybersecurity and Standards"[16] providing an overview of the ITU-T structure and relevant security activities. Mr. Rosa explained the importance of the work conducted in the ITU-T Study Groups, how this fits in with ITU's overall work, and highlighted some activities of ITU-T Study Group 17, which is the main ITU-T Study Group for security. The ITU-T security building blocks which include the X.800-series (Security Architecture Framework), X.805, X.1000-series (Telecommunication Security), Y.2700-series (NGN Security), etc. were also explained. Mr. Rosa also mentioned some of the security and identity management-related activities that have been undertaken by the ITU-T Focus Group on Identity Management (IdM)[17]. To date, the Focus Group has developed four main reports, including: one identifying requirements based on case scenarios; another identifying generic IdM framework components; a standards gap analysis to identify new standards work that ITU-T Study Groups and other SDOs should undertake; and a "living list" of relevant bodies dealing with IdM.

25. Mike Harrop, Rapporteur on ITU-T Study Group 17's Communications Security Project, gave the workshop participants further insight into "ITU-T Network Security Initiatives"[18]. He showed how the ITU-T security standards activities fit in to the larger security standards arena, highlighting some of key areas of work in SG 17 Working Party 2 and SG 13 Question 15, and reported on the results achieved through specific SG 17 security projects and outreach activities. For example, the ITU-T Security in Telecommunications and Information Technology Manual[19] provides an overview of existing ITU-T recommendations for secure telecommunications.

[12] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html
[13] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/richardson-national-cybersecurity-ciip-self-assessment-buenos-aires-oct-07.pdf
[14] http://www.itu.int/ITU-D/cyb/cybersecurity/index.html
[15] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf
[16] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/rosa-itu-t-cybersecurity-and-standards-buenos-aires-oct-07.pdf
[17] http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html
[18] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/harrop-itu-t-network-security-buenos-aires-oct-07.pdf
[19] http://www.itu.int/pub/T-HDB-SEC.03-2006/en

The Security Compendium[20] is a catalogue of approved ITU-T Recommendations related to telecommunication security. The newly released Security Standards Roadmap[21] (v.2, 2007) is an online security standards resource which has been developed by ITU in collaboration with the European Network and Information Security Agency (ENISA) and the Network and Information Security Steering Group (NISSG). The Roadmap comprises five parts: Part 1 contains information about organizations working on ICT security standards; Part 2 is a database of existing security standards; Part 3 lists (or links to) current projects and standards in development; Part 4 identifies future needs and proposed new standards; and Part 5 lists security best practices. Mr. Harrop also mentioned that Study Group 17 is currently establishing a Security Standards Exchange Network (SSEN) to maintain on-going dialogue on key security standardization issues.

Session 4: Watch, Warning and Incident Response

26. 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. This first session on the second day of the workshop was moderated by Romulo Dantas, Inter-American Committee against Terrorism (CICTE) of the Organization of American States and discussed best practices and related standards for the technical, managerial and financial aspects of establishing national or regional watch, warning, and incident response capabilities.

27. Jason Rafail, CERT/CC, Software Engineering Institute (SEI), Carnegie Mellon University, United States of America, opened the session his presentation providing an "Overview of the CERT/CC and CSIRT Community"[22]. He emphasized that countries need to ensure that accessibility and sustainability is maintained during an attack on national infrastructure, and national CSIRTs have an important role to play in this regard. Being proactive and building a culture of security are key to protecting national information infrastructure. Promoting the creation of national CSIRTs is part of a solution on the national level. National CSIRTs provide a conduit for communications and coordination and a goal could be to establish at least one coordinating CSIRT in every country. There are currently around 40 national CSIRTs around the world. Services that the national CSIRTs provide include technical services (such as coordination, alerting services, technical publications, incident analysis, vulnerability analysis, artifact analysis, forensic analysis, training, etc.) and non-technical services (such as alerting services, user focused publications, general security and computing information). Mr. Rafail described why partnerships are needed for successful response and prevention of incidents.

28. All parties and stakeholders involved need to better understand how the use of information and communication technologies is impacting their everyday business activities. While highlighting that people need to have access and knowledge about available security tools, Mr. Rafail also shared information on some online security training resources and tools that the participants could take back with them to countries. These included: the Virtual Training Environment (VTE)[23] which is a library of information assurance and computer forensics best practices, Secure Coding Training[24] resources targeted at enhancing developer skills and capabilities.

29. Ricardo Woolery, CONATEL, Honduras in his presentation "Honduras - An Overview"[25] provided some general information on the development of ICTs in Honduras as well as an insight into the current status of security in three different sectors of the economy: government, academic institutions and schools, and financial institutions. He mentioned that CONATEL, the National Telecommunications Commission, as the telecoms regulator, requires that each operator implements security mechanisms in their networks. Each government agency also has an IT strategy to protect their networks. When looking at the academic institutions in the country, the universities have established their own networks to offer services (such as academic portals, electronic libraries, administrative services, access points, etc.) and security has been made a key component in most, if not all of these. With regard to financial institutions, some banks have certified their networks, and measures are being put in place to protect customers' bank accounts. Overall though, Mr. Woolery noted, a clear unifying cybersecurity strategy or framework that would allow for consensus on policies at the national and sectoral levels for the country was still missing.

30. The next presentation was given by Gastón Franco, ArCERT, Oficina Nacional de Tecnologías de Información (ONTI), Argentina, who provided an insight into the mandate and activities of "ArCERT"[26], as the first and only CSIRT in Argentina. Mr. Franco also mentioned that ArCERT has been appointed to CICTE as the national cybersecurity contact, and is an active promoter of building additional CSIRT capabilities in Argentina as well as

[20] http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D0000090001MSWE.doc
[21] http://www.itu.int/ITU-T/studygroups/com17/ict/
[22] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/rafail-buenos-aires-oct-07.pdf
[23] http://www.vte.cert.org/
[24] http://www.cert.org/secure-coding/
[25] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/woolery-honduras-overview-buenos-aires-oct-07.pdf
[26] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/franco-arCERT-buenos-aires-oct-07.pdf

in other countries in the region. The team is also actively participating in related international fora for incident handling and response. The main preventive activities undertaken by ArCERT include providing training, policy advice, alerts and information dissemination, and other related security-related services and products. Mr. Franco described a few cases of phishing in Argentina that ArCERT have handled to allow meeting participants to better understand their activities. For example, based on the information gathered for a phishing site, a CSIRT can see how many ISPs and users have accessed the site.

Session 5: Watch, Warning and Incident Response

31. The discussions related to Watch, Warning and Incident Response continued in Session 5 with Marcelo HP Caetano Chaves, CERT-br, Brazil, and his presentation on "Using Honeypots to Monitor Spam and Attack Trends"[27] where he shared information on some of the ongoing CERT-br projects and research. As an example, he showed what had been done by his team to understand whether Brazil really is as big a source of spam as stated by the media, or whether Brazil was just being targeted as a platform for attacks. He shared details on the Brazilian Honeypots Alliance Distributed Honeypots Project[28] which aims to increase the capacity of incident detection, event correlation and trend analysis in the Brazilian Internet. He also shared details on the Brazilian SpamPots Project which uses honeypots to measure abuse of end-user machines to send spam. Some upcoming activities for CERT-BR include developing more comprehensive spam analysis using data mining techniques, determining patterns in language, embedded URLs, etc., and a project to propose best practices for ISPs including port 25 management and proxy abuse monitoring. Mr. Chaves emphasized that international cooperation is also high on CERT-br's agenda.

32. Fred Clark, Superintendencia de Telecomunicaciones, Guatemala, presentad on the Guatemala CSIRT CSIRT-gt, "CSIRT-gt: El Equipo de Respuesta a Incidentes de Seguridad Informática de Guatemala"[29]. Guatemala is currently in the process of establishing a national CSIRT and Mr. Clark shared information on why a national CSIRT is urgently needed also in Guatemala. The role of the CSIRT is to train and prepare Guatemalans to protect Guatemala's assets. Challenges faced by the CSIRT-gt to date includes enabling 24/7 availability and ensuring that the team is properly trained and equipped to help guarantee security in the national networks.

33. Mr. Clark mentioned that the initiative to establish CSIRT-gt came from a recommendation from CICTE. There are currently four people working at the CSIRT and the team is currently looking for new ways to get further funding for its operations. Ultimately, the CSIRT would be able to become self-sufficient, however, some creative ideas are needed to find ways for the CSIRT to generate money from its activities and services provided. It is also interesting to note that the people currently running the CSIRT received a lot of their training from CERT-br in Brazil, showing the importance of regional and international cooperation in all different cybersecurity related areas.

34. Suresh Ramasubramanian, Outblaze, India, shared information on the "ITU Botnet Mitigation Toolkit Project". In his presentation Mr. Ramasubramanian explained what people are able to do with botnets, in addition to sending spam ,as had been mentioned in earlier presentations: Examples included the attack on a country's Internet infrastructure, extortion, such as threats to launch denial of service attacks to cripple e-commerce websites, identity theft and industrial espionage, theft of credit card information, passwords etc. from infected personal computers (PCs), and/or launch stock pump-and-dump scams. He talked about the underground economy that has sprung up around botnets, yielding significant revenues for authors of computer viruses, botnet controllers and criminals who commission this illegal activity by renting botnets. Pointing out that the threat from botnets is growing fast. The latest generation of botnets (such as Zhelatin/Storm Worm), uses particularly aggressive techniques such as fast-flux networks and DDoS attacks against security vendors trying to mitigate them.

35. In response to this, ITU has an ongoing project to develop a *Botnet Mitigation Toolkit*[30] to help deal with the growing problem of botnets. The Botnet Mitigation Toolkit is a multi-stakeholder, multi-pronged approach to track botnets and mitigate their impact, with a particular emphasis on the problems specific to emerging Internet economies. The toolkit draws on existing resources, identifies relevant local and international stakeholders and takes into account the specific constraints of developing economies. The toolkit seeks to raise awareness among Member States of the growing threats posed by botnets and their linkages with criminal activities and incorporates the policy, technical and social aspects of mitigating the impact of botnets. The first draft of the toolkit will be made available in December 2007 with pilot tests planned in a number of ITU Member States in 2008.

Session 6: The Role of CSIRTs in Promoting a Culture of Cybersecurity

36. Considering that personal computers and mobile phones are becoming ever more powerful technologies and converging, the use of ICTs is becoming more and more widespread, and that connections across national borders are increasing, all participants who develop, own, provide, manage, service and maintain information networks must understand cybersecurity issues and take action appropriate to their roles to protect networks.

[27] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/chaves-certbr-buenos-aires-oct-07.pdf
[28] http://www.honeypots-alliance.org.br/
[29] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/clark-CSIRT-guatemala-buenos-aires-oct-07.pdf
[30] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html

This session, explored the concept of promoting a culture of cybersecurity, and took a closer look at some of the roles of the different stakeholders, especially the role of CSIRTs, in making this a reality.

37. Christine Sund, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Sector (ITU-D), in her presentation on "Promoting a Culture of Cybersecurity"[31] provided an overview of what a culture of cybersecurity means and what could be some of the possible roles of different stakeholders in the Information Society in creating a global culture of cybersecurity. She highlighted nine elements for creating a culture of cybersecurity as stated 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 elements included awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment. Member States and all relevant international organizations were asked to address and take these elements into account in the preparation for the two phases on the World Summit on the Information Society (WSIS)[32] in 2003 and 2005. The outcome documents from the two WSIS phases furthered emphasized the importance of building confidence and security in the use of ICTs and countries' commitment to promoting a culture of security.

38. Ms. Sund's presentation mentioned some possible roles for governments in promoting a culture of cybersecurity, including: ensuring that a nation's citizens are protected; 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; to curb abuses and to protect consumer rights; and to lead national, regional, and international cybersecurity cooperation activities. Ms. Sund emphasized that as ICT infrastructures are, for the most part, owned and operated by the private sector, their involvement in promoting a national and global culture of cybersecurity is crucial. Effective cybersecurity needs an in-depth understanding of all aspects of ICT networks, and therefore the private sector's expertise and involvement are paramount in the development and implementation of national cybersecurity strategies. Furthermore, Ms. Sund highlighted that governments and businesses need to assist citizens to obtain information on how to protect themselves online. With the right tools readily accessible, each participant in the Information Society is responsible for being alert and protecting themselves, noting though that cybersecurity at its core is a shared responsibility.

39. Two panellists, Bradford Willke, CERT/CC Software Engineering Institute (SEI), United States of America and Patricia Prandini, ArCERT, Argentina then provided their insights on the subject. Mr. Willke with his presentation on "CSIRT Contributions to National Efforts in Critical Information Infrastructure Protection"[33] examined some best practices pervasive in CIIP frameworks related to CSIRTs, common intersections of CSIRT-to-CIIP activities, benefits of planning or scoping of CSIRT-to-CIIP activities and multi-national event coordination under a CIIP framework. Mr. Willke mentioned some of the CSIRT activities that he considered closely linked to national critical information infrastructure protection. These CSIRT responsibilities include developing and sustaining an understanding of national cybersecurity environment, i.e. threats, vulnerabilities, risks, capabilities, and sensitivities involved; creating metrics to quantify understanding of these threats; tracking the state of cybersecurity over time; assisting critical information infrastructure providers and government regulatory bodies in identifying and addressing information security vulnerabilities and threats; disseminating "lessons learned" from analysis of the cyber environment and information gained from the various sectors to expand and improve the overall state of security within the nation; and liaising with law enforcement, regulators, subject matter experts, etc. on technical solutions and implications. Mr. Willke also highlighted that any international cybersecurity goals would benefit largely by facilitation done through and/or by CSIRTs. Activities where CSIRTs could expand their activities include to: identify experts and resources needed; coordinate the vendor and service provider communities on technical and procedural solutions and remedies; coordinate within management frameworks (such as critical infrastructure protection (CIP) programmes, national emergency response plans, etc.; advise government and industry on steps to take, and actions not to take; and maybe participate in planning, design, implementation, operation, and reconstitution processes with the partners.

40. Patricia Prandini, ArCERT[34], Argentina talked about the specific role of the CSIRT "Rol de los CSIRTs"[35] by first looking at what tasks the CSIRT should undertake. Activities she mentioned included: to produce technical materials and initiate training programs to enable responsible use of ICTs, contribute to the formulation of standards and best practices in computer security, provide unique services by being able to identify priority groups and thematic interest, and deepen awareness of the groups that provide need services. Furthermore, she mentioned that CSIRTs can help improve daily national operations and minimize the occurrence of cyber incidents. Ms. Prandini also shared information on some of the cybersecurity awareness raising initiatives that are currently taking place in the region, such as COLARIS (Conferencia Latino Americana de Respuesta a Incidentes de Seguridad) which organizes transit courses, security workshops, and the FIRST-TC meetings. She also mentioned that CICTE (Comité Interamericano contra el Terrorismo) and OAS have initiatives that

[31] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/sund-promoting-a-culture-of-cybersecurity-buenos-aires-oct-07.pdf

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

[33] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/willke-role-of-csirts-buenos-aires-oct-07.pdf

[34] http://www.arcert.gov.ar

[35] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/prandini-rol-de-los-CSIRTs-buenos-aires-oct-07.pdf

incorporate IT security into regional meetings and events, as well as coordination of some regional CSIRT activities. For example, LACNIC has provided capacity building training of CSIRT personnel along with other coordinating activities. Ms. Prandini also shared information on some of the national Argentinean awareness raising initiatives that have been implemented and others planned for the future.

Session 7: Legal Foundation, Regulatory Development and Enforcement

41. Appropriate 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 law, procedures and policy to address cybersecurity incidents and respond to cybercrime. As a result, many countries have made amendments to their penal codes, or are in the process of adopting amendments, in accordance with international conventions and recommendations. Sessions 7 and 8 of the workshop reviewed various national legal approaches and potential areas for international legal coordination and enforcement efforts. The Session 7 moderator, Marco Gercke, Germany opened the session with an insight into what is currently happening in the international community with regard to revising existing laws and developing new legislation to deal with citizens' increasing use of information and communication technologies.

42. The first presentation was delivered by Albert Rees, Computer Crime and Intellectual Property Section (CCIPS), Department of Justice, United States of America. He started his presentation on "Legal Foundation"[36], by asking generally how countries can successfully investigate, prosecute, and convict people who use computers and the Internet to commit crimes. He noted that the goals of the various cybersecurity stakeholders may be different, but it is nonetheless important to work together on fighting cybercrime as it impacts and affects everyone and every country. It does not matter at what stage of development the country is, every country is affected in one way or another. A critical component of any national response taken is communication and cooperation, this within government, with the private sector, and internationally. Mr. Rees mentioned three main things that countries can do to combat cybercrime which included: 1) ensuring that there are adequate cybercrime and related laws in place, 2) putting into place and educating specialized law enforcement who understand technology and laws in the country and how these fit together, and 3) connecting and sharing information with other countries.

43. Mr. Rees highlighted the need to ensure that the legislative cybercrime framework established in any country must be tailored to meeting the domestic goals, so that the laws and legislations meet the special requirements of that country. However, at the same time, due to the global nature of cybercrime as the Internet has no direct national border, the laws established need to facilitate international collaboration – and as a result national cybercrime laws need to be compatible with those in other countries as much as possible. The Council of Europe Convention on Cybercrime sets forth a framework for the type of laws that are needed. For example, as the legal system in the United States is very different from that in Bolivia, what the Convention does is it provides a framework that all countries can consider when establishing their laws. There are also resources available from a number of sources that can assist countries with drafting of legislation in this regard. In the Americas region, OAS and REMJA have endorsed the Convention on Cybercrime. Originally the REMJA group suggested that looking at a regional framework was preferred, but now the group is looking closer at using the Convention and possibly also acceding to the Convention. In the region, both Mexico and Costa Rica are now showing interest in the Convention, to better understand what it can provide. Mr. Rees ended his presentation by encouraging countries to ask for assistance and support in reviewing and drafting legislation. He highlighted that the Council of Europe has a very active program to review legislation, and the United States Department of Justice also has a program for this.

44. Gilberto Martins de Almeida, Brazil, discussed the "Brazilian Legal Approach on Cybercrimes"[37] and also gave the meeting participants an overview of where different countries in the Americas region stand when it comes to making amendments to their codes. With regard to Brazil's legal approach to cybercrime, Mr. Martins de Almeida showed that there can be conflicts in a country's national agenda. A practical problem in Brazil is that criminal code and the civil code have 30 sections. Due to this, if Brazil needs legislation for cybercrime, this would not be very practical as direct comparisons are not very applicable. He said that the country should not try to "prove too much that we need a law, but at the same time we need to make the point that a law is needed." Mr. Martins de Almeida discussed the Council of Europe Convention on Cybercrime and what this has meant to Brazil. Generally, he noted that the Convention provides substantive and procedural criminal legal basis, defines investigative powers and relevant safeguards/limits, provided guidelines for relationships with service providers; and guidelines for overall development of national legislation, as well as a basis for international cooperation. Overall, he noted, the Convention on Cybercrime has changed the mindset of the Brazilian community involved in legislative matters — one reason is that it leaves the balance between security and privacy to national legislation. He noted that the Convention serves as a guideline for the development of national cybercrime legislation by providing a coherent approach to national legislation, harmonization and compatibility of criminal law provisions on cybercrime with those of other countries, and procedural measures for more efficient investigations. Additionally, the Convention provides for a number of tools for the gathering of electronic evidence, including tools for the investigation of cyber-laundering, cyberterrorism and other serious crime, and these tools can also be applied in the context of international cooperation.

[36] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/rees-legal-foundation-buenos-aires-oct-07.pdf

[37] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/almeida-brazil-legal-approach-buenos-aires-oct-07.pdf

45. Fernando Maresca, National Office of Information Technology (ONTI), Argentina presented views on the legal aspects of cybercrime in his presentation "Aspectos Legales del Cibercrimen"[38] including examples of what Argentina is currently doing with regard to revising it legal frameworks. Mr. Maresca started his presentation by noting that one of the challenges that practitioners in the area of cybercrime come across involve outdated descriptions of what kinds of crimes should fall under the heading "cybercrime" where often existing descriptions and definitions are not sufficient to do anything about activities that arise due to the use of new criminal methods. He further noted that cybercrime can be looked at from different perspectives. While some argue that cybercrime should be considered as a new type of crime, others claim that cybercrime does not exist but is just an extension of existing crime. He said that if this is indeed the case, we are not dealing with a new kind of crime but rather just a terminology issue.

46. Mr. Maresca noted that Argentina currently has a cybercrime bill in congress and it is quite likely that this bill will be passed as a specific cybercrime law. He noted that in the region, only 11 countries have some kind of cybercrime legislation in place. He also noted that where countries have legislation for electronic crimes, specific penalties are quite different across countries. He argued that agreed standards for criminalizing and penalizing acts are urgently needed, as is overall harmonization between country legislation in the region.

Session 8: Legal Foundation, Regulatory Development and Enforcement

47. In Session 8, discussions related to building a legal foundation, regulatory development and enforcement continued.

48. Jody Westby, Global Cyber Risk LLC, United States of America, presented on the "International Issues In Responding to Cybercrime: A Call for Harmonization"[39]. Ms. Westby started her presentation by talking about cybersecurity in terms of a stool with three legs; cybercrime, privacy and cybersecurity, all of which are global issues. Cybercrime, privacy and security of information infrastructures are very important to both national and economic security interests as well as public safety. While industrialized countries are increasingly trying to address these issues, the world's developing countries are lagging behind. She went on to note that the global legal system is highly inconsistent and there are currently, major differences in cybercrime laws. This is in part due to the fact that while countries and organizations have been trying to bridge the "digital divide", we have also created a "legal divide". She also asked the question why cybercrime laws are important also for developing countries to consider. Here she noted that enacting cybercrime laws and legislation will help countries ensure that no specific country is a safe haven for cyber criminals and that criminals in the end no longer have any safe havens. Ms. Westby also highlighted the main areas where harmonization is needed including: definitions and scope; jurisdictional provisions; substantive provisions; procedural provisions, and in the domain of international cooperation.

49. To help countries develop model cybercrime legislation, Ms. Westby mentioned an ongoing ITU initiative, the "ITU Toolkit for Model Cybercrime Legislation"[40]. This toolkit represents one of the five elements identified in the ITU-D Study Group Q22/1 developed *Framework for Organizing a National Approach to Cybersecurity*. Deterring cybercrime is an integral component of a national cybersecurity/CIIP strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures. As threats can originate anywhere around the globe, the challenges are inherently international in scope and it is desirable to harmonize legislative norms as much as possible to facilitate regional and international cooperation. The Toolkit for Model Cybercrime Legislation aims to provide countries with model legislation that can assist in the establishment of a legislative framework to deter cybercrime. Development of the toolkit is being undertaken by a multidisciplinary international group of experts, of which Ms. Westby is one, and the initial draft will be made available in the first quarter of 2008.

50. Marco Gercke, Germany, in his presentation entitled "The Challenge of Fighting Cybercrime in Developing Countries and the Role of National, Regional, and International Cybercrime Legislation"[41] highlighted some of the challenges that developing countries face in their fight against cybercrime with details on the forthcoming 2007 ITU publication on this topic[42]. He also elaborated on national, regional and international cybercrime legislation for promoting a global culture of cybersecurity. In this context he highlighted the importance of harmonisation and referred to the Convention on Cybercrime as the only international framework that is currentl available. Mr. Gercke noted that finding adequate solutions to respond to the threat of cybercrime is a major challenge for developing countries. The development and implementation of a national strategy for cybersecurity including fighting cybercrime, requires time, and can be quite costly, which may prevent countries from taking necessary steps to improve security. Mr Gercke further emphasized that it is important to point out that risks related to weak protection measures can easily impact the societal and business environment in critical ways. As a consequence, developing countries risk attracting cybercrime activity and negatively impact the national market place. However, he also noted that starting from a blank slate may give developing

[38] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/maresca-cibercrime-buenos-aires-oct-07.pdf
[39] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/westby-model-law-project-buenos-aires-oct-07.pdf
[40] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html
[41] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/gercke-cybercrime-guide-buenos-aires-oct-07.pdf
[42] http://www.itu.int/ITU-D/cyb/cybersecurity/index.html

countries have a unique opportunity to align their cybercrime strategies with necessary standards right from the start.

51. Mr. Gercke also pointed out that the Internet is a very good place to hide information about "secret" things. The drawback with the facilities that the Internet offers is that there are many criminals who are very good at using these techniques. The live demos given by Mr. Gercke in his presentation were highly appreciated by the workshop participants in that it allowed them to better understand techniques to, for example, embed hidden conversations in images and e-mails.

Session 9: Regional and International Cooperation

52. Regional and international cooperation is extremely important in fostering a culture of security, along with the role of regional fora to facilitate interactions and exchanges. This session reviewed some of the ongoing regional and international cooperation initiatives in order to encourage meeting participants to participate in further concrete actions that could be implemented in the Americas region and internationally.

53. Albert Rees, Department of Justice, United States of America, also representing OAS REMJA (Reuniones de Ministros de Justicia o Ministros o Procuradores Generales de las Américas/Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas), and its Group of Governmental Experts on Cybercrime, in this session opened up the discussions in the session with his presentation on "International Cooperation"[43]. He mentioned that REMJA provides assistance to the OAS Member States through, among other things; regional workshops, policy and legislative development, computer investigations and forensics, and international cooperation. Mr. Rees also talked about the 24/7 High Tech Crime Network, originally a G8 initiative, which provides an emergency contact network for online crime issues. The network is made up of law enforcement people who share information and advice related to data preservation, ISP contacts, and how to start mutual legal assistance processes.

54. Currently the 24/7 High Tech Crime Network has contact points in about 50 countries, and in the Americas region Brazil, Canada, Chile, the Dominican Republic, Jamaica, Peru, and the United States are all participating in the network. The network is open to all, and Mr. Rees mentioned that it is easy to 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 cybercrime is handling digital forensic evidence. The person also needs to know domestic laws and procedures. Therefore, there are no special barriers to participate in the 24/7 High Tech Crime Network. Mr. Rees mentioned that countries interested in learning more about the network can contact the US Department of Justice Computer Crime and Intellectual Property Section (CCIPS)[44]

55. Romulo Dantas, representing the Inter-American Committee against Terrorism/El Comité Interamericano contra el Terrorismo (CICTE) of the Organization of American States (OAS), presented on the OAS Critical Infrastructure Protection Program in his presentation "Programa de la OEA de Protección de Infraestructuras Críticas"[45]. He noted that OAS is stepping up its efforts in the field of infrastructure protection in response to an increasing number of security incidents. He also noted that during the past year, many OAS Member States have made significant progress in complying with the commitments made through the Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity[46]. Noteworthy is that all OAS countries have signed this strategy, and appointed national points of contact which are available on the CICTE website. Through these national contact points, the experts involved have direct access to people in national governments who have an understanding of the possible impact of cyber-related threats.

56. The strategy recognizes the need to create an Inter-American alert, watch, and warning network to allow for rapid cybersecurity information dissemination, and to assist countries in responding to and recovering from crises, incidents, and threats to computer security. Thus one of the commitments under the regional strategy involves establishing computer incident response teams (CSIRTs) in OAS Member States to respond to cybersecurity incidents. Whilst the strategy pools the efforts and expertise of CICTE, CITEL, and REMJA, it recognizes the necessity for all participants in networks and information systems to become aware of their roles and responsibilities in regard to security, in order to build a culture of cybersecurity. Mr. Dantas noted that CICTE focuses its activities on helping countries strengthen their capabilities by helping to develop and train CSIRT staff in the region. Under an ambitious strategy, CICTE has also committed to developing plans for the creation of a hemisphere-wide 24-hour per day, seven-day per week network and CSIRTs play an important role in this as they are capable of, and have responsibility with appropriately and rapidly disseminating cybersecurity information and providing technical guidance and support in the event of a cyber incident. One of the goals is to take national points of contacts, and transform these into fully fledged CSIRTs in the future.

57. Mr. Dantas elaborating further on the overall preparedness of OAS Member States, looking at which countries had integrated cybercrime into their legislation, and how far along they have come in implementing the specific items mentioned in the Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity.

[43] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/rees-international-cooperation-buenos-aires-oct-07.pdf
[44] http://www.cybercrime.gov
[45] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/dantas-cicte-buenos-aires-oct-07.pdf
[46] http://www.cicte.oas.org/Rev/En/Documents/OAS_GA/AG-RES.%202004%20(XXXIV-O-04)_EN.pdf

58. Wayne Zeuch, Alcatel-Lucent, presented on behalf of the Inter-American Telecommunication Commission/ Comisión Interamericana de Telecomunicaciones (CITEL) of the Organization of American States, with a presentation titled "CITEL's Focus on Cybersecurity and Critical Infrastructure Protection"[47]. Mr. Zeuch started his presentation by noting that in the OAS mandate related cybersecurity and critical infrastructure protection, CICTE, CITEL, and REMJA each represent a pillar of the Comprehensive Inter-American Cybersecurity Strategy, and the multidisciplinary efforts of these bodies aim to support the growth, development, and protection of the Internet and related information systems, and protect users of those information networks. In CITEL, the related cybersecurity and critical infrastructure activities are undertaken within CITEL's Permanent Consultative Committee I (PCC.I). Mr. Zeuch explained that the mandate of the group includes studying the security aspects related to communication network development (including the role in supporting critical infrastructures, the role of private sector in securing communication networks, and domestic and regional approaches in the Americas required. It also includes assessing current work underway in the OAS, ITU, and other fora on security issues and critical infrastructure protection, in addition to developing domestic and regional approaches to network security, deployment strategies, information exchange, and outreach to the public and private sectors. PCC.I also reviews frameworks and guidelines on networks and cybersecurity and their applicability within the Americas, and tries to foster dialog with regard to the work of ITU-T Study Group 17, and other relevant fora.

59. Mr. Zeuch mentioned what is called the PCC.I "Cybersecurity Technical Notebook", which is an archive of results of workshops, cybersecurity and CIIP strategies deployed by Member States, and it includes appendices with specific national experiences. He also mentioned that a "Critical Infrastructure Protection Technical Notebook" is also currently being worked on. The purpose of this workbook is to complement the cybersecurity notebook by providing information on Critical Infrastructure Protection and making it available to the telecom industry and Member States, documenting national CIP strategies of Member States, highlighting relevant CIP-related recommendations from the ITU and other relevant fora, so that the Member States can better address new technical CIP issues as they arise. At the most recent PCC.I meeting in late 2007, a "Fraud in the Provision of Telecom Services Technical Notebook" was also proposed. Mr. Zeuch concluded his presentation by discussing CITEL's standards coordination work that relate not only to security-related standards but more broadly to standards in most areas of telecommunication. However, in the security standards area, CITEL is utilizing coordinated standards documents to increase awareness of relevant security standards and to endorse the use of the relevant standards in the region.

Round Table Information Exchanges

60. At the end of each of the first two days of the workshop, participants broke into smaller groups to allow focused peer-to-peer discussion of the programme topics of the day in a roundtable format under the overall guidance of a moderator. The moderator ensured that all participants were given the opportunity to share country specific experiences and ask questions from the experts involved in the discussions at each table. During the three day event, the smaller groups discussed five different topics:

- Development of a National Strategy, moderated by Joseph Richardson;
- Technical Standards for Cybersecurity, moderated by Mike Harrop, ITU-T Study Group 17, Rapporteur on the Security Project;
- Watch, Warning and Incident Response, moderated by Jason Rafail, CERT/CC SEI, United States of America;
- Promoting a Culture of Cybersecurity and the Role of CSIRTS, moderated by Patricia Prandini, ArCERT, Argentina;
- Legal Foundation, Regulatory Development and Enforcement (1), moderated by Albert Rees, Department of Justice, United States of America;
- Legal Foundation, Regulatory Development and Enforcement (2), moderated by Jody Westby, Global Cyber Risk LLC, United States of America.

61. Before ending the workshop in the afternoon, the groups each reported back to the meeting participants and provided a brief summary of the topics discussed and main challenges identified. The findings and common understandings that emerged during these discussions were later summarized in Session 10 of the meeting. Details on these are highlighted in Session 10 below.

Session 10: Wrap-Up, Recommendations and the Way Forward

62. The final session of the meeting, facilitated by Robert Shaw, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Sector (ITU-D), provided a summary of the different sessions presented during the workshop and posed questions about what future strategies, solutions, partnerships, frameworks are now needed to move forward on these discussions related to frameworks for cybersecurity and critical information infrastructure protection. Representatives of the five main areas provided their main takeaways

[47] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/zeuch-citel-buenos-aires-oct-07.pdf

from the event, especially reflecting the discussions that took place in the session they presented in as well as their views on what some possible and constructive next steps could be.

63. Sessions 1 and 2, Frameworks for Cybersecurity and CIIP: Daniel Hurley, Department of Commerce, National Telecommunications and Information Administration (NTIA), United States of America. Mr. Hurley highlighted the importance of government-industry collaboration, and noted that this would be much easier if all parties tried to cooperate in the manner described by the speaker from Microsoft. Mr. Hurley also brought the workshop participants' attention to the ITU National Cybersecurity/CIIP Self-Assessment Toolkit, which can assist countries in developing a baseline for cybersecurity; helping the country establish where it is and can also assist countries to prioritize activities according to their specific needs. As a proposed next step to move forward, Mr. Hurley emphasised the need to move from awareness-raising activities to devoting time and resources to capacity-building on specific topics to improve cybersecurity.

64. Session 3, Technical Standards for Cybersecurity: Mike Harrop, ITU-T Study Group 17, Rapporteur on the Security Project. Mr. Harrop noted that it is important to urgently improve the engagement of the countries in Latin America as well as lesser developed countries around the world in ITU standards activities to give an added voice to the standards work. He mentioned that what he had heard throughout the workshop is that countries have asked about other countries' cybersecurity policies, and how effective they are, therefore it could be interesting to start looking closer at a possible cybersecurity/CIIP readiness index to assist countries to understand where they are in preparedness. This is to assist each country to know where they are at a national level but also to know where they stand in comparison to other countries.

65. Sessions 4, 5 and 6, Watch, Warning and Incident Response, and The Role of CSIRTs in Promoting a Culture of Cybersecurity: Patricia Prandini, ArCERT, Argentina. Ms. Prandini mentioned that she was happy to learn during the workshop that no country is starting at zero when it comes to building capacity for cybersecurity and CIIP but also at the same time no country is complete, and therefore all countries have work to do. She compared the work being undertaken to a necklace made up of beads: She rhetorically asked "we already have the beads but how do we string these beads together?" For example, she noted that in Argentina we have a CSIRT and are about to pass a cybercrime bill but we do not yet have an overall framework that pulls all elements of a national strategy together. The ITU toolkits that have been mentioned during the workshop, especially the National Cybersecurity/CIIP Readiness Toolkit would allow all of us to better position ourselves, in relation to previous achievements and also towards other countries. Ms. Prandini stated her belief that she was sure we are all doing better than we think we are. As a concrete step forward, Ms. Prandini highlighted the need for a cybersecurity web portal where all meetings, training resources, programmes could be found, all in one place. She also suggested that in order to establish an effective way to work with each other, a common calendar of events would also be quite useful. Ms. Prandini also brought the participants' attention to the possible creation of a regional Latin American CERT.

66. Sessions 7 and 8, Legal Foundation, Regulatory Development and Enforcement: Jody Westby, Global Cyber Risk LLC, United States of America. The three main points that Ms. Westby emphasized was the need for increased international cooperation in the legislation and enforcement area, the need to build out the 24/7 High Tech Crime Network in the coming year, and the possibility to create a step-by-step "Search and Seizure Cookbook". Ms. Westby also put forward an open request to CISCO, who had sponsored the coffee/tea breaks during the workshop, to establish tele-presence centers in the Americas region, and in other regions around the world, so that people attending regional workshops and meetings like this one can continue these discussions online in addition to face-to-face meetings.

67. Session 9, Regional and International Cooperation: Romulo Dantas, Inter-American Committee against Terrorism (CICTE) of the Organization of American States. Mr. Dantas noted that some fundamental tensions between national, regional, and international cybersecurity approaches still seems to exist, while at the same time a protection philosophy is common to all. He then mentioned that cooperation, not only regionally but also intra-regionally, across and amongst regions should be further fostered and encouraged. Finally, he emphasized that as building cybersecurity is something that the government cannot do alone, partnerships with the industry and the private sector are very important and should be an area of focus. Mr. Dantas ended his remarks by noting that the cyber-threat is broad in scope and a multi-disciplinary education could make a difference.

Meeting Closing

68. Gonzalo Heredia, Coordinator for National Information Society Programs, Secretaría de Comunicaciones, Argentina provided closing remarks[48] to conclude the three day event. He noted that security is no longer a problem exclusive to the information technology area, a particular organization, industry or government, but rather nations needed to ensure that threats and vulnerabilities to cybersecurity are dealt with in a coordinated manner across all these domains. He voiced his appreciation for the recent initiative taken by ITU to assist countries in building national strategies for cybersecurity and the protection of critical information infrastructure and that Argentina was happy to be able to host this event to assist with this important initiative. He also thanked the workshop participants and speakers for taking time out of their busy schedules to travel to Buenos Aires to take part in the workshop. He concluded by highlighting that all of us, all participants in the

[48] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/closing-remarks-heredia-buenos-aires-18-oct-07-s.pdf (Español)

Information Society, have a role to play and responsibility in creating a global culture of cybersecurity. There is work for everyone to be done in this area and Mr. Heredia hoped that this workshop would be a milestone towards a better online world.

69. In his closing remarks[49], on behalf of ITU-D Director Sami Al-Basheer and ITU-T Director Malcolm Johnson, Paolo Rosa, Workshops and Promotion Division, ITU Telecommunication Standardization Bureau, thanked the local Argentinean hosts for their outstanding work in making this regional cybersecurity event, jointly organized by the ITU Telecommunication Standardization and Development Sectors, a highly successful workshop. He relayed special thanks to the Secretaría de Comunicaciones, Argentina and Comisión Nacional de Comunicaciones (CNC), Argentina for the excellent hosting of the event and for their cooperation in the planning and organization of this event; all workshop speakers for taking time out of their busy schedules to share their experiences and expertise with the meeting participants; delegates for their attention and active participation and contribution; and CISCO for their for their sponsorship of coffee breaks and evening cocktail. As the main facilitator for WSIS Action C5 dedicated to building confidence and security in the use of ICTs, and with its long withstanding activities in the standardization and development of telecommunications, it was emphasized that ITU will 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, and for comments and questions related to the ITU Cybersecurity Work Programme for Developing Countries (2007-2009)[50], is **cybmail(at)itu.int**. For information sharing purposes, all meeting participants will be added to **cybersecurity-americas(at)itu.int**[51] mailing list and related discussion forums for matters concerning ITU-D cybersecurity-related activities. If you have not participated directly in the workshop, 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**.

[49] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/closing-remarks-itu-buenos-aires-18-oct-07.pdf

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

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