



GOVERNO DE CABO VERDE



# ITU West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP)

Document RWPR/2007/01-E  
1 December 2007  
Original: English

## Draft Meeting Report : ITU West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and CIIP, Praia, Cape Verde, 27-29 November 2007

Please send any comments you may have on this draft meeting report to [cybmail\(at\)itu.int](mailto:cybmail(at)itu.int)

### Purpose of this Report

1. The ITU West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP) was held in Praia, Cape Verde, 27-29 November 2007<sup>1</sup>. The workshop aimed to bring together government representatives, industry actors, and other stakeholder groups in the West Africa region to discuss, share information, and collaborate on the elaboration and implementation of national policy, regulatory and enforcement frameworks for cybersecurity and CIIP. The event sought to benefit the following key stakeholders: information and communication policy makers from ministries and government departments in the region; institutions and departments dealing with cybersecurity policies, legislation and enforcement; and representatives from operators, manufacturers, service providers, industry and consumer associations involved in promoting a culture of cybersecurity. The workshop also considered initiatives on the regional and international level to increase cooperation and coordination amongst these different stakeholders.
2. Approximately 120 people participated in the event, from countries in the West Africa region, including from the host country Cape Verde, the African continent, as well as 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/prai/](http://www.itu.int/itu-d/cyb/events/2007/prai/). 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.

### West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and CIIP, held in Praia, Cape Verde, 27-29 November 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 therefore requires a comprehensive, multi-disciplinary and multi-stakeholder approach. This event discussed some of the key elements in developing such policy and regulatory frameworks.

### Meeting Opening and Welcome

4. The Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection was opened with a [welcoming address](#)<sup>2</sup> by Margarida Evora-Sagna, representative from the ITU Area Office for West Africa in Senegal. On behalf of the ITU, Ms. Evora-Sagna welcomed the workshop participants to the event and highlighted why this workshop is an important step towards building cybersecurity capacity in the region. Ms. Evora-Sagna mentioned that in most African countries there is a gap in cybersecurity regulatory frameworks

<sup>1</sup> <http://www.itu.int/ITU-D/cyb/events/2007/prai/>

<sup>2</sup> <http://www.itu.int/ITU-D/cyb/events/2007/prai/docs/evora-sagna-opening-remarks-prai-27-nov-07.pdf>

and that issues related to cybersecurity do not get the attention they deserve. On the one hand, a minority of people in Africa has access to ICTs, but at the same time there is an emphasis on accelerating access to ICTs without providing citizens with the tools to protect themselves and deal with related threats. However, Ms. Evora-Sagna continued, the presence of so many African countries at this workshop seems to prove that countries in the region are now willing to take action in order to enhance cybersecurity and boost activities to protect critical information infrastructures. She concluded her opening remarks by thanking the local organizers for supporting this event, and hoped that the recommendations and conclusions that come out of the workshop can guide countries in creating a favorable ICT environment that fully integrates the important aspects related to cybersecurity – and by doing so ensure the creation of a knowledge economy for the further development and well-being of West African nations.

5. This was followed by opening remarks given by Patricia de Mowbray, representing the Joint United Nations Office in Cape Verde. On behalf of the United Nations (UN), she discussed the revolution that the Internet has proven to be with regards to health and education, and as an essential tool for modern society to stimulate future socio-economic development. With information and communication technologies as tools for reducing poverty, and the Internet demonstrating the advantages Internet access can give society in many areas, she went on to describe the link between the Internet and security, and the growing demand for increased cybersecurity measures. Ms. de Mowbray also mentioned some of the relevant cybersecurity-related UN resolutions: particularly [UN General Assembly Resolution 57/239](#)<sup>3</sup>, which concerns creating a global culture of cybersecurity and provides countries with some main guidelines for activities to be implemented on the national level. She ended her opening remarks by wishing the organizers a successful event, hoping that the workshop would provide a good forum to further develop the necessary tools to fight cybercrime.

6. H.E. Manuel Sousa, Minister of Infrastructure, Transport and Sea, Cape Verde then provided a welcoming address on behalf of the Ministry of Infrastructure, Transport and Sea, Ministério das Infraestruturas e Transportes e Mar, Cape Verde, stating that cybersecurity and critical information infrastructure protection are very important challenges to the Information Society that cannot be addressed without concrete action. He noted that it was an honour for Cape Verde to be hosting this event, and working with the experts and participants to strengthen links with all African countries in this area. Mr. Sousa also 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 West African region and other parts of the world, 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. Everyone, security experts and users alike, need to better understand what is at stake in the different countries, and what can be done about this. Mr. Sousa concluded by extending his greetings to all those present at this very important meeting on cybersecurity and CIIP and invited the workshop participants to engage in fruitful debate and focused discussions during the three day workshop.

## **Session 1: Creating a National Strategy and Framework for Cybersecurity and Critical Information Infrastructure Protection (CIIP)**

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, non-institutional approach. Many countries have not yet established a national strategy for cybersecurity and CIIP. This session discussed the concept of a national framework for cybersecurity and CIIP and ongoing efforts to elaborate a best practices framework in the ITU, in order to provide participants with a broad overview of the issues and challenges involved.

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 the 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](#)”<sup>4</sup> and shared details on the [ITU-D Cybersecurity Work Programme to Assist Developing Countries \(2007-2009\)](#)<sup>5</sup>. Some of the ongoing and planned ITU cybersecurity initiatives mentioned in his presentation included: *activities dealing with the identification of best practices in the establishment of 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

<sup>3</sup> [http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN\\_resolution\\_57\\_239.pdf](http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf)

<sup>4</sup> <http://www.itu.int/ITU-D/cyb/events/2007/praha/docs/shaw-itu-d-cybersecurity-activities-praha-nov-07.pdf>

<sup>5</sup> <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf>

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, Study Group 1 Question 22, 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, reference material, 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's 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. He also mentioned that the ITU is planning at least two additional cybersecurity events on the African continent in the coming year, and hopes to launch a Cybersecurity Fellowship Programme<sup>6</sup> in 2008.

10. Jorge Lopes, Nucleo Operacional da Sociedade de Informacao (NOSI), Cape Verde, in his presentation "[e-Governance e Cybersecurity/e-Governance and Cybersecurity](#)"<sup>7</sup> shared some ideas concerning the implementation of e-government services in Cape Verde, and how the country is working to improve governance and service delivery through e-government. He started by providing the workshop participants with an insight into the context of e-government in the country, focusing on how Cape Verde is dealing with issues related to security and the specific aspects of security that are currently being addressed. In doing so he discussed the three main pillars of the country's e-government strategy, namely the relationship between the citizen and the government, the relationship between the government and the private sector, and the relationship between the government and the public sector service providers. He pointed out that security on the Internet is an essential element for the safety of users of ICTs and that the full potential of the Internet in economic and trade relations can only be realized through a stable and more secure environment. With wireless hotspots increasingly being rolled out throughout the country and a wide range of value-added government services being implemented, increasing levels of security to ensure that these services are not being accessed and misused by criminals have put pressure on the government to deal with the security aspects. Mr. Lopes ensured that measures have been put in place to provide the right conditions to be able to respond to the new challenges of providing these services. In doing so, Cape Verde has noted that the creation of a culture for increased collaboration and effective horizontal cooperation among government departments is very important.

11. Mr. Lopes concluded by noting that in Cape Verde the link between e-governance and security is based on the guidelines that have been established by ITU and Council of Europe Convention on Cybercrime. However, he also noted that management of the state network has not been developed with a clear understanding of security in mind, and as a matter of priority, this will now need to be addressed in moving forward. The country needs to better understand who is who on the network, who is responsible for the different tasks, etc., and highlighting also the Minister's comments earlier this morning on the need for cybersecurity and critical information infrastructure protection to be given higher priority than the present situation in Cape Verde.

12. James Ennis, Department of State, United States of America, in his capacity as the Rapporteur for ITU-D Study Group 1 Question 22: *Securing Information and Communication Networks: Best Practices for Developing a Culture of Cybersecurity*, 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 "[Best Practices for Organizing National Cybersecurity Efforts](#)"<sup>8</sup>. 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*<sup>9</sup> which governments can use as a guideline when developing and undertaking national strategies for cybersecurity and CIIP. Mr. Ennis invited workshop participants and countries to join the Q22/1 activities which were initiated at the World Telecommunication Development Conference (Doha, 2006). Three meetings have taken place to date, with the next meeting scheduled to take place in April 2008.

13. The report being developed by the Study Group addresses the major problems that policy makers are faced with when dealing with cybersecurity. The draft report starts with a working definition of cybersecurity ("Cybersecurity is the prevention of damage to, unauthorized use of, exploitation of, and - if needed - the restoration of electronic information and communication systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems."), and also notes that different levels of security are necessary for different systems, highlighting the need for adequate risk management. The *Framework for National Cybersecurity Efforts* elaborated on in the report, looks at five main components for best practices in cybersecurity, namely: 1) Developing a National Strategy for Cybersecurity; 2) Government-Industry Collaboration; 3) Deterring Cybercrime; 4) National Incident Management Capabilities; and, 5) A 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. Mr. Ennis further noted that the *Best Practices for Organizing National Cybersecurity Efforts* report, including the framework, is a living document and as such, will evolve over time.

<sup>6</sup> <http://www.itu.int/ITU-D/cyb/cybersecurity/>

<sup>7</sup> <http://www.itu.int/ITU-D/cyb/events/2007/praha/docs/lopes-e-government-cybersecurity-praha-nov-07.pdf>

<sup>8</sup> <http://www.itu.int/ITU-D/cyb/events/2007/praha/docs/ennis-best-practices-cybersecurity-praha-nov-07.pdf>

<sup>9</sup> <http://www.itu.int/md/D06-SG01-C-0130/en> (ITU TIES login and password required)

14. Mr. Ennis also highlighted in his presentation that cybersecurity is one of the most important topics in the telecommunications arena today. Mr. Ennis recognized that presently, all critical sectors of society rely on information and communication networks for their stable functioning, and in order to achieve a maximum level of security, these systems need to be reliable, secure, and trusted. All nations (developed and developing countries) are affected by this.

## Session 2: Development of a National Strategy for Cybersecurity and Critical Information Infrastructure Protection (CIIP)

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 Basil Udotai, Directorate for Cybersecurity, Office of the National Security Adviser, Nigeria, sought to explore in more detail various cybersecurity approaches and best practices, and identify key building blocks that could assist countries in the West African region in establishing national strategies for cybersecurity and CIIP.

16. In Session 2, Mr. Udotai, in his presentation on the development of a national strategy "[Framework for Cybersecurity in Nigeria](#)"<sup>10</sup>, shared some insights into the challenges involved in developing a national strategy for cybersecurity and CIIP, with specific examples from Nigeria and other West African countries. He highlighted that the cybersecurity challenges that countries face today are very similar in developed and developing countries, as societies' reliance and dependence on computers and computer networks increases to provide all kinds of different services. In Sub-Saharan Africa, Mr. Udotai noted, there are a lack of true incentives and compelling factors for governments to make changes to laws and legislation and take the necessary measures to effectively deal with cybercrime and build cybersecurity. The private sector and industry in these countries are also not doing enough to deal with cybersecurity as the market is developing well and these actors may not see an immediate need for this extra expense. The development of ICTs in the region is moving on a horizontal level with the addition of new value added services.

17. Mr. Udotai brought participants' attention to what he called the "*development paradox of cybersecurity*". On the one hand, developing countries are encouraged to increase their use of ICTs and the Internet, promoting ICT adaptation and increased Internet penetration, while at the same time they are warned of the dangers and threats that cyberspace exposes governments, businesses and citizens to. Mr. Udotai noted that although the Internet, more than any other tool, has the potential to redefine global cooperation, concurrently all parties involved should be aware of the realities of *forum shopping*, which is the tendency for hackers and spammers to exploit the least-regulated and most permissive jurisdictions from which to launch cyber attacks. He stated that because there is little or no incentive for security in developing economies and since it is Internet connectivity, not proximity, which determines who one's neighbors on the Internet are, developing countries represent the weakest link in the chain of the Information Society. Mr. Udotai continued with an overview of the Nigerian approach to cybersecurity, its committees and sub-committees, challenges and plans for the future. He shared information on what Nigeria is currently doing to deal with the problems related to cybersecurity, noting that a lot of initiatives have been undertaken ranging from legal reform to awareness-raising activities. Mr. Udotai mentioned that draft legislation has been put together with help and assistance from many different internal and external parties.

18. Mr. Udotai ended his presentation by noting that while no two countries or legal jurisdictions are the same, issues related to cybersecurity cut across many countries and jurisdictions. Therefore, basic frameworks that focus on necessary changes in policy, laws, capacity building, industry partnerships, international cooperation and public enlightenment, should be developed at national levels, employing models that have been already adopted successfully in other countries. He noted that if this workshop encourages any country represented to take a look at its existing legal framework or operational activities of its law enforcement organizations, with the purpose of reform to meet the new challenges of ICTs, then this will have been a very successful conference.

19. Christine Sund, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Sector (ITU-D), in her presentation on "[Promoting a Culture of Cybersecurity](#)"<sup>11</sup> 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 nine elements included: a) awareness, b) responsibility, c) response, d) ethics, e) democracy, f) risk assessment, g) security design and implementation, h) security management, and i) reassessment. Through the Resolutions, Member States and all relevant international organizations were asked to address and take these elements into account in preparation for the two phases on the World Summit on the

<sup>10</sup> <http://www.itu.int/ITU-D/cyb/events/2007/prai/docs/udotai-nigeria-cybersecurity-framework-prai-nov-07.pdf>

<sup>11</sup> <http://www.itu.int/ITU-D/cyb/events/2007/prai/docs/sund-promoting-a-culture-of-cybersecurity-prai-nov-07.pdf>

Information Society (WSIS)<sup>12</sup> in 2003 and 2005. The outcome documents from the two WSIS phases further emphasized the importance of building confidence and security in the use of ICTs and countries' commitment to promoting a culture of security.

20. 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.

21. Building on the presentations made in Sessions 1 and 2, showcasing frameworks for cybersecurity and CIIP and different national strategies and approaches, Joseph Richardson, United States of America, with his presentation on "[Management Framework for Organizing National Cybersecurity Efforts: Self-Assessment Tool](#)"<sup>13</sup> described the elements of the ongoing ITU work to develop a comprehensive [National Cybersecurity/CIIP Self-Assessment Toolkit](#)<sup>14</sup>. 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](#)"<sup>15</sup> and the [ITU Cybersecurity Work Programme to Assist Developing Countries \(2007-2009\)](#)<sup>16</sup> 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. Ennis in Session 1 of the workshop, namely: 1) national strategy; b) government-private sector collaboration; c) deterring cybercrime; d) national incident management capabilities; and, e) a culture of cybersecurity, the necessary institutions, as well as the relationships between government, industry and other private-sector entities.

22. Mr. Richardson noted in his presentation 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 made through the ITU-D cybersecurity website ([www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html](http://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.

23. In the last session at the end of the first day 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 first day the topics of Creating a National Strategy and Framework for Cybersecurity and Critical Information Infrastructure Protection and the Development of a National Strategy, were discussed amongst the workshop participants.

24. In the evening of the first day of the workshop the participants were invited by the organizers to a reception at the workshop venue, the Praia Mar Hotel.

### **Session 3: Legal Foundation, Regulatory Development and Enforcement**

25. 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

---

<sup>12</sup> <http://www.itu.int/wsis/>

<sup>13</sup> <http://www.itu.int/ITU-D/cyb/events/2007/praiadocs/richardson-cybersecurity-framework-and-readiness-assessment-praiainov-07.pdf>

<sup>14</sup> <http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html>

<sup>15</sup> <http://www.itu.int/ITU-D/cyb/cybersecurity/index.html>

<sup>16</sup> <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf>

accordance with international conventions and recommendations. Sessions 3, 4 and 5 of the workshop reviewed various national legal approaches and potential areas for international legal coordination and enforcement efforts. The Session 3 moderator, Matoso Carvalho, Angolan Institute of Communications (INACOM), Angola, introduced the speakers in this first session, and highlighted the growing problems related to different legal frameworks in countries around the world and the urgent need for increased collaboration between all countries in this area.

26. Marco Gercke, Germany, opened the session with an insight into what is currently happening in the international community with regards to revising existing laws and developing new legislation with his presentation entitled “[The Challenge of Fighting Cybercrime in Developing Countries and the Role of National, Regional, and International Cybercrime Legislation](#)”<sup>17</sup>. He highlighted some of the challenges that developing countries face in their fight against cybercrime with details in the forthcoming ITU publication on this topic<sup>18</sup>. 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 a harmonisation and referred to the Budapest [Convention on Cybercrime](#)<sup>19</sup> (2001) as the only international framework that is currently 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 in turn 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 cyber protection measures can easily impact the societal and business environment in critical ways. As a consequence, developing countries risk attracting cybercrime activity and as a result negatively impact the national market place. However, he also noted that starting from a blank slate may provide developing countries with a unique opportunity to align their cybercrime strategies with necessary standards right from the start.

27. Mr. Gercke also pointed out that the Internet is a very good place to hide secret information. 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 available techniques to, for example, embed hidden conversations and messages in images and e-mails.

28. Gabriela Sarmiento, Consultant, Venezuela, followed with her presentation on “[Les Délits Informatiques, Les Lois que Les Punissent et La Pratique Judiciaire/ Cybercrime: Law, Cases and Justice](#)”<sup>20</sup> where she considered some of the legal approaches adopted by countries to deal with cyber-related crimes. She shared with workshop participants some of the national norms applicable to cybercrime, international conventions, some practical cases, and details on committed crimes and punishments. In her presentation Ms. Sarmiento also showed the results of a survey indicating that in the Latin American region, including the Caribbean, 22 countries have been working on adopting a cybercrime bill or changing their penal code to ensure that there is legislation in place to deal with cybercrime. She described the type of legislation that had been adopted around the world to deter cybercrime, highlighting that the number of countries that have adopted some kind of measures has increased. Ms. Sarmiento also gave an example of one unnamed country that was in the process of creating cybercrime legislation that had explicitly said that they were not including the private sector in the process due to the fear of being criticized. Ms. Sarmiento highlighted that any cybercrime legislative project should be able to withstand criticism in order to be effective and to help ensure that the implementation of the legislation in question will be successful.

29. Ms. Sarmiento advised countries to start by identifying what the national problems are, where the country is at in terms of their legislation, and then go from there. She further encouraged workshop participants to make use of the available resources and good models and best practices that are already available. Examples mentioned included ITU’s cybersecurity resources, the OECD anti-spam toolkit to counter spam, Interpol’s manual for cybercrime investigations, Europol’s train-the-trainers resources, etc.. As practical steps forward for countries, Ms. Sarmiento mentioned the need to a) standardize the concept of cybercrime; b) harmonize the laws governing the crime; c) facilitate legal proceedings to collect evidence; and d) improve international cooperation among police forces, and competent judges, and nation states. The need for regional cooperation and mutual assistance in the area of cybercrime legislation to ensure harmonization was also stated by Ms. Sarmiento as an important factor for improved cybersecurity.

#### **Session 4: Legal Foundation, Regulatory Development and Enforcement (continued)**

30. In Session 4, discussions related to building a legal foundation, regulatory development and enforcement continued. The Session 4 moderator, Marco Gercke, Germany, opened the session with an insight into some of the existing “[National, Regional and International Solutions in the Fight Against Cybercrime](#)”<sup>21</sup> with a focus on the Budapest [Convention on Cybercrime](#)<sup>22</sup> (2001). He noted that there are a number of international initiatives

<sup>17</sup> <http://www.itu.int/ITU-D/cyb/events/2007/praiadocs/gercke-challenge-of-fighting-cybercrime-praiadocs-nov-07.pdf>

<sup>18</sup> <http://www.itu.int/ITU-D/cyb/cybersecurity/index.html>

<sup>19</sup> <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>

<sup>20</sup> <http://www.itu.int/ITU-D/cyb/events/2007/praiadocs/sarmiento-cybercrime-laws-practice-praiadocs-nov-07.pdf>

<sup>21</sup> <http://www.itu.int/ITU-D/cyb/events/2007/praiadocs/gercke-convention-on-cybercrime-praiadocs-nov-07.pdf>

<sup>22</sup> <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>

for cybersecurity and the fight against cybercrime, and that all these different initiatives have a role to play. With regards to the Budapest Convention on Cybercrime, or the Council of Europe Convention on Cybercrime as it is more widely known, he mentioned that this is the only existing international agreement that covers all relevant areas of cybercrime legislation (including substantive criminal law, procedural law, and international cooperation) and can be applied to both common law and civil law countries.

31. He introduced the workshop participants to the concept of a legal “DNA”. With a legal cybercrime-related DNA established to note initiatives and legislation for criminalizing the misuse of ICTs in each country, legal DNA comparisons can be made to show and ensure that many countries are criminalizing the same cyber-related offences. He went on to explain that the Council of Europe Convention on Cybercrime was not designed only for European countries and that other countries were involved in developing the convention. The main goal of the Convention is to provide a framework to be used when countries aim to draft, update and revise national legislation. He explained how, in practice, the Convention can help countries in adopting a national cybersecurity agenda. Mr. Gercke noted that countries interested in learning more about the Convention can get in touch with the Council of Europe’s contact points to get further assistance.

32. He then continued with a discussion of the borderless nature of the Internet and how borders in cyberspace can still exist. With “borders”, Mr. Gercke referred to the ability to block IP addresses and block certain national IP addresses, or use geo-tracking abilities that exist today. His objective was to analyze the arguments against regional and national solutions for cybercrime, as many claim that as the Internet does not have any borders and boundaries, only a truly international solutions was necessary. Here Mr. Gercke noted that the international dimension requires harmonisation in order to effectively fight cybercrime, however, this does not exclude the need for regional and national approaches. The purpose of the Convention on Cybercrime is to harmonize national laws to international levels and to ensure that international cooperation is possible. If countries criminalize the same offences, then these countries can cooperate effectively when it comes to investigating crimes, collecting evidence, preparing prosecutions, etc. Mr. Gercke concluded his opening remarks to the session by mentioning that the Secretariat for Convention on Cybercrime (2001) is actively seeking more countries to show interest in the Convention.

33. Baye Issakha Gueye, Membre du Conseil de Régulation de l’Agence de Régulation des Télécommunications (ART), Senegal, continued with a presentation on “[Fondements Juridiques et Démarche Réglementaire pour la Cybersécurité – Survol des Enjeux et Perspectives au Senegal/ Legal and Regulatory Approaches for Cybersecurity – Overview of Issues and Perspectives in Senegal](#)”<sup>23</sup>, noting that cyber-criminals do not need visas to enter countries and that the protection of citizens is the responsibility of each state. Mr. Gueye recalled that several solutions for enhancing cybersecurity have already been proposed, including the establishment of national cybersecurity strategies, awareness-raising, harmonization of standards, and the establishment of strong laws and legislation. He continued with a discussion of what Senegal is currently doing at the national level to put in place the appropriate legal and regulatory frameworks for cybercrime. As an example, he mentioned that measures to facilitate rapid detection, investigation, prosecution, the collection of electronic evidence, extradition and mutual legal assistance, have been considered and selected for inclusion in the body of law in the country.

34. In closing, Mr. Gueye, discussed what he called his futuristic vision for “cyberjustice” and the notion of “e-justice”, where, among other things, national courts have integrated rules applicable to cybercrime and have trained people capable of dealing with related cases. The adoption of new ICT-specific offenses requires a variety of appropriate penalties and the development of criminal proceedings related to ICT crimes. Mr. Gueye called for greater national cybersecurity awareness and that appropriate measures to deal with this be taken.

35. The next speaker, Mody Ndiaye, United Nations Office on Drugs and Crime (UNODC), in his presentation on “[Application de la Loi contre le Cybercrime – Quelle Stratégie en Afrique de l’Ouest?/ Law Enforcement Tools to Investigate Cyber-Attacks – Does West Africa Have a Cybersecurity Strategy](#)”<sup>24</sup>, discussed the most common crimes currently taking place in Africa, one of which is cybercrime. He recognized that trans-national organized crime, including drug trafficking, human and firearms trafficking, and smuggling of migrants, terrorism, corruption, economic and financial crimes, including money-laundering, and cybercrime, severely hamper sustainable socio-economic developments, lowers productivity, reduces efficiency and effectiveness, and undermines the integrity of the social, economic, cultural and political order. Mr. Ndiaye mentioned some of the recent UN General Assembly and UNODC resolutions and texts that deal with cybercrime. Mr. Ndiaye stated that in West Africa the responses to the growing phenomenon of cybercrime are inadequate. With a lack of knowledge amongst law enforcement, in police schools, and other important stakeholders on what cybercrime is and what it consists of, responsible people do not have access to the right tools and mechanisms. He also noted that increased criminal use of technological systems requires increased cooperation and coordination among states and with the private sector.

36. Mr. Ndiaye then elaborated on the question of which approach would be most effective to combat cybercrime. Here he talked about the need to make sure that the Budapest [Convention on Cybercrime](#)<sup>25</sup> (2001) is shared and communicated to all countries, ensuring that harmonization and coordination on a regional basis, is

<sup>23</sup> <http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/gueye-senegal-perspective-praia-nov-07.pdf>

<sup>24</sup> <http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/ndiaye-cybercrime-strategy-for-west-africa-praia-nov-07.pdf>

<sup>25</sup> <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>

encouraged further. He ended by stating: ‘If a crime crosses a border, responses to such crimes are also needed.’”

## **Session 5: Legal Foundation, Regulatory Development and Enforcement (continued)**

37. In Session 5, discussions related to building a legal foundation, regulatory development and enforcement, continued with David Gomes, Agencia Nacional das Comunicações (ANAC), Cape Verde as the session moderator.

38. The first presentation in this session was delivered by Joel Schwarz, Computer Crime & Intellectual Property Section (CCIPS), Criminal Division, Department of Justice, United States of America. In his presentation, “[Legal Foundation and Development: The Risk of Cybercrime and Its Impact on Africa](#)”<sup>26</sup>, he walked the participants through different cases from around the world demonstrating how almost every case that prosecutors deal with today, whether organized crime, gambling, kidnapping, etc., has some computer-related component involved. Cybercrime no longer involves only attacks on computers, instead people that do not know much about computers are using computers online today, and these numbers are growing rapidly. People will continue to use computers and other devices online even if prosecutors and policemen do not. He noted that if countries are considered unsafe when it comes to the online world, industry and investors will most likely stay away from that country in the future. He continued discussing the great potential for economic growth that the Internet can bring, but noting that all these benefits depend on reliable and secure information networks, and that all of these benefits are in danger if a country cannot provide secure information networks for citizens and businesses. Therefore, it is increasingly important for each country to develop the capabilities and competences to investigate abuse or misuse of those networks and ensure that punishment of criminals who attack or exploit those networks is implemented.

39. Mr. Schwartz then continued with a discussion on how countries should respond to the threat of cybercrime from a law enforcement perspective. In order to successfully investigate, prosecute, and convict people who use computers and the Internet to commit crimes, as a first step, he recommended focusing on implementing a number of measures including: establishing and implementing adequate cybercrime and related laws, establishing specialized law enforcement, and ensuing connections with other countries. In this regard, he gave some simple advice on how to make sure that a country’s legislation is up-to-date. This included considering that if the country does not want to re-draft laws, to at least amend existing laws, and to check that current laws do not use words that just relate to the physical world. He advised countries to consider using the Council of Europe Convention on Cybercrime as a checklist to review existing legislation in a country. The Convention starts by laying out of some definitions which he noted was the most contested issue in the drafting of the Convention. Even today, when reviewing different laws, one can see differences in definitions

40. Mr. Schwartz concluded his presentation by mentioning a number of projects that the US Department of Justice have been closely involved in on the African continent. Among other things, he mentioned two workshops in Botswana in 2006, in which 20 countries had participated. As a result of these meetings and other awareness-raising activities, a mailing list had been created and two new African countries had recently joined the 24/7 High Tech Crime Network of Contacts.

41. The next speaker, Alex da Costa, Public Utilities Regulatory Authority (PURA), The Gambia, in his presentation on “[Legal and Regulatory Perspectives](#)”<sup>27</sup>, looked at the role of the regulator in fighting cybercrime and promoting cybersecurity from the perspective of his country, The Gambia, and the multi-sector regulatory authority which he represented. He noted that the challenges in the area of building a legal foundation are great and that countries cannot do anything about cybercrime if the appropriate legislation is not in place. He highlighted the need for all countries to amend existing laws and establish new laws to deal with the growing threats related to the misuse of ICTs. He also mentioned the importance of building a culture of cybersecurity. He focused his view on cybersecurity to the process of regulatory development, noting that regulation is direct regulatory control over specific sectors of the national economy, and likened the lack of direct government involvement in regulation of some sectors of the economy to “returning to the jungle”. Mr. da Costa also elaborated on the critical success factors for regulatory development and some of the specific functions of a regulator including independence, autonomy, authority, accountability, and stakeholder consultations.

42. Mr. da Costa explained that in The Gambia there is no existing legislation on cybersecurity, data protection and flow of information. However, he noted that someone needs to take overall responsibility for this in each country. He asked whether this is the responsibility of regulators, the justice ministry, or some other stakeholder in each country? This might seem like an easy question, he noted, but in reality it is often not an easy question to answer. As there is always a fight for government resources, there is typically no agreement regarding what are critical needs, he noted. He concluded his presentation by calling for action and not just talk. He emphasized that the absence of laws is a major problem. West Africa needs to wake up to the need for both proper infrastructure and legal frameworks. He closed by noting that effective cybersecurity requires the full cooperation and participation of all stakeholders globally, consumers, utilities, and most importantly all arms of the State.

---

<sup>26</sup> <http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/schwartz-legal-development-praia-nov-07.pdf>

<sup>27</sup> <http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/da-costa-gambia-praia-nov-07.pdf>

43. Before ending the workshop in the afternoon, the meeting participants discussed and asked questions in an open session dedicated to Legal Foundation, Regulatory Development and Enforcement, providing a brief summary of the topics discussed by the experts during the day as well as the main challenges identified. The findings and common understandings that emerged during these discussions were later further highlighted in Session 9 of the meeting.

## Session 6: Watch, Warning and Incident Response

44. 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 Seymour Goodman, Georgia Institute of Technology, United States of America, 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.

45. Seymour Goodman, Georgia Institute of Technology, United States of America, opened the session with a presentation entitled “[Watch, Warning, Incident Response \(and Other\) Capabilities](#)”<sup>28</sup>. Mr. Goodman started his presentation by discussing the different aspects of cybersecurity and not only cybercrime, as this is merely one aspect of the cybersecurity landscape. He emphasized that he wanted to bring more into the workshop discussions the other aspects of cybersecurity: identification and location of criminals is just one more narrow aspect of cybersecurity. More broadly, cybersecurity includes vulnerabilities, threats and what one can do about them. The exploiters are called the “threat”, but there are also other threats, including threats to critical information infrastructures, some of which are not human. Mr. Goodman emphasized that trust is an intrinsic part of cybersecurity. He noted that systems we use every day need to be designed with security in mind and the reason that security assurance is a difficult area is that security was not originally built into the design of systems.

46. In presenting on the watch, warning and incident response and other sustainable operational activities, Mr. Goodman asked: who does the watch and who does the warning, and who gets the information from the watching and warning? This is very important in ensuring that cyberspace is made into a safer and more secure place. The criminal law aspects of cybersecurity have been discussed in detail during these three days, and Mr. Goodman wanted to point out again that this is just one aspect of cybersecurity. Today, Mr. Goodman continued, there are laws on seatbelts in cars and these are put in place for people’s own safety when driving. Similarly, there are things that should be done by people when they are connected to ensure that they are more secure in cyberspace. Mr. Goodman noted that we are a long way from a safe and secure cyberspace and we have much work to do. Assuming that countries already have laws and national policies for cybersecurity in place, operational functional capabilities are needed that include the following: prevention and deterrence; watch and warning; incident management (which includes investigative forensics); what you need to do when you are under an attack; a strategy on how you need to act under an attack; consequence management which includes reconstitution (what to do when the attack is over) and revenge (getting a hold of the people that did this to you). Mr. Goodman emphasized that is very important to figure out what got broken and how to get operational again when there are real problems in cyberspace.

47. However, emphasis is also needed to be focused on prevention, standards, certification, and compliance including adopting best practices and encouraging adherence to standards, for their own good and to ensure that others are secure as well – particularly as everyone is connected. Mr. Goodman noted that users must develop a culture of security so that they are more aware of how to use certain security products, and how to act more secure online. Currently attacks in cyberspace are becoming increasingly sophisticated and thus despite all the cybersecurity work being carried out, current trends are not good as there are more and more capable criminal elements out there. Mr. Goodman emphasized that being an attacker in cyberspace is much easier than being a defendant and counter measures are not being developed fast enough to handle threats. This means that we are in many ways losing the battle against cybercrime.

48. Mr. Goodman then went on to discuss the establishment of national cybersecurity centers in Africa, new technologies and innovation. Mr. Goodman also reminded participants of the survey on the assessment of information security in Africa that he had handed out earlier. Mr. Goodman noted that there are 54 countries in Africa and all of them are developing countries. He stated that for countries in this category, the best approach to developing functional capabilities is to develop operational capabilities and asked workshop participants where these functional capabilities should reside. He proposed several options, such as Computer Emergency Response Teams (CERTs) or in Computer Security Incident Response Teams (CSIRTs), but emphasized that these two terms might be a bit misleading since as what is needed in most African countries is rather something like a National Cybersecurity Center (NCSC). Rather than CERT/CSIRT “fire departments”, a broader approach is needed and a good first question relates to who these entities are supposed to serve.

---

<sup>28</sup> <http://www.itu.int/ITU-D/cyb/events/2007/prai/docs/goodman-watch-warning-prai-nov-07.pdf>

49. Mr. Goodman continued to elaborate on how a NCSC might be envisioned. He put forward that NCSCs are national organizations that provide the country with the operational capabilities needed to protect systems and networks, as well as the users who are dependent on these systems. He opined that NCSCs should be government centers to make the best use of limited human resources. The level of technical talent to fight cybercrime is generally not very extensive in African countries. Therefore, bringing technical experts together in an NCSC might be more effective by encouraging them to interact and help each other. In addition, it is also not clear how best to find, train and retain people in this field. Thus, setting up an NCSC is one way that this might work – particularly to support work by law enforcement and forensics. Mr. Goodman noted that in many African countries the private sector is often too weak and there is little or no business incentive for actors to take on these roles and responsibilities. Furthermore, in these countries, government ICT assets are a major part of what needs protection in the country (e.g., e-government, control over top level domains (TLDs) as this is the country's signature on the Internet and therefore is an asset that the country wants to protect). In concluding his presentation, Mr. Goodman gave some possible options of where the NCSC should be located which included: 1) as an independent organization within a Ministry; 2) as a department in an existing center (e.g., in a National Computer Center); 3) as a unit under the national telecommunications regulatory agency (another set of laws that are not criminal laws); 4) as a unit outsourced to the private sector (domestic or foreign private sector) while emphasizing that many nations would feel uncomfortable doing this, and if outsourced, stringent auditing would be required. Mr. Goodman emphasized that the functions and constraints of the NCSC should be defined by law.

50. In the next intervention, Belhassen Zouari, National Agency for Computer Security (ANSI), Cert-Tcc, Tunisia, presented "[Implementing a National Strategy: The Case of the Tunisian CERT](#)"<sup>29</sup>. Mr. Zouari, the CEO of CERT-Tcc, which is the only [FIRST](#)<sup>30</sup>-recognized CERT on the African continent, gave the participants an overview of how the agency came into being. At the end of 1999, a unit (a "Micro-CERT"), specialized in IT Security was created. The original objective of the unit was to raise awareness amongst decision makers and technical staff about security issues and to create the first task-force of Tunisian experts in IT Security with the goal of monitoring the security of highly critical national infrastructures and applications. In 2002, the unit started to establish a strategy and a National Plan in IT Security. In January 2003, there was a decision of the Council of Ministers, headed by the President and dedicated to informatics and IT Security, to create a National Agency, specialized in IT Security as a tool for the execution of the national strategy and plan. In September 2005, the Computer Emergency Response Team - Tunisian Coordination Center (Cert-Tcc) was launched. Some activities that Cert-Tcc are involved in include watch, warning, and information dissemination, awareness (involving different kinds of awareness-raising campaigns, developing a culture of cybersecurity, information for judges, etc.), information sharing, analysis and collection, incident handling, coordination, etc. The partners that Cert-Tcc engages with differ depending on the activity in question. Cert-Tcc also engages in providing specific expertise on IT security. Mr. Zouari emphasized that ISPs are an important partner in this activity as they manage ports that go in and out of the country. Mr. Zouari also highlighted that Cert-Tcc is happy to share their experiences with other countries in the region which are considering or are currently in the process of setting up similar programmes and initiatives.

51. It was also noted that ITU has an ongoing project to develop a [Botnet Mitigation Toolkit](#)<sup>31</sup> to help deal with the growing problem of botnets where were mentioned in Session 6 on Watch, Warning and Incident Response. 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 background material for the project was made available in December 2007 with pilot tests planned in a number of ITU Member States in 2008.

## Session 7: Government-Industry Collaboration

52. With privatization, the vast majority of each country's ICT networks are now owned and operated by the private sector. A key element of a national framework for cybersecurity and CIIP is bringing industry and government together in trusted forums to address common national security challenges. The basis of successful industry-government partnerships is trust which is necessary for establishing, developing and maintaining sharing relationships between the private sector and government. This session discussed industry-government partnerships and included discussion of telecoms fraud and collaborative solutions deployed to mitigate them. The session moderator, El Hadji Mansor Sy Tandine, a representative of the Présidence de la République du Sénégal, Senegal, proposed that countries in Africa work together to develop solutions for cybersecurity with close collaboration between the private sector and governments. He emphasized that the world needs a safe and secure cyberspace and noted that the recent Internet Governance Forum held in Brazil had also highlighted this point.

<sup>29</sup> <http://www.itu.int/ITU-D/cyb/events/2007/praiadocs/zouari-cert-tunisia-praiadocs-nov-07.pdf>

<sup>30</sup> <http://www.first.org>

<sup>31</sup> <http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html>

53. Luis Sousa Cardoso, Service Quality & Network Security, PT Comunicações, Portugal, opened the session with his presentation on “[Cybercrime and Critical Information Infrastructure Impact](#)”<sup>32</sup>, where he introduced the Forum for International Irregular Network Access (FIINA). FIINA currently has 250 members and in order to join the forum, you have to be an operator, service provider, or carrier. The purpose of the forum is to share information between operators only and no other parties receive information shared. Six companies and organizations started FIINA, and the ITU’s Telecommunications Standardization Sector (ITU-T) Study Group 2 is also involved in their activities.

54. Mr. Cardoso spoke about the current situation with regard to cybercrime in Africa from the experiences he has gained working in the region. He noted that although current research indicates that Africa is neither the source nor target of major cyber attacks, it remains very vulnerable to most major attacks. When looking at the evolution of cybercrime, one can now negate any protection that limited connectivity may have provided in the past. Therefore, the impact of increased connectivity and capacity with Africa with insufficient security technology, expertise and policies is significant. If no measures are put in place, Africa will emerge as an entry point for cyber criminals and terrorists where the continent will be used as a hub to coordinate and launch attacks. Mr. Cardoso presented some of the main issues seen in 2007 which included wholesale fraud, fraud with calling cards, SMS fraud, botnets (service providers are now disconnecting users that are part of botnets because they are not protecting themselves against botnets), threats to e-commerce (including credit card fraud), VoIP fraud as well as, *inter alia*, pharming. He noted that as more people get their hands on a formerly restricted communications infrastructure that has more openness, one should: expect more innovation to come with an influx of new companies with new ideas; expect more security implication as things are not hidden anymore; and expect more need for quality assurance and security services. Another issue to keep in mind is the security of mobile phones as the number of security attacks reported by mobile phone operators in 2006 and 2007 indicates a fivefold increase compared to previous years.

55. Mr. Cardoso also shared some insights into the growing area of online gambling and gaming. Online games are those that are played online via the LAN, Internet or another telecommunications service. Normally, when it comes to online gambling, the only technical requirements for playing online games is a web browser and/or appropriate client software. With the growth of information technology, online gambling and gaming has become a very successful and profitable industry. Mr. Cardoso noted that according to DataMonitor.com, the global online gaming market represented USD 3.2 billion and had 113 million users in 2005. The success of online gaming is changing software business models, and has led to prosperous growth in related industries, such as deployment of broadband networks, online payment schemes, Internet café use, advertising, etc. Mr. Cardoso discussed the economic impact of cybercrime and diminishing related consumer confidence including loss of productivity and trade secrets.

56. Almiro Rocha, Cabo Verde Telecom, Cape Verde, continued with his presentation on “[CVTelecom and Security in Information Systems](#)”<sup>33</sup>. Mr. Rocha shared with the workshop participants a practical case study showing how a telecom company has had to adopt and reinvent itself in a constantly changing threat environment. He explained how Cabo Verde Telecom, a provider of communications services which until 2005 had a monopoly in the market, is dealing with the different challenges. He noted that 2006 was a year of significant regulatory changes in the Cabo Verde telecommunications market, and from the beginning of 2007 there has been liberalization of the telecommunications market in Cape Verde. Due to these changes, Mr. Rocha continued, the company has had to be divided into three different companies under the competition laws (CVTELECOM, CVMOVEL and CVMULTIMEDIA) and this has now become the Group CVTelecom.

57. Mr. Rocha described how the previous model that the organization had used to screen for cases of telecom fraud was based on the collection of international traffic data, which constituted the largest business area for the company. However, the current view of protecting the information systems and infrastructures has grown out of the need to meet demands to mitigate events that hurt the relationship between the provider and its customers who were faced with unrealistic costs. According to the earlier model, the majority of efforts went into the service of telecommunications, now instead the approach has been directed towards protecting the customer service platforms through a standard product available in the market. The company’s existing billing system, Mr. Rocha continued, was not able to detect fraudulent cases in a timely manner. Consequently, the damage occurred increased significantly, especially targeting international traffic which was the main revenue stream for the company. Mr. Rocha explained some of the critical points and challenges that the company has had to deal with when implementing their specific security plan. Here, he mentioned the need to ensure that the company is internally prepared when it comes to security, training and continuously updating the know-how of technicians with regards to related technologies and techniques as well as having the right tools and equipment available to act and take care of incidents in a crisis situation.

## Session 8: Regional and International Cooperation

58. 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 support and

<sup>32</sup> <http://www.itu.int/ITU-D/cyb/events/2007/prai/docs/cardoso-cybercrime-impact-prai-nov-07.pdf>

<sup>33</sup> <http://www.itu.int/ITU-D/cyb/events/2007/prai/docs/rocha-security-in-information-systems-prai-nov-07.pdf>

participate in further concrete actions that could be implemented in the West African region as well as internationally. The moderator of the session, Sekou Kromah, Ministry of Posts and Telecommunications, Liberia, opened the session and introduced the two meeting speakers, Alain Aina and Joel Schwarz.

59. Alain Patrick Aina, Member of ICANN Stability and Security Advisory Committee (SSAC), Togo, in his presentation "[Cybersécurité en Afrique: Appel pour une Collaboration Régionale et Internationale/Cybersecurity in Africa: For Increased Regional and International Collaboration](#)"<sup>34</sup> discussed the cybersecurity situation in the African context, mentioning some of the specific problems that African countries are forced to deal with. Here he mentioned the poor system capacity which increases vulnerability, weak human and technical capacity, poorly deployed and ill managed systems, and poorly-educated users, among other things. Mr. Aina noted that even though there may not be many major interesting targets in the African countries for attackers, the countries are of interest as potential customers for botnets to launch attacks on other destinations.

60. Other things he mentioned as specific to African countries included the increase in the number of cybercenters/cybercafés without the establishment of any kind of legislation that protects young people against pedophiles, etc. Mr. Aina provided the workshop participants with an overview of some regional and international initiatives, mentioning the existing Forums AfriPKI, CERT-Tcc in Tunisia, AfNOG, AfriNIC, AfriSPA, AfLTD, etc. In Africa, he emphasized there is a need to better coordinate initiatives and increase regional and international collaboration. As each individual country may not have sufficient resources (either financial and/or human) to deal with cyber threats, it is even more important for African countries to cooperate. Mr. Aina proposed three principles to boost regional security collaboration: a) provide security based on African expertise, b) avoid reinventing the wheel, and c) adopt a multi-stakeholder approach involving civil society, government, and private sector participants. He added that putting more money into the universities to engage in security work in the region could be a positive and necessary move forward in the region.

61. Mr. Aina concluded his presentation with a few recommendations in order to make Internet security a major focus for regional and international cooperation, mentioning the need for a legal framework and digital confidence for development, increased capacity building, the establishment of national watch, warning and incident response capability in each African country, and ensuring that African nations actively contribute to global cybersecurity efforts.

62. Joel Schwarz, Computer Crime & Intellectual Property Section (CCIPS), Department of Justice, United States of America, in his presentation discussed "[International Cooperation in Cybercrime Investigations](#)"<sup>35</sup>. He started with an overview of the challenges of globalization of criminal investigations and he noted the need to: enact sufficient laws to criminalize computer abuses; commit adequate personnel and resources; improve abilities to locate and identify criminals; and to improve abilities to collect and share evidence internationally to bring criminals to justice. Mr. Schwartz highlighted the urgent need to criminalize attacks on computer networks in all countries, noting that when one country criminalizes certain conduct and another country does not, a bridge for cooperation may not exist (a necessity referred to as "dual criminality"). Extradition treaties and mutual legal assistance treaties are therefore needed. The Budapest [Convention on Cybercrime](#)<sup>36</sup> (2001) can act as a mutual legal assistance treaty where countries do not have an existing treaty, a model to ensure that acts are criminalized in each country – he noted that laws do not need to have the same name or even the same verbiage. Mr. Schwarz emphasized that law enforcement in each country needs experts and expertise dedicated to high-tech crime. He explained that this means experts that are available 24 hours a day that are provided with continuous training and continuously updated equipment.

63. To help workshop participants to better understand how important international cooperation is in the area of law enforcement, Mr. Schwartz thought it would be useful to look at a specific case. The first investigative step in a case is to locate the source of the attack or communication. He noted that often what occurred is relatively easy to discover, but identifying the person responsible is very difficult. He noted through the example that there was the need to share information amongst stakeholders and between countries. He noted that countries must improve their ability to share data quickly, as if not done quickly, the electronic "trail" will quickly disappear. Unfortunately, he noted most cooperation mechanisms take months or years and not minutes.

64. Mr. Schwarz noted that by participating in the Convention on Cybercrime, parties agree to provide assistance to other countries to obtain and disclose electronic evidence. In this regard, Article 30 refers to expedited disclosure of traffic data, the need to preserve domestic traffic data, notifying a requesting country if a trace leads to a third country, and providing sufficient data to allow for the request of assistance from the third country. In order to work together to identify targets, Mr. Schwarz 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. Currently the 24/7 High Tech Crime Network has contact points in about 50 countries. The network is open to all and Mr. Schwarz mentioned that it is easy to join the 24/7 network. The only requirement is availability but this does not necessarily mean a commitment to help. Countries interested in joining the network need to identify a primary contact point who has sufficient technical knowledge when it comes to dealing with cyber-related crimes – particularly as one of

<sup>34</sup> <http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/aina-cybersecurity-africa-praia-nov-07.pdf>

<sup>35</sup> <http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/schwarz-international-cooperation-praia-nov-07.pdf>

<sup>36</sup> <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>

the main issues with cybercrime is handling digital forensic evidence. The person also needs to know something about domestic laws and procedures in this specific topic area. Mr. Schwartz mentioned that countries interested in learning more about the network can contact the US Department of Justice Computer Crime and Intellectual Property Section (CCIPS)<sup>37</sup>

## **Session 9: Wrap-Up, Recommendations and the Way Forward**

65. The final session of the meeting, jointly facilitated by Robert Shaw, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Sector (ITU-D), and David Gomes, Agencia Nacional das Comunicações (ANAC), Cape Verde, 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 CIIP. Mr. Shaw noted that during the three days of the workshop the workshop participants have heard a series of very interesting presentations addressing the major cybersecurity issues faced by countries in Africa, information on the work underway within the ITU, other international and regional organizations, as well as in individual countries to improve cybersecurity. It was also recognized that improving cybersecurity is a global problem and that each country must undertake action to join and support the international efforts to improve cybersecurity. During the workshop, there was sharing of related activities and approaches that have worked in other countries and regions. Representatives from the five main areas provided their main “takeaways” from the event, reflecting not only the discussions that took place in their session but as well their views on some possible and constructive next steps forward.

66. **Sessions 1 and 2 on Frameworks for Cybersecurity and CIIP:** Joseph Richardson, United States of America: brought the workshop participants’ attention to the ITU National Cybersecurity/CIIP Self-Assessment Toolkit, which can assist countries in developing a baseline for cybersecurity and help a country establish where it is and prioritize activities according to its specific needs. As a proposed next step forward, Mr. Richardson used a football analogy to highlight to the workshop participants why initiatives related to cybersecurity need to be undertaken today. He explained that the cybersecurity arena is like a multi-dimensional football field where everyone, all countries, have their own national fields that they are playing on, and what each of us is doing on our field is affecting other nations’ fields. In such a highly complex environment what is needed is a framework that a country can use to organize its national team, to ensure that all the players out on the field at the same time are collaborating to help defend the national pitch in the best way possible but also at the same time contributing to helping protect other countries’ fields. Mr. Richardson explained that ITU is ready to help countries ensure that the relevant people in each economy are aware of their responsibilities, and to talk through the issues and the frameworks that have been discussed during these three days with interested countries. Practically, this could be done in an individual country, maybe even in small groups of countries in the regions, to ensure that small resources are used in the most effective way. Mr. Richardson suggested using the football analogy to share information on elaborate a framework for cybersecurity and CIIP with relevant parties in their countries.

67. **Sessions 3, 4, and 5, Legal Foundation, Regulatory Development and Enforcement:** Marco Gercke, Germany, in his remarks highlighted that there are two kinds of conferences: the ones where you just talk and those where there are some real outcomes. He noted that looking at the recent related ITU Regional Workshops on Frameworks for Cybersecurity and CIIP, which were held in Hanoi, Vietnam, in August 2007<sup>38</sup> and in Buenos Aires, Argentina, in October 2007<sup>39</sup>, these conferences were starting points for many other kinds of development and activities in the respective regions and internationally. He noted that this workshop in Cape Verde is already a conference of outcomes, good contacts have been established between stakeholders and with this network can lead to positive outcomes. He mentioned that he hoped that the practical work seen here and at other related conferences can continue and that countries can get the assistance that they need to establish national frameworks for enhanced cybersecurity.

68. **Session 6, Watch, Warning and Incident Response:** Belhassen Zouari, National Agency for Computer Security (ANSI), CERT-Tcc, Tunisia, noted that the workshop had allowed the meeting participants and speakers to share a lot of different ideas on how to tackle the challenges that countries are experiencing when it comes to dealing with threats to cybersecurity. He felt that the presentations had provided a good overview of the issues to address first and foremost, and also provided useful tools for countries to address these challenges.

69. **Session 7, Government—Industry Collaboration:** El Hadji Mansor Sy Tandine, a representative of the Présidence de la République du Sénégal, Senegal, noted that important messages related to cybersecurity and critical information infrastructure protection have been delivered through the presentations at the workshop, and that it is imperative that cybersecurity is put high up on the agendas of countries. With this remark, Mr. Tandine hoped that the delegates at the workshop will now be in the position to deliver this message back in their home countries. He also expressed his wish that a similar meeting could take place in the region again in the near future. Mr. Tandine highlighted that there are no longer any excuses not to act for enhanced cybersecurity and expressed the need for further harmonization between countries in the region and beyond.

---

<sup>37</sup> <http://www.cybercrime.gov>

<sup>38</sup> <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/>

<sup>39</sup> <http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/>

70. **Session 8, Regional and International Cooperation:** Basil Udotai, Directorate for Cybersecurity, Office of the National Security Adviser, Nigeria, and Alain Aina, Member of ICANN Stability and Security Advisory Committee (SSAC), Togo, outlined their main “takeaways” from the event. Mr. Aina emphasized the need for increased cooperation and better collaboration to ensure that all parties were using the combined energy to do good things for enhanced cybersecurity worldwide. Mr. Udotai said that what he had seen during the three day event showed a convergence not only of the necessity and the reality of cybersecurity but also a convergence of different models and approaches to take for improved cybersecurity. He noted that maybe what is now needed is to shift the discussion to practical measures that can be adopted on the national, regional and international levels to bring about a culture of cybersecurity. He noted that organizations like ITU, the Council of Europe, etc., are ready to help in bringing real solutions to countries in Africa, and some good examples of what can be done in this area have been heard during this event. With this, Mr. Udotai asked the meeting participants to make sure that the leaders of the countries represented at the workshop understand the issues involved and the follow-up actions that are required in order to move forward.

## Meeting Closing

71. David Gomes, Agencia Nacional das Comunicações (ANAC), Cape Verde, 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.

72. In her [closing remarks](#)<sup>40</sup>, on behalf of the International Telecommunication Union, Margarida Evora-Sagna, representative from the ITU Area Office for West Africa, thanked everyone who had directly or indirectly contributed to the success of this West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and CIIP. She relayed special thanks to the local Cape Verde hosts, the Government of Cape Verde, the Ministry of Infrastructure, Transport and Sea, the Ministry of Justice and the Agência Nacional das Comunicações (ANAC) for their outstanding work in making this regional cybersecurity workshop a highly successful event. She continued by mentioning the workshop sponsors, CVTelecom, CVMovel, CVMultimedia, etc. who responded immediately to the invitation to join the organizers in preparing the event, as well as all workshop speakers for taking time out of their busy schedules to share their experiences and expertise with the meeting participants. Finally, Ms. Evora-Sagna thanked the meeting interpreters who had provided excellent simultaneous interpretation in three languages, English, French and Portuguese, during the three day event, as well as the delegates for their attention and active participation and contributions. ITU with its long withstanding activities in the standardization and development of telecommunications 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.

73. The final closing remarks were provided by Jose Manuel Andrade, Minister of Justice, Ministry of Justice, Cape Verde. Mr. Andrade hoped the three days in Cape Verde had proven useful for the workshop participants, with fruitful and engaging discussions. He noted that today one cannot speak about cyberspace with the absence of cybersecurity, and that all are aware of the fact that the Information Society is a real challenge for Cape Verde, as this brings with it not only technical but also political and social challenges. He highlighted that the information society should be closely linked to the general society in a country, and that governments are responsible for putting in place the appropriate measures and tools to overcome the many threats that have been discussed during the workshop in order to build a culture of cybersecurity. Mr. Andrade acknowledged that Cape Verde is fully engaged in a number of initiatives related to setting up a board/committee to take care of sensitive information as data increasingly crosses borders and the approval of a law for cybersecurity. He noted that accession to the Budapest Convention on Cybercrime (2001) is also a goal for Cape Verde. However, Mr. Andrade continued, commitment was needed throughout the country agencies to support these initiatives and to ensure cybersecurity for all citizens.

This draft meeting report<sup>41</sup> is currently open for the comments for a period of 30 days after reception and publication on the workshop website. The email address for comments on this draft report, and for comments on the ITU Cybersecurity Work Programme to Assist Developing Countries (2007-2009)<sup>42</sup>, is [cybmail\(at\)itu.int](mailto:cybmail@itu.int)<sup>43</sup>. For information sharing purposes, all meeting participants will be added to the [cybersecurity-africa\(at\)itu.int](mailto:cybersecurity-africa@itu.int)<sup>44</sup> 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](mailto:cybmail@itu.int).

<sup>40</sup> <http://www.itu.int/ITU-D/cyb/events/2007/prai/docs/evora-sagna-closing-remarks-praia-29-nov-07.pdf>

<sup>41</sup> <http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/doha-cybersecurity-forum-report-feb-08.pdf>

<sup>42</sup> <http://www.itu.int/ITU-D/cyb/cybersecurity/index.html#workprogramme>

<sup>43</sup> Please send any comments you may have on the workshop report to [cybmail@itu.int](mailto:cybmail@itu.int)

<sup>44</sup> Regional ITU cybersecurity mailing list: [cybersecurity-africa@itu.int](mailto:cybersecurity-africa@itu.int). Please send an e-mail to [cybmail@itu.int](mailto:cybmail@itu.int) to be added to the mailing list.