United Nations

Inter-Parliamentary Union

International Telecommunication Union

REPORT

Fourth Parliamentary Forum on Shaping the Information Society

The Triple Challenge of Cyber-Security: Information, Citizens and Infrastructure

Geneva, 18 - 20 May 2011

Organized through the Global Centre for ICT in Parliament
A partnership initiative of the United Nations Department of Economic and Social Affairs
and the Inter-Parliamentary Union inspired by the outcome of the
World Summit on the Information Society

United Nations

Inter-Parliamentary Union

International Telecommunication Union

Report

FOURTH PARLIAMENTARY FORUM ON SHAPING THE INFORMATION SOCIETY
THE TRIPLE CHALLENGE OF CYBER-SECURITY: INFORMATION, CITIZENS AND INFRASTRUCTURE

18-20 May 2011
Room II – ILO Conference Center
International Labour Organization
Geneva, Switzerland

INTRODUCTION

The Fourth Parliamentary Forum on Shaping the Information Society "The Triple Challenge of Cybersecurity: Information, Citizens and Infrastructure" was held from 18 to 20 May 2011 at the Headquarters of the International Labour Organization in Geneva, Switzerland. The event was co-organized by the United Nations Department of Economic and Social Affairs (UN/DESA), the Inter-Parliamentary Union (IPU) and the International Telecommunication Union (ITU).

It was the fourth meeting of members of parliament focusing on issues relating to the Information Society organized within the framework of the Global Centre for ICT in Parliament, a partnership initiative launched by UN/DESA and the IPU at the World Summit on Information Society (WSIS) in 2005.

The aim of the Forum series is to further dialogue among legislators on parliamentary actions that can contribute to the shaping of the future Information Society in view of the WSIS implementation, follow-up and future 2015 review. It also intends to strengthen the interaction at international level between members of parliaments and representatives of international organizations working in this domain with a view to identifying good parliamentary practices for the advancement of ICT-related policies in favour of the internationally-agreed development goals, including the MDGs.

The fourth meeting focused on the representative, law-making and oversight responsibilities of members of parliaments in the area of cybersecurity. It addressed the particular challenges posed by the illicit use of information and communication technologies (ICT), such as the safeguarding of citizens in the connected environment; the protection of State information, data and infrastructures; and the transnational response to cybercrime.

The Parliamentary Forum aimed to further the dialogue among legislators on the different strategic and political priorities implemented at the national level, outline a broad perspective of different national engagements directed at responding to the challenge discussed, delineate the role and responsibilities of parliaments in their legislative and oversight functions with respect to the topic addressed, identify good parliamentary practices and draw recommendations for action by legislatures.

The agenda of the Forum is enclosed as an Annex. The documentation, the recorded webcasts of the sessions and the presentations of the Forum are available at: http://www.ictparliament.org/parliamentaryforum2011/

INAUGURAL SESSION

Mr. Hamadoun Touré, Secretary-General of the International Telecommunication Union (ITU), stressed the importance of ICT in the 21st Century and for the future, and exhorted legislators to cooperate so that ICT can benefit the greatest number of people and can become an effective developmental tool.

He described the work of the ITU as a specialized branch of the United Nations tasked to increase connectivity but he also reminded all present that with greater connectivity comes the need for greater cybersecurity. For this purpose in 2007 ITU launched the Global Cybersecurity Agenda (CGA) as a framework for international cooperation on cybersecurity, and adhered to the International Multilateral Partnership against cyberthreats (IMPACT) that offers adherents access to specialized assistance to counter cyberthreats effectively. Mr. Touré informed the audience that there are 130 member countries of ITU-IMPACT and urged more countries to join, outlining the benefits that derive from ITU-IMPACT membership.

Mr. Touré highlighted three new collaborations between ITU and other institutions. The first one is the collaboration between ITU and the UN Office on Drug and Crime to provide technical assistance on cybercrime and cybersecurity. The second collaboration is the partnership between ITU and Symantec Corporation, a leading ICT security provider. The third one is the Child Online Protection Initiative which, with the President of Costa Rica as patron, will significantly increase activities to protect children online.

Mr. Touré concluded his speech by highlighting that to adapt to the rapid changes in ICT all present must work together to ensure a safe and growing ICT sector.

Mr. Patrice Martin-Lalande, Member of the National Assembly of France, and co-President of the Study Group on "Internet, audiovisual and Information Society", gave the inaugural speech in lieu of Mr. Gurirab, President of the Inter-Parliamentary Union, who could not be present due to commitments as President of the National Assembly of Namibia.

Mr. Martin-Lalande expressed gratitude for the participation of ITU and recognition for its initiatives within the framework of the Global Agenda for Cybersecurity. He also thanked UN/DESA and pointed out the long partnership between the IPU and the United Nations to implement the outcomes of the WSIS.

He applauded the ever greater number of parliamentary groups present in the audience which according to the speaker demonstrated the growing realization of the importance of ICT for the future of our countries.

Mr. Martin-Lalande reminded the audience that in 2003 the IPU adopted a resolution that exhorts parliaments to make use of ICT and spells out the risks of the Information Society and the necessity of international cooperation to combat these risks. He pointed out that if the resolution were to be written again today it would be very different because of the huge changes in ICT, the massive number of new users thanks to the easy access to mobile phones, the new uses of ICT for citizen's greater participation in their governments (for e.g. Tunisia and Egypt) and also the greater criminal use of the Internet.

The rapid evolution of ICT creates serious challenges for countries particularly because governments are used to thinking nationally whereas these issues need to be addressed internationally. In addition, the recent Wikileaks situation highlighted the tension that exists between freedom of expression and transparency.

Mr. Martin-Lalande reminded the audience that the politician's role is to balance the often diverging issues of security, fundamental human rights and social order. He expressed the hope that the Forum will allow participants to welcome progress in international cooperation for cybersecurity.

Mr. Gherardo Casini, Head of the UN/DESA Office, welcomed all present and thanked ITU and IPU for their cooperation in the organization of the Parliamentary Forum series of events.

Mr. Casini discussed the massive increase in mobile phone use and Internet connectivity and how these have changed our social interactions and boosted Internet businesses. He pointed out how there is also a negative side to this in the lack of data security and personal privacy protection, in

addition to a large increase in cybercriminality. National legal frameworks struggle to face criminal activities which ignore national boundaries.

Cybercrime increasingly affects governments directly. Therefore the speaker underlined how it has become a priority for governments to address the issue of cybersecurity, while avoiding negative consequences on the global economy, people's lives and national security. Thus, coordinated international responses become necessary.

Mr. Casini reminded the audience of the importance of not upsetting the balance between security, commercial interests and personal privacy. Parliaments are fundamental in keeping the balance of competing interests by actively adopting legislation to create a people-centered Information Society, maintain economic and social development and guarantee security of information and infrastructure.

Mr. Casini underlined the importance of cooperation and exchange among members of parliaments to strengthen cybersecurity laws and stated that the goal of the Forum is to provide a platform for legislators to discuss cybersecurity issues, identify priorities to be implemented and outline good parliamentary practices.

In his conclusion Mr. Casini looked at the progress there has been in creating an Information Society in the ten years since the first phase of the WSIS but he also recommended focusing on the challenges for the future.

SESSION ONE: *BALANCING FUNDAMENTAL HUMAN RIGHTS AND SECURITY CONCERNS: THE CRITICAL ROLE OF LEGISLATORS*

The session was chaired by **Mr. Ramón Farias Ponce**, Member of the National Congress of Chile who talked about Chile's experience and its goal of contributing to the discussion on security. One of the issues the moderator highlighted is the difference in speed of technology versus the work of legislators. While technology moves and changes rapidly laws need to be debated and agreed upon nationally and internationally and are by nature slower.

Mr. Michael Katundu, Assistant Director, Information Technology, Communications Commission of Kenya, recalled the Declaration of Principles of the WSIS in 2005 which addressed the issue of cybersecurity and the need for ICT in development.

He highlighted the creation of the East Africa Communications Organization (EACO) Cybersecurity Taskforce to enhance cybersecurity in the region. This Taskforce became necessary after making three fiber optic cables operational in the region which has led to a huge increase in ICT use but has also greatly increased the risk of attack. The EACO Taskforce was meant to create a region-wide system to identify and resolve potential and actual cyberattacks. EACO has achieved international recognition and is pushing for the creation of national computer response teams (CIRTs) in each individual member country.

Mr. Katundu then talked about Kenya's specific achievements in the field of cybersecurity. Kenya has enacted the Kenya Communication Amendment Act of 2009, which covers issues of electronic transactions, including Cybersecurity management. The country has also recently promulgated its new Constitution, which lays a strong foundation for freedom of expression and it is in the process of revising all its ICT laws so they will be aligned with the new Constitution.

The speaker concluded by reminding the audience of the global nature of cybersecurity and thus the need for international collaboration in this field.

Mr. Nemanja Malisevic, Counter Terrorism News (CTN) Coordinator, Organization for Security and Co-operation in Europe (OSCE), pointed out that the cyberuniverse is extremely interconnected. He discussed the need to find a balance between fundamental Human Rights, cybersecurity and the role of regulators. He stated that this balance can be achieved only through a comprehensive approach to cybersecurity.

Dependence on IT and the interconnectivity of infrastructure make a secure cyberspace vital to the functioning of a modern state. The OSCE recognizes the need for a more comprehensive approach to fight cybercrime but at the same time the need to safeguard the Internet as a space for free social networking and assembly.

Mr. Malisevic pointed out that a comprehensive approach is important because there is no individual cyberspace. Fragmentation and disconnection present opportunities for criminals. Fragmentation occurs when there are different perceptions of the threat, different ideas on the attribution of the crime, and what steps to take. Fragmentation can make the problem or conflict worse and the OSCE has seen that particularly in the political/military sector where these problems persist.

The speaker stressed that cooperation is vital since cybercriminals are far ahead and specialized knowledge and best practices need to be shared. Cooperation is necessary among countries but also among organizations.

Mr. Malisevic stated that the key to fight cybercrime is to improve user awareness and end-user education and this is where parliaments play a very large role. They need to raise the awareness of political decision makers on the issue of cybersecurity and to sell the idea that cybersecurity is not an individual concern. An educated public will accept regulations more easily.

SESSION TWO: *PROTECTING CITIZENS' PRIVACY IN THE ERA OF SOCIAL MEDIA*

The session was moderated by **Mr. Julio César Valentín Jiminián**, Member of the Senate of the Dominican Republic.

Mr. Patrice Martin-Lalande, Member of the National Assembly of France, stated that with Internet today we can access a wide range of services and exchange information with anyone.

Mr. Martin-Lalande stressed that members of parliament must find a balance between freedom of expression and privacy protection. In democratic societies the respect for privacy is a fundamental right that can be put at risk by the use of Internet and social networks. Personal data can be looked at and used for commercial ends and for targeted advertising. Private data can be used by third parties which the original user is not aware of and, needless to say, criminals can exploit these open exchanges very easily.

The speaker stated that the issue of freedom of expression is complicated because online exchanges should not be limited unless they are illegal or threatening but the computerized collection of data needs to be controlled. Those controlling stored data should be independent bodies and answer to parliaments. Mr. Martin-Lalande also stated that countries should recognize a need for digital removal; there needs to be created a time limit beyond which personal data should be eliminated.

Ms. Solange Ghernaouti-Hélie, Professor, Faculty of Business and Economics at the University of Lausanne, gave a talk on the issue of use of ICT versus the need to protect personal privacy and personal data. She argued that privacy protection and data control are fundamental human rights which need to be upheld and protected.

The Internet is not only a means used by people and companies to stay in touch, foster social and economic development but it is also a tool that allows traceability and surveillance, a highly unregulated marketplace and an instrument of power. Ms. Ghernaouti–Hélie argued that these aspects need to be regulated in an internationally recognized manner.

The speaker underlined that data may be used in ways different than what was intended and stored for longer than planned. Ms. Ghernaouti–Hélie spoke about the problems that arise when people put their personal data on the Internet but then lose control over it. Internet users are responsible for what they write, she stated, but this data can also be used out of context or many years later for a purpose not intended.

The protection of personal data is not governed internationally and therefore its misuse can have serious consequences. People tend to ignore these risks in exchange for the convenience that the Internet offers. According to Ms. Ghernaouti–Hélie, personal data should be considered and protected as part of the Universal Declaration of Human Rights.

Some resist the need for privacy protection for fear of hurting businesses. The issue thus arises whether the protection of privacy is compatible with a mercantile Internet that uses personal data collection as a way to sell its products.

The speaker pointed out that since cyberspace is universal international coordination and cooperation are necessary. In this regard, she stressed the importance of initiatives such as the ICT Global Cybersecurity Agenda and IMPACT.

SESSION THREE: *HIGH-LEVEL DIALOGUE ON BUILDING CONFIDENCE AND SECURITY IN CYBERSPACE*[1]

The Session was moderated by **Mr. Tim Unwin**, Professor at the University of London.

Mr. Hamadoun Touré, Secretary-General, ITU, stated that cybersecurity is one of the most important challenges in ICT faced by the international community, and also one of the biggest tests in international cooperation. He informed that the ITU Global Cybersecurity Agenda (GCA) is built upon five strategic pillars 1) Leagal Measures Legal Measures 2) Technical & Procedural Measures 3) Organizational Structures 4) Capacity Building 5) International Cooperation. He stated that cybersecurity is not an issue for only one country, but a global issue, and we are as strong as our weakest link. He also went on to state that the concept of a superpower is becoming obsolete, since in an increasingly technological world, every individual has the opportunity to become a superpower. For example, the Filipino author of the ILOVEYOU Bug wrote this devastating virus on a computer worth less than USD1000. In closing, Mr. Touré emphasized the importance of protecting children as a normalizing, common denominator between all stakeholders.

Mr. Haruna Iddrisu, Minister of Communications, Ghana, urged that improved legislation, which goes beyond data projection, needs to be put in place to more effectively deal with matters in cyberspace. He also highlighted that much of ICT infrastructure is owned by the private sector, and called attention to their role in the larger cybersecurity discourse.

Mr. Mohamed Nasser Al Ghanim, Director-General, Telecommunications Regulatory Authority, UAE, emphasized the need for a legal framework for cybersecurity. He pointed out that although a number of countries have begun the creation and implementation of legal frameworks, agendas and roadmaps, many countries have not. This is a concern due to the transnational, borderless nature of cybersecurity threats, and international collaboration is the only way to effectively counter cybercrime.

Mr. Ilya Massukh, Deputy Minister, Ministry of Telecom and Mass Communications, Russian Federation, pointed out that ICTs are a locomotive for local economy and increase in GDP, yet they are also a very attractive vehicle for unlawful and illegal elements. He stated it was of upmost important to discuss cyberthreats and encouraged multilateral cooperation. In closing he said that Russia is only one country and that one country cannot develop rules to govern the global phenomenon which is the Internet. To this end he reemphasized the role of international cooperation.

Mr. Mohd Noor Amin, Chairman, International Multilateral Partnership Against Cyber Threats (IMPACT), drew parallels between infectious diseases and cybersecurity. He pointed out that during a disease outbreak there is international cooperation and coordination in moderating ports of entry. This model is possible through concerted global action and institutional assistance. The Chairman hoped to replicate this model for cyberthreats, using IMPACT as a vehicle.

Mr. John Mroz, CEO, EastWest Institute (EWI), said that due to the increasing digitalization of the global economy, cyber criminality has been growing. He drew attention to the speed of advancements in technology in contrast to the slow adaptation and creation of agreements, policies, standards and regulations in which to govern them. He addressed the lack of trust between international actors and gave examples of some activities which encouraged discussion and built trust between countries: the Chinese-American partnership which aimed to tackle spam, and the Russo-American initiative to agree on 23 definitions. In closing he emphasized that more initiatives which provide solutions and build trust are needed.

Mr. Rainer Wieland[2]**,** Vice-President, European Parliament, addressed the speed at which technological advancement is increasing, which in turn creates new opportunities for cybercrime. The Vice-President urged the creation of a culture to combat cybercrime which is needed if we wish o build trust and confidence in our efforts. In closing he stated we must address and educate two parts of society: the younger generation who know more than their grown-up counterparts and the lder generation who know far too little.

Ms. Marielos Hernandez, Executive President of PANI, Costa Rica, reported on Costa Rica's efforts in dopting global online child protection. It included initiatives for raining in prevention,

1 This session was part of the High Level Dialogue of the WSIS Forum. It created a linkage between the two events.
2 Co-Chair of the Global Centre for ICT in parliament.

educating children about cyberthreats, establishing guidelines for industry codes of conduct, and establishing national informational hotlines. The President, by presidential decree, also created the National Online Security Commission which is a multistakeholder and interdisciplinary initiative to deal with cyberthreats.

During the following **discussion** the presenters were asked by the moderator to indicate what, in their views, is most important in building confidence amongst citizens with regards to cybersecurity. Mr. Touré reemphasized that cybersecurity will only be achieved when we have a global framework and that the protection of children can act as a common denominator on which to build our efforts. Mr. Wieland stressed the importance of having a legal agenda and a list of core crimes which can be commonly agreed upon. Mr. Massukh stated that there is no single bullet for global cybersecurity regulations but that each country should take steps to protect citizens. He also emphasized the need for education, especially as it related to new trends such as digital signatures. Ms. Hernandez stated that when we talk about children we have to talk about children within both a national and multidisciplinary, inter-institutional global framework. She also highlighted the need to teach prevention to parents and educators. Mr. Mroz agreed that the discussion of child protection creates awareness and that awareness is critical in making the dialogue on cybersecurity relevant to the general population. Mr. Al Ghanim pointed out that there is a need to train people on evolving threats on a monthly basis, and also that there is a need for basic awareness in actions.

Mr. Iddrisu raised the question of how governments can commit to the safety and security of cyberspace if cybersecurity is a transnational problem. Mr. Amin highlighted the strong motivations and ideologies of cybercrime perpetrators and that only international collaboration can effectively counter them. He also stressed that the private sector has a responsibility to share information regarding which systems have been compromised.

Participants highlighted that cybercrime is not a technical issue but an economic and societal issue. Mr. Mroz emphasized that a new way of thinking is required to effectively deal with cybersecurity and that there is a need to involve ourselves in discussions surrounding cybersecurity issues.

The presenters then expressed their views about possible ways to counter cybercrime. Mr. Wieland stated the need for a clear definition of cybercrimes and the need to find a code of conduct for international procedures in prosecution. He stated that there is a need to address the issue of state criminality at the United Nations level and resolutions are needed to effectively engage it.

Mr. Touré stated that the nature of technology will always put it ahead of legislation, and that we need to operate as though we are in a time of war, with a strong code of conduct and best practices for Member States to follow. He re-emphasized the need for action and not deliberation. He highlighted ITU's role in awareness-building, not only through the Member States but also through the partnership with 700 private companies. He pointed out that a new global treaty would be needed for cyberspace – no longer will it be restricted to countries but it should also involve corporations and the private sector.

Mr. Mroz stated the need for better measurement tools of cybercrime and urged the private sector to cooperate in reporting how cybersecurity is affecting them. He closed by emphasizing the need for action-based initiatives.

Mr. Iddrisu, Mr. Al Ghanim and Mr. Amin stressed the need for more international cooperation. Mr. Iddrisu called for the need of a comprehensive framework that is mindful of differences between countries and cultures. Mr. Al Ghanim said that prerequisites will be needed for a global treaty, proper response rates and the need for international actors to take violations seriously. He also stated the need for the private sector to participate in a larger global framework due to its deep involvement in ICT Mr. Amin re-emphasized IMPACT's agenda for capacity-building and an invitation to utilize the training and programmes offered by IMPACT.

Ms. Hernandez stated the need for a human rights approach by investing in education and health. She stressed the importance of allowing children and younger people to participate in the larger discussion of cybersecurity.

Mr. Massukh re-emphasized the need for fighting child pornography. He also highlighted the need to regulate social networks more strictly due to the high amount of child participation. He agreed that the private sector should be involved in the discussion of a global framework.

SESSION FOUR: *ENFORCING APPROPRIATE LEGAL FRAMEWORKS TO FIGHT NEW AND EMERGING FORMS OF CYBERCRIME*

Mr. Timothy Hamel-Smith, President of the Senate of Trinidad and Tobago, opened the session stating that this is a borderless world and the difficulty is to find the appropriate legislation that will bring us to speed in the fight on cybercrime. He expressed his concern that 'silos' will be created, in which each country closes in on itself without addressing the international issues of extradition and cybersovereignty. He recalled the Council of Europe's convention on cybercrime, which tries to minimize the procedural and jurisdictional obstacles to fighting cybercrime effectively.

Mr. Hamel-Smith also expressed the fear that in the future there will be cyberhavens which will be the new dimension to be tackled. He stated that probably the next war will be a cyberwar in which one nation shuts down another. The creation of an international cybercrime court is necessary.

Mr. Zoltán Précsényi, Government Relations Manager, European Government Relations Team, Symantec Corporation, stated that putting in place a legislative framework is a political decision. In taking it, policy makers need to be aware of the fact that investigative tools may be, to some extent, privacy invasive. As such, they can be faced with a lack of public acceptance, and this can happen even if and where the policy objective is perfectly legitimate and perceived as such.

Mr. Précsényi stated that once a framework is in place, enforcing it is a different matter. Measures taken must make sense technologically and be workable in practice. Issues such as attribution of cyberattacks (who is behind the attack) and jurisdiction (where is the attacker located) are inherent to the cross-border nature of the cyberspace. Sorting out these requires a common understanding on harmonized definitions and legislation across countries, and international cooperation between authorities, meaning effective mutual legal assistance processes. Last but not least, law enforcement authorities need to have the proper resources, commensurate with the threat they are facing and consistent with the volume of criminal activities they are addressing.

About the content of the framework the speaker stated that new and emerging forms of cybercrime are mostly "new" in their volume and sophistication (the growth is constant and exponential), and "emerging" in the technologies they leverage (e.g. mobile). Cybercriminals are after fortune, not fame, so they will attack anything likely to yield substantial gains: as new technologies emerge, cybercriminals will turn to them and use them for malicious purposes as soon as it becomes worthwhile. However, from a legal standpoint, the concepts already existing e.g. in the Council of Europe's ten-year-old Cybercrime Convention (ETS 185) are sufficient to address most, if not all new forms of cybercriminality.

Mr. Précsényi concluded that the way forward is for countries around the globe to implement these concepts in their national legislation in a harmonized and coherent fashion, to define suitable sanctions, to equip law enforcement authorities with sufficient tools and resources to do their job properly, and devising effective cooperation mechanisms to address the cross-border nature of cybercrime.

Mr. Steve Santorelli, Director of Global Outreach, Team Cymru, being a professional investigator, gave a speech outlining the realities and practicalities of what happens in investigation and enforcement of cybercrimes. He stated that law enforcement agencies know exactly who the criminals are, but enforcement fails time and again. It fails because of legislation and politics, the lack of technical competence of prosecutors and judges, and the sluggish pace of the bureaucratic decision-making process.

The speaker talked about emerging crimes and explained that it must be clear to all that Internet has always been driven by business needs, not by security needs. The new technologies used by cyber criminals include geo-location, user-generated content and cross-platform MAUERS.

Mr. Santorelli also pointed out that there has been a change in perception on privacy on the part of users. He then stated that there is a new modulization of criminal activity with many people participating in cybercrimes rather than one person committing a crime from conception to action.

Ms. Jody Westby, CEO and Founder, Global Cyber Risk, focused her presentation on the concept of bridging the security divide. She pointed out that in the past people referred to the need to

bridge the digital divide but now, with the enormous expansion of Internet use, the problem has become the security divide. Many systems in many different countries are not updated, software continues to be vulnerable and many countries do not have the trained personnel to guarantee cybersecurity. The speaker explained that IMPACT has been a great achievement but much work still remained.

At the moment cybercrime laws are inconsistent or worse there are no laws at all. In some countries these types of crimes are given civil penalties which are too low to be an effective deterrent.

Ms. Westby stated that many parliaments have little knowledge in ICT, lack qualified law enforcement personnel and have inexperienced judges and lawyers. The problem is that cybercriminals take advantage of these weaknesses.

The goal for the future is geo-cyber-stability, which the speaker defined as the ability of all countries to use Internet for national security and economic, political and social benefit. It is vital that a nation's infrastructure not be disrupted and an international framework needs to exist for countries to assist each other and to spread information on scientific and technological advances. Ms. Westby highlighted that both the Council of Europe Convention on Cybercrime and the ITU's tool-kit on cybercrime legislation can be used by countries to develop a legal framework.

Ms. Westby stated that it is necessary to have a global plan and global commitment to these issues and encouraged the creation of a global coordination centre. Since the adoption of international treaties is very slow Ms. Westby proposed that each country make its own laws trying to harmonize them with the rest of the world and then only later work on an international treaty.

The following **discussion** centered on the need for international cooperation to solve cybercrimes. Some participants stated the need for more precise definition of the crimes being discussed and the fact that prevention may be more useful than sanctions.

SESSION FIVE: *PROTECTING CHILDREN ONLINE*

The session was moderated by **Mr. Manuel B. Dengo**, Permanent Representative, Permanent Mission of Costa Rica to the United Nations Office and other international organizations in Geneva.

Ms. JeoungHee Kim, Policy and Legal Analyst at the ITU, introduced ITU's Child Protection Initiative which was discussed during the two phases of the WSIS in 2003 and 2005 when world leaders entrusted ITU with dealing with the challenges of ICT, and ITU made a commitment to the protection of children in cyberspace.

The ITU Child Online Protection Initiative (COPI) was launched under the Global Cyber-Security Agenda (GCA) to bring together all the stakeholders in this sector to ensure a safe and positive online experience for children everywhere.

Ms. Kim stated that the ITU drafted four different Child Protection Guidelines for different audiences: 1) policy makers/legislators, 2) industry, 3) parents and educators, and 4) children.

Elaborating on the guidelines for policy makers Ms. Kim highlighted that legislators need to consider the existing legal framework and to ask themselves whether the current laws already cover the issue of cybercrime, keeping in mind that sometimes laws dealing with off-line crimes can be used for the same crimes that occur online.

She stated that it is important that policy makers lead the way so that all stakeholders (industry, governments, parents and educators) work together. Policy makers must also be sure to commit the necessary resources to implement the rules. In addition, they need to encourage industry to regulate itself, while at the same time educate their citizens and raise awareness of the issues.

The speaker then pointed out that ITU is now moving from issuing guidelines to taking action based on five strategic pillars: 1) legal measures, 2) technical and procedural measures, 3) organizational structure, 4) capacity building and 5) international cooperation. ITU is working on offering a road map to harmonize laws. In its Plenipotentiary Conference it agreed to Resolution 179 which governs online protection and gives clear mandates in this important sector.

Ms. Deborah Taylor Tate, Former Commissioner, Federal Communications Commission, United States of America, highlighted the work that ITU has carried out and encouraged parliamentarians to accept the assistance that ITU can offer.

She reminded the audience that the Secretary-General of ITU was the first to connect children to the issue of cybersecurity. She urged those present to participate in ITU events and meetings which can help educate people and explain why laws are necessary.

The goal of ITU, the speaker explained, is not to limit access to ICT but rather to train youths and promote laws to protect children's use of Internet.

The speaker stressed that laws should allow a multi-jurisdictional exchange of information. She also stated that law enforcement will need new authority to be more effective in the quest for cybersecurity, decide which age groups need to be protected and what the definition of child is.

Ms. Taylor Tate encouraged the parliamentarians present to use their unique position to discuss the importance of child online protection by holding parliamentary hearings and urging industry to self-regulate on this issue.

Ms. Clara Sommarin, Child Protection Specialist, Exploitation and Violence, Child Protection Section, Programme Division, UNICEF, began her speech by pointing out the many benefits for children that have come from the massive expansion of information technology use. These benefits include full participation of children in society, access to culture, entertainment and education.

Naturally there are also unwanted consequences to greater Internet connectivity. Children have always been exposed to violence and exploitation but now the scale of the problem has changed.

Ms. Sommarin stated that there are many different forms of harm. There is the expansion of online solicitation of children and the wide-spread streaming of live abuse videos. Ms. Sommarin also stated that children themselves often act in a risky manner. They forget that Internet is seen by everyone and anyone for possibly a very long period of time. There is also the expanding phenomenon of child on child violence, more often called cyberbullying, which has become more

invasive. Finally there is the issue of children being exposed to violent images and adult pornography.

The speaker reported that UNICEF has begun a study on the effect of ICT with relation to pornography and violence on children. The research, most of which was carried out in the developed world, has shown that younger children tend to become victims of pornography and violence online, while older, adolescent children can become perpetrators of peer on peer violence.

The research also found that there is a difference in the way children access Internet between developed and developing countries. In developed countries children tend to access Internet more at home or at school so they tend to be online many more hours. In developing countries use seems to be more in cybercafés but this is changing as mobile phone use spreads. One thing that is in common all over the world is that often adults do not know how children use ICT.

SESSION SIX: *EXERCISING OVERSIGHT ON THE SECURITY OF CRITICAL INFRASTRUCTURE*

Mr. Michael Frendo, Speaker of the House of Representatives of Malta, stated in his introduction that protecting critical infrastructure is a key component of cybersecurity. Some areas are more "critical" than others such as the military defense system. Mr. Frendo highlighted that an attack on a country's infrastructure is a grave concern for parliaments who should be guardians of public confidence.

Mr. Andrea Rigoni, Director General, Global Cybersecurity Centre of Italy, touched upon various aspects of critical infrastructure protection.

One of the problems, in Mr. Rigoni's view, is that countries are aware of national infrastructure but often have trouble imagining regional or international infrastructure. Defining telecommunications and the Internet as national infrastructure is very limiting. The speaker stated that people tend to think of infrastructure as something physical but Information Services or the Internet are certainly not tangible and therefore a different terminology is necessary. Mr. Rigoni preferred to talk about 'critical services'.

An important characteristic of the Internet and infrastructure served by ICT is that they are in some countries mainly managed and operated by private entities. It is therefore important that governments manage to have a positive collaboration with the private sector in order to ensure protection of the infrastructure.

Examples of "critical infrastructure", said Mr. Rigoni, are the energy sector, transportation, ICT and Internet. There are also certain hidden services that are critical such as the DNS (Domain Name Service) which is a global service with no clear owner that works because of many interdependencies that need to be protected.

Mr. Rigoni's suggestion to improve the security of infrastructure is to strengthen the role of information sharing. The problem with this is that often the rules that protect data can harm the attempt to share important information.

Mr. Carlos Cantero, Member of the Senate, National Congress of Chile, presented the experience of the Chilean Parliament. The Parliament has found on its computer systems 1,500-1,700 viruses per month and 1 million attacks. The attacks increase even more when there is a period of particular political conflict.

According to Mr. Cantero the growing number of attacks on the Parliament of Chile is very serious. The Parliament has invested a great amount of money to prevent attacks. It has tried to create a system of internal security by making departments separate and water-tight from each other. It has also tried to enact a system of external security by using encryption and information policy which limits access to certain information. Departments are not allowed to be linked directly to the Internet. The Parliament of Chile also carries out internal security audits and perimeter audits, and runs tests to see if intrusions are possible.

He urged the need for regulation on the use of Internet and encouraged the United Nations and ITU to promote rules on cybersecurity to foster prevention.

Mr. Javier D. De Andrés, IT Director, Congress of Deputies of Spain, gave a presentation on the difficulty of fighting cybercrime.

In 2010, Spain passed a royal decree that proposed a national security scheme and set conditions of trust so data communication can function effectively. The decree forces the state to regulate electronic exchanges. Despite all security measures taken attacks to the Parliament's infrastructure still occur.

Mr. De Andrés reported that the Parliament's webpage was recently attacked when the Parliament was discussing a law that would limit Internet use. The Parliament's web page was swamped by millions of e-mails and had to shut down for a short period of time. The first idea was to shut the page down completely but this would have seemed a move to limit the freedom of expression because it is hard to prove that all those e-mails had a malicious intent. Eventually in response to the protests the law under discussion was slightly changed.

The speaker wondered how to avoid this occurrence in the future. One of the measures taken was to change the web page design by dividing it into pieces so that even under attack some part of the web page will still work.

SESSION SEVEN - *THE PARLIAMENTARY RESPONSE: GOOD PRACTICES IN ENHANCING CYBER-SECURITY*

The moderator of the session, **Mr. Sebastiaan von Solms**, Professor, Academy for Information Technology, University of Johannesburg, South Africa, initiated the panel discussion by urging parliamentarians to face the issue of cybersecurity by giving the audience some good advice, offering concrete examples from their own countries and sharing their experiences. Mr. von Solms offered the experience of South Africa where all banks, for example, offer Internet banking but no one takes responsibility when their clients lose money because of cybercrime. With this example he highlighted the concept that parliamentarians must have an oversight role on behalf of citizens.

Mr. Michael Mukuka, Principal Clerk (ICT) and Member of the National Working Group on Cybersecurity, National Assembly of Zambia, gave a presentation about the response by parliaments to cybersecurity using the example of his country.

In 2004, the Parliament passed the Computer Misuse and Crimes Act which was improved in 2009 by the Electronic Communication and Transaction Act. Through the work on these acts, Zambian parliamentarians realized that their work, the information they disseminate and their infrastructure needed to be secure.

In 2009, the Parliament also created necessary statutory bodies and regulatory bodies to fight cybercrimes. In particular the speaker highlighted the function of the Zambia Information and Communication Technology Authority (ZICTA) and the National Working Group on Cyber-Security conceived after a 2008 ITU Conference. The Group offers a multi-sectoral approach to cybersecurity and drafted a national cybersecurity strategy.

In Mr. Mukuka's view, the most important role for parliamentarians on the issue of cybersecurity is oversight. Parliamentarians, however, are for now not carrying out this role well since there is no focused attention on cybercrimes and security. Mr. Mukula stated that Zambia needs to speed up parliament's response to cybersecurity in particular by using inter-parliamentary cooperation and existing initiatives.

Mr. Zondol Hersesse, President of the Constitutional Laws Committee, National Assembly of Cameroon, spoke about the importance of protecting ICT to allow the development of an Information Society. The enormous multiplication of forms of electronic communication and information has created new forms of criminality. There is therefore an important role for parliaments and governments to play in guaranteeing security in this field.

The speaker highlighted the laws in Cameroon on the development of ICT. In 1998 the Parliament passed a law establishing the Cameroon telecommunication sector which allowed the private sector access to the telecommunication business. Mr. Hersesse also underlined the generous resources Cameroon dedicates to telecommunication and the laws created to promote cybersecurity. He then talked about the Parliament of Cameroon's role in controlling the actions of the government in enhancing cybersecurity by holding question/answer sessions each week and parliamentary inquiries. In addition, the speaker reminded the audience about the educational role a parliament has of spreading the word about innovations in cybersecurity, and the use of new technologies in daily life.

Mr. Hersesse concluded by underlining the importance of international meetings to keep participants updated and to make their work more efficient in their own countries.

Mr. Marco Gercke, Director, Cybercrime Research Institute, outlined the three key findings he always shares with parliamentarians when advising parliaments on the response to the issue of threats to cybersecurity.

The first finding is the need for constant monitoring and for immediate response. Since cybersecurity is constantly evolving - types of attack, their scope and methods change - thinking on cybersecurity needs to be amended continuously.

The second key finding the speaker outlined is response. Parliaments must no longer think nationally but globally. Parliamentarians must look at what the international community is doing and at the existing initiatives. The speaker mentioned the Global Cyber-Security Agenda and the Convention on Cyber-Crime which has been ratified by 30 countries. He pointed out that the Commonwealth countries, East Africa and Caribbean nations all are moving in the right direction,

and mentioned in particular the experience of the Caribbean nations who created a legal framework that was quickly implemented and put to practical use.

The final key finding Mr. Gercke talked about was the concept of capacity building. The speaker underlined that the information to guarantee cybersecurity is there. Rather than spending money on new information, parliamentarians should focus on political aspects and policy decisions that fit the demand of their countries. He pointed out that the 2009 ITU Cyber-Crime Guide for Developing countries defines crimes and legal response, and offers best practices and good examples to follow.

SESSION EIGHT - *INTER-PARLIAMENTARY COOPERATION FOR CYBER-SECURITY*

The moderator of the session, Mr. Andy Richardson, Information Specialist at the Inter-Parliamentary Union, reiterated that cybersecurity is a global issue that cannot be tackled in isolation. Cooperation can come about through bilateral agreements and also through International Organizations such as the United Nations and ITU, working closely with parliaments. The moderator asked the speakers to come up with practical ideas and suggestions.

Mr. Marco Obiso, Coordinator, Inter-Sectoral Activities at ITU, talked about the importance of establishing an international and regional legal framework for cybersecurity.

Mr. Obiso stated that many countries have new regulations on cybersecurity but very few laws concerning cooperation and more specifically extradition. He highlighted the fact that as long as there is even only one country without a legal framework for cybersecurity cybercriminals will migrate there and the country under attack can do nothing to solve this problem.

The speaker pointed out that some countries have lack technical means and organizational structure to coordinate the work within the government. For example few countries have a Computer Incident Response Team, which acts as a focal point for efforts to secure cybersecurity. In all of Africa only one country has this capability.

Mr. Obiso also highlighted the lack of international cooperation and awareness of the issue. He recalled the ITU Global Cyber-Security Agenda aimed to create a framework for international cooperation. Since 2008, ITU has been in the implementation stage, trying to press countries to implement the framework for international cooperation.

The ITU has identified three areas where coordination needs to be strengthened. The first one is the legal sector where laws need to be harmonized. The second is the technical area where there needs to be a standardized approach to the production of devices. The last area where coordination is vital is the organizational sphere where governments need to put in place organizations that will monitor cybersecurity and coordinate the many stakeholders in this issue.

To assist in the coordination of legal measures the ITU has two tools it can offer countries: 1) the tool-kit for cybercrime legislation and 2) the ITU's cybercrime guide for developing countries.

Mr. Obiso stressed that ITU needs to go along with steps taken by parliamentarians. One way this can happen is with international partnerships. In this regard, he mentioned IMPACT, the creation of a global response centre to be able to give early warnings of potential problems coming up, and something like the Electronically Secure Collaborative Application Platform for Experts (ESCAPE), which provides a means to aggregate expertise.

The speaker concluded by saying that 130 countries, which is two-thirds of the United Nations member states, have signaled their desire to collaborate and provide joint technical assistance. Different entities need to communicate and work together and parliamentarians need to be part of this, share their expertise and make sure all parts of their governments are involved.

Ms. Gillian Murray, Chief, Conference Support Section, Focal Point for Cybercrime at the United Nations Office for Drugs and Crime (UNODC), gave her presentation on the work carried out by UNODC.

The speaker stated that the first step in fostering cyber-ecurity is creating the necessary legislation which is a particularly big challenge in developing countries. The United Nations Convention on Transnational Crime, signed by 162 member states, gives a mandate to UNODC to help countries in their legislative framework and also provides a platform to provide mutual legal assistance and extradition rights. The speaker pointed out that other United Nations Resolutions were too limited in scope to be useful for cybercrime enforcement.

Ms. Murray told the audience that in the last year there has been a lot of discussion about drafting a new Convention but for now no consensus was reached. In the meantime the United Nations has undertaken a study on the issue of cybersecurity to try to look at what is on the ground already through a questionnaire distributed to all member states.

Mr. Frederick Wamala, Research Associate/Cybersecurity Advisor, Department of Management, Information Systems and Innovation Group at the London School of Economics, talked about the ITU National Cyber-Security Strategic Guide, which is the practical implementation of the Global Cyber-Security Agenda (GCA), and how exactly parliaments can put this Agenda to use in their own countries.

The speaker said there are three fundamental issues which make up the GCA: 1) legal measures, 2) technical procedures and 3) organizational structure.

The GCA was created to offer parliaments a tool for cooperation and some useful definitions of the issues at hand. The GCA is based upon the "ends, ways and means" model. It declared that cybersecurity is context-based, which means that the GCA understands that each country has its own objectives, conditions and values which must be understood before implementing any cybersecurity measures. The GCA is also risk-management based which means that since there are often limited resources, countries need to identify which cybersecurity threats are the most harmful and tackle those first. The GCA has also adopted a balanced approach, which means that responses to cybersecurity must be moderated to not risk harming commercial benefits.

Mr. Wamala highlighted that to be successful cybersecurity needs to take into account national values which are defined as the rights of citizens, state security and national economic interests.

The speaker then outlined what parliamentarians can actually do. They need first of all to understand the impact that cyber-security has on the economy, social order and public safety of their country. Mr. Wamala then listed all the actions that members of parliaments could take to further cybersecurity starting with making laws and treaties, setting the government's agenda and deciding which of their government's committee does what. The speaker highlighted the fundamental role that parliaments play and how they can be assisted in their action by the ITU National Cyber-Security Strategic Guide. Lastly he stated that it would be important to create a cybersecurity culture by working on people's awareness of the issue.

The following **discussion** highlighted the difficulty in moving from knowledge to action and in implementing legislation. Ms. Murray stated that the UNODC's first step in assisting countries is to review if their laws are adequate and to train those who will be involved in the implementation process. She stated that the UNODC maintains a presence in the country during the implementation process and stressed that in certain countries there is a lack of political will which hampers efforts. The discussion also highlighted that a very big effort needs to be made on coordination and communication both at the international level and within individual countries.

CLOSING SESSION

Mr. Gherardo Casini on behalf of UN/DESA thanked all participants for attending. He then explained to the audience the role of the Global Centre for ICT in Parliament, which is a joint initiative of the United Nations and the IPU launched in 2005. He stated that one of the two main objectives of the Centre is to strengthen the role of parliaments in the promotion of the Information Society, through fostering ICT-related legislation.

Mr. Casini stressed that the Forum highlighted the important and urgent role that parliamentarians play to further cyber-ecurity in their countries through their three main responsibilities of law making, representation and oversight.

Mr. Andy Richardson, on behalf of the IPU, thanked all present for their active participation and urged parliamentarians to keep in contact. He stated that the framework for coordination is there so they must make good use of it.

Mr. Marco Obiso, on behalf of ITU, stated that he felt that a mechanism has been created to foster coordination and hoped that there would be active participation in the future.

Mr. Ramón Farias Ponce, Member of the National Congress of Chile, read a Final Declaration prepared by a committee formed by members of parliaments (enclosed as Annex) which was endorsed by all parliamentary delegations participating in the Forum.

AGENDA

Day 1 - 18 May	
15:00 – 15:30	Inaugural Session • **Hamadoun Touré**, Secretary-General of the International Telecommunication Union (ITU) • **Patrice Martin-Lalande**, Member of the National Assembly of France • **Gherardo Casini**, Head of the Office of the United Nations Department of Economic and Social Affairs
15:30 – 16:15	**Session One** ***Balancing fundamental human rights and security concerns: the critical role of legislators*** The Internet has become a potent means of political expression and civic action, as well as a vehicle for sharing users' generated content, real-time news and information. In some cases, however, these exchanges may pose a threat to the security of national interest or businesses. The session will focus on the responsibility of the legislators in ensuring that the fundamental rights of the citizens are preserved while providing businesses and governments with appropriate means to respond to the growing security challenges. ***Moderator**: **Ramón Farias Ponce**, Member of the National Congress of Chile* • **Michael Katundu**, Assistant Director, Information Technology, Communications Commission of Kenya • **Nemanja Malisevic**, Counter Terrorism News (CTN) Coordinator, Organization for Security and Co-operation in Europe (OSCE)
16:15 – 16:30	Coffee break
16:30 – 18:00	**Session Two** ***Protecting citizens' privacy in the era of social media*** As an unprecedented amount of private information is revealed via online social networks by ordinary citizens, including youngsters, legislators are increasingly called upon to ensure the safeguarding of citizens' privacy and data protection from commercial and non-commercial actors, as well as from criminal organizations. The session will discuss the impact of the use of social media on users' privacy and the response options available to governing institutions. ***Moderator**: **Julio César Valentín Jiminián**, Member of the Senate of the Dominican Republic* • **Patrice Martin-Lalande**, Member of the National Assembly of France, co-President of the Study Group on "Internet, audiovisuel et société de l'information" • **Solange Ghernaouti-Hélie**, Professor, Faculty of Business and Economics, University of Lausanne

Day 2 – 19 May	
09:00 – 11:15	**Session Three ITU High Level Panel**[3] ***Building Confidence and Security in Cyberspace*** The growing incidence of cyberthreats and cybercrime, from financial and identity related frauds to illicit use of ICT services and applications, undermines the willingness to fully exploit the potential benefit of the Information Society, limiting the opportunity to use ICTs as enabler to improve effectiveness and efficiency of the online presence. This session will focus on the measures that can be adopted to foster an enabling environment for to confidently use Information and Communication Technologies. ***Moderator**: **Tim Unwin**, Professor, Royal Holloway, University of London* • **Hamadoun Touré**, Secretary-General of the International Telecommunication Union (ITU) • **Rainer Wieland**, Vice President of the European Parliament • **Haruna Iddrisu**, Minister of Communications, Ghana • **Mohamed Nasser Al Ghanim**, Director General, Telecommunications Regulatory Authority, United Arab Emirates • **John Mroz**, CEO, East West Institute (EWI) • **Mohd Noor Amin**, Chairman, International Multistakeholder Partnership Against Cyberthreats (IMPACT) • **Marielos Hernandez**, Executive President, PANI, Costa Rica
11:15 – 11:30	Coffee Break
11:30 – 13:00	**Session Four** ***Enforcing appropriate legal frameworks to fight new and emerging forms of cybercrime*** By adopting appropriate legal frameworks for prosecuting cybercrimes and overseeing their implementation by governments and law-enforcement agencies, parliaments have an important role to play in curbing the rising tide of cyber-criminality. The session will focus on the growing concern of businesses and citizens towards new and emerging forms of cybercrime and the legal measures to fight them. ***Moderator**: **Timothy Hamel-Smith**, President of the Senate of Trinidad and Tobago* • **Zoltán Précsényi**, Government Relations Manager, European Government Relations Team, Symantec Corporation • **Steve Santorelli**, Director of Global Outreach, Team Cymru • **Jody Westby**, CEO and Founder, Global Cyber Risk
13:00 – 14:30	Lunch break

3 The High Level Panel is not formally part of the Parliamentary Forum. Interpretation is available in English and French.

14:45 – 16:15	**Session Five** ***Protecting children online*** The use of the Internet greatly increases the risks that children face from predators. This session will examine some of the special provisions that parliaments may adopt to protect children online based on the work carried out at the international level by the ITU and other international organizations. ***Moderator**: **Manuel B. Dengo**, Permanent Representative, Permanent Mission of Costa Rica to the United Nations Office and other international organizations in Geneva* • **Jeoung Hee Kim**, Policy and Legal Analyst, ITU • **Deborah Taylor Tate**, Former U.S. Commissioner, Federal Communications Commission, 2009 WTISD Laureate • **Clara Sommarin**, Child Protection Specialist, Exploitation and Violence, Child Protection section, Programme Division, United Nations Children's Fund (UNICEF)
16:15 – 16:30	Coffee break
16:30 – 18:00	**Session Six** ***Exercising oversight on the security of critical infrastructure*** The increasing number of cyber-attacks on national infrastructure, from internal and external sources, is becoming a priority concern for governments. This session will focus on the parliament's oversight role in ensuring that the executive is appropriately building its capacity to respond to these threats and exercise it effectively. ***Moderator**: **Michael Frendo**, Speaker of the House of Representatives of Malta* • **Andrea Rigoni**, Director General, Global Cybersecurity Centre, Italy • **Carlos Cantero**, Member of the Senate, National Congress of Chile • **Javier D. De Andrés,** IT Director, Congress of Deputies of Spain

Day 3 - 20 May	
09:30 – 11:00	**Session Seven** ***The parliamentary response: good practices in enhancing cyber-security*** Law-making in specialized parliamentary committees, oversight over regulatory bodies and scrutiny on governmental actions, targeted hearings and investigations, and representations of citizens and businesses concerns are some of the options available to parliaments to enhance cyber-security. The session will review a few practices carried out by legislatures around the world to respond to the cyber-security challenges and their effectiveness. ***Moderator**: **Sebastiaan von Solms**, Professor, Academy for Information Technology, University of Johannesburg, South Africa* • **Michael Mukuka**, Principal Clerk (ICT), Member of the National Working Group on Cybersecurity, National Assembly of Zambia • **Zondol Hersesse**, President of the Constitutional Laws Committee, National Assembly of Cameroon • **Marco Gercke**, Director, Cybercrime Research Institute
11:00 – 11:15	Coffee break
11:15 – 12:30	**Session Eight** ***Inter-parliamentary Cooperation for Cyber-Security*** The absence of an internationally-agreed legal framework hampers the fight against cybercrime. This session will examine the existing mechanisms for international coordination on cyber-security and discuss options for inter-parliamentary cooperation on and support to the cyber-security agenda. ***Moderator**: **Andy Richardson**, Information Specialist, Inter-Parliamentary Union* • **Marco Obiso**, Coordinator, Inter-Sectoral Activities, ITU • **Gillian Murray**, Chief, Conference Support Section, Focal Point for Cybercrime, United Nations Office on Drugs and Crime (UNODC) • **Frederick Wamala**, Research Associate/Cybersecurity Advisor, Department of Management, Information Systems and Innovation Group, London School of Economics
12:30 – 13:00	Closing Session

FOURTH PARLIAMENTARY FORUM ON SHAPING THE INFORMATION SOCIETY
THE TRIPLE CHALLENGE OF CYBER-SECURITY: INFORMATION, CITIZENS AND INFRASTRUCTURE

18-20 May 2011
Geneva, Switzerland

The Fourth Parliamentary Forum on Shaping the Information Society, held in Geneva on 18, 19 and 20 May 2011, highlighted that effective and harmonized legal frameworks are necessary to address the challenges of cybersecurity.

Confidence in cyberspace is vital for the development of the information society. As parliamentarians, we have the responsibility to enact legislation that promotes a safe and enabling environment for citizens, businesses and institutions to fully benefit from the Internet revolution, without constituting a threat to the peace and sovereignty of societies and in accordance with the principles of the World Summit on the Information Society.

Yet the Internet knows no borders. We recognize that cybercrime and the illicit use of ICT cannot be combated effectively without greater harmonization of our national legislation. The lack of harmonization creates an environment in which criminal activities can proliferate in relative impunity, and it is therefore urgent to act promptly.

While noting with satisfaction the regional and international initiatives to promote cybersecurity, we deplore the absence of an internationally agreed instrument that would provide a comprehensive framework for countries to coherently address cybersecurity issues in a coordinated manner.

We commend the organizers of the Fourth Parliamentary Forum for convening this meeting. We call upon the Global Centre for ICT in Parliament – a joint initiative of the IPU and the United Nations – to strengthen its engagement with parliaments on topics related to the Information Society. In particular, we request the Global Centre to create a working group of parliamentarians to explore ways to harmonize legislation on cybersecurity, and to report back on progress at the next Parliamentary Forum.

List of Participants

NATIONAL PARLIAMENTS

Angola

ALÈ FERNANDES, Ana (Ms.)	Member of the National Assembly
COHEN, Teresa (Ms.)	Member of the National Assembly
CHIMONA, Tito (Mr.)	Member of the National Assembly
DE CARVALHO, Adriano (Mr.)	Member of the National Assembly
FRANCISCO, Joaquim (Mr.)	IT Engineer, National Assembly
GARCIA, Anabela (Ms.)	Secretary of Committee, National Assembly

Belgium

DEDECKER, Peter (Mr.)	Member of the House of Representatives
DAEMS, Hendrik (Mr.)	Member of the Senate
MERCENIER, Eric (Mr.)	MP Assistant, Senate

Cambodia

CHHEANG Vun	President of Foreign Affairs, International Cooperation and Information Committee, National Assembly

Cameroon

HERSESSE, Zondol (Mr.)	President of the Constitutional Laws Committee, National Assembly

Chile

FARIAS PONCE, Ramón (Mr.)	Member of the Chamber of Deputies
CANTERO, Carlos (Mr.)	Member of the Senate
FIGUEROA ESPINOZA, Hernán (Mr.)	Head of ICT, Chamber of Deputies

Colombia

OLANO BECERRA, Plinio (Mr.)	Member of the Senate
FERRO SOLANILLA, Carlos (Mr.)	Member of the Senate

Democratic Republic of Congo

SILUNVANGI, Raphael (Mr.)	Member of the Senate
MUTINGA MUTUISHAYI, Modeste (Mr.)	Rapporteur of the Senate
MWEMBO, Jean Claude (Mr.)	Head of Communication Division, Senate
NGANDU, Délance (Mr.)	Head of IT Division, Senate

Denmark

RUGHOLM, Daniel (Mr.)	Member of the Science and Technology Committee, Parliament

Djibouti

MOHAMED DINI, Houmed (Mr.)	Vice President of the Foreign Affairs Committee, National Assembly
GAMIER ASSOWEH, Abdoulkader (Mr.)	Head of IT, National Assembly

Dominican Republic

DILEPCIO-NUNEZ, Ramon (Mr.)	Member of the Chamber of Deputies
CRESPO, Rafael Tobías (Mr.)	Member of the Chamber of Deputies
GUILLEN, Jose Nelson (Mr.)	Member of the Chamber of Deputies
ABREU, Rafael Leónidas (Mr.)	Member of the Chamber of Deputies
VALENTÌN, Julio César (Mr.)	Member of the Senate

Ecuador

GAGLIARDO, Gastón (Mr.)	Member of the National Assembly

Estonia

KOROBEINIK, Andrej (Mr.)	Member of the Constitutional Committee, Parliament

France

MARTIN-LALANDE, Patrice (Mr.)	Member of the National Assembly
DRAIN, Michel (Mr.)	Counsellor, National Assembly

Ghana

TWUMASI-APPAH, Felix (Mr.)	Chairman of the Committee on Communications, Parliament
BOTWE, Daniel Kwaku (Mr.)	Member of the Committee on

	Communications, Parliament
JABANYITE, Samuel Abdulah (Mr.)	Member of the Committee on Communications, Parliament
ADDOW-QUARSHIE, David Melford (Mr.)	Head of ICT, Parliament
MORVORDZI, Frederick Yao (Mr.)	Assistant to the Chairman of the Committee on Communications, Parliament

Guatemala

ESTRADA LIMA, Erasmo (Mr.)	Member of the Committee on Education, Science and Technology, Congress of the Republic
GRESSI CAMPOSECO, Osbelí Avenamar (Mr.)	Member of the Committee on Education, Science and Technology, Congress of the Republic
GÓMEZ CRISTIANI, Paúl Estuardo (Mr.)	Member of the Congress of the Republic

India

SINGH RAO, Inderjit (Mr.)	Member of the House of the People
VIKRAM JARDOSH, Darshana (Ms.)	Member of the House of the People
ANWAR ANSARI, Ali (Mr.)	Member of the Council of States
LUTHRA, Sudesh (Ms.)	Director, House of the People Secretariat

Iraq

KHUDHUR AHMED, Majid (Mr.)	Director General of ICT Directorate, Council of Representatives
JABBAR ABBOOD, Sattar (Mr.)	ICT Advisor, Council of Representatives
ABUBAKR AHMED, Mohammed (Mr.)	Director General of Media Directorate, Council of Representatives
AL-DYIN MOHAMED, Ayad (Mr.)	ICT expert, Council of Representatives

Jordan

ALGHWIRI, Salameh (Mr.)	Member of the House of Representatives
ALSQOUR, Mujhem (Mr.)	Member of the House of Representatives
HAWAMDEH, Hazem (Mr.)	Parliamentary Affairs Officer, House of Representatives

Maldives

MUSTHOFA, Ahmed (Mr.)	Head of ICT, People's Majlis

Mali

BRAHIMA, Dianessy (Mr.)	Member of the National Assembly

Malta

FRENDO, Michael (Mr.)	Speaker of the House of Representatives
SCICLUNA, Raymond (Mr.)	Clerk Assistant, House of Representatives

Morocco

ADDAB ZEGHARI, Mohamed (Mr.)	Member of the House of Councillors
AKLIM, Hassan (Mr.)	Member of the House of Councillors
ARCHANE, Abdessamad (Mr.)	Member of the House of Councillors
EL HILAA, Rahhou (Mr.)	Member of the House of Representatives
SENTISSI, Omar (Mr.)	Member of the House of Representatives
GHOUIRGATE, M. Youssef (Mr.)	Officer, House of Councillors

Namibia

AMWEELO, Moses (Mr.)	Chairperson of the Standing Committee on ICT, National Assembly
LUCKS, Heiko (Mr.)	Member of the Standing Committee on ICT, National Assembly
NAHOGANDJA, David (Mr.)	Parliamentary Staff, National Assembly

Niger

BOUKARI, Abdou (Mr.)	Member of Parliament, President of the Parliamentary Network of ICT, National Assembly
YAHAYA, Mahamane (Mr.)	Chief of Cabinet of the President, National Assembly
ABDOU, Moussa (Mr.)	Parliamentary Administrator, Counselor of the Parliamentary Network of ICT, National Assembly

Pakistan

HUSSAIN BOKHARI, Syed Nayyer (Mr.)	Leader of the House, Senate
KAZIM KHAN, Muhammad (Mr.)	Member of the Senate
ADEEL, Haji Muhammad (Mr.)	Member of the Senate

GHAFOOR HAIDERI, Maulana Abdul (Mr.)	Member of the Senate
ABBASS, Syed Mussarrat (Mr.)	Secretary, Senate
BABAR, Iftikhar Ullah (Mr.)	Special Secretary, Senate

Panama

SAAD, Antonio (Mr.)	Director, ICT Department, National Assembly

Romania

LAZĂR, Sorin Constantin (Mr.)	Secretary of the Committee for Human Rights, Cults and Minorities, Senate
DUMITRESCU, Cristina (Ms.)	Head of the Division for International Parliamentary Organizations, Senate

Russian Federation

ZHELEZNYAK, Sergey (Mr.)	Chairman of the Committee on ICT, State Duma
REZNIK, Boris (Mr.)	Deputy Chairman of the Committee on ICT, State Duma
NOSKOVA, Olga (Ms.)	Member of the Committee on ICT, State Duma
KARMEEV, Anbyar (Mr.)	Head of Secretariat, Committee on ICT, State Duma
STAVITSKY, Valery (Mr.)	Secretary of delegation, State Duma
TRIBUNSKY, Alexander (Mr.)	Interpreter, State Duma

Rwanda

GASAMAGERA, Wellars (Mr.)	Member of the Senate, Member of Parliament ICT Steering Committee

Saudi Arabia

ALABOUD, Fahad (Mr.)	Member of the Consultative Council
ALSADOUN, Abdullah (Mr.)	Member of the Consultative Council
ALSAEED, Anas (Mr.)	Parliamentary Relations Officer, Consultative Council
ALATEEG, Adel (Mr.)	Protocol Officer, Consultative Council

South Africa

POLIAH, Ravi (Mr.)	Division Manager, Corporate Services, Parliament

Spain

DE ANDRÉS, Javier D. (Mr.)	IT Director, Congress of Deputies

Swaziland

MSIBI, Themba (Mr.)	Member of the Senate

Trinidad and Tobago

HAMEL-SMITH, Timothy (Mr.)	President of the Senate

Ukraine

DOVGYI, Stanislav (Mr.)	Member of Parliament
SYDORENKO, Oleksiy (Mr.)	Head of ICT, Parliament
GULIAIEV, Kyrylo (Mr.)	MPs assistant
DEYNEKA, Igor (Mr.)	MPs assistant

Venezuela

PEÑA GONZÁLEZ, Geovanni J. (Mr.)	Vice President of the Science, Technology and Innovation Committee, National Assembly

Zambia

MUKUKA, Michael (Mr.)	Principal Clerk (ICT), Member of the National Working Group on Cybersecurity, National Assembly

OTHER PARLIAMENTS AND PARLIAMENTARY ASSEMBLIES

European Parliament

WIELAND, Rainer (Mr.)	Vice President
TOORNSTRA, Dick (Mr.)	Director, Office for the Promotion of Parliamentary Democracy (OPPD), Directorate-General for External Policies
BECKER, Georg (Mr.)	Assistant to the Vice President

ECOWAS Parliament

TOURE, Adama (Mr.)	Webmaster, IT Unit
SOTUMINU, Adesina (Mr.)	Parliamentary Clerk

Parliamentary Assembly of the Francophonie

EZA, Mireille (Ms.)	Director, Programme Noria
AMAR, Saliou (Mr.)	Technical Assistant, Programme Noria
CACHALDORA, Carlos (Mr.)	IT Specialist

INTERNATIONAL ORGANIZATIONS

United Nations

CASINI, Gherardo (Mr.)	Head, Office of the United Nations Department of Economic and Social Affairs in Rome and Secretary to the Board, Global Centre for ICT in Parliament
GIACOMELLI, Daniela (Ms.)	Programme Officer, Global Centre for ICT in Parliament, United Nations Department of Economic and Social Affairs
MURRAY, Gillian (Ms.)	Focal Point for Cyber Crime, United Nations Office on Drugs and Crime (UNODC)
SOMMARIN, Clara (Ms.)	Child Protection Specialist, Exploitation and Violence, Child Protection section, Programme Division, United Nations Children's Fund (UNICEF)

Inter-Parliamentary Union

RICHARDSON, Andy (Mr.)	Information Specialist

International Telecommunication Union

TOURÉ, Hamadoun (Mr.)	Secretary-General
PONDER, Jaroslaw (Mr.)	Strategy and Policy Advisor
OBISO, Marco (Mr.)	Coordinator, Inter-Sectoral Activities
JEOUNGHEE, Kim (Ms.)	Policy and Legal Analyst
LICCIARDELLO, Carla (Ms.)	Project Officer
NTOKO, Alexander (Mr.)	WSIS C5 Focal Point and Head of Corporate Strategy Division
ASSEFA, Sorene (Ms.)	IT System Officer
NDEUCHI, Ghislain (Mr.)	Intern

OSMANI, Orhan (Mr.)	Emergency Telecomm Coordinator
SOUHEIL, Marine (Ms.)	Head, ICT Applications and Cybersecurity Division
EUCHNER, Martin (Mr.)	Advisor of Study Group 17

Organization for Security and Co-operation in Europe

MALISEVIC, Nemanja (Mr.)	Assistant Programme Officer, Counter Terrorism News Coordinator, Action against Terrorism Unit

GOVERNMENTS

Bulgaria

KANTCHEV, Petko (Mr.)	Advisor to the Vice Minister, Ministry of Transport, Information Technology and Communications

Chile

OYARCE, Pedro (Mr.)	Ambassador, Permanent Representative, Permanent Mission to the United Nations and other International Organizations in Geneva
GUZMÁN, Fernando (Mr.)	Third Secretary, Permanent Mission to the United Nations and other International Organizations in Geneva
PARODI, Luciano (Mr.)	Deputy Chief of Mission, Permanent Mission to the United Nations and other International Organizations in Geneva
VERDUGO, Ximena (Ms.)	Fist Secretary, Permanent Mission to the United Nations and other International Organizations in Geneva

Ghana

IDDRISU, Haruna (Mr.)	Minister of Communications

Israel

ADAM, Ron (Mr.)	Deputy Permanent Representative, Permanent Mission to the United Nations Office and other international organizations in Geneva

Kenya

KATUNDU, Michael (Mr.)	Assistant Director, Information Technology, Communications Commission of Kenya

Oman

AL-SALEHI, Badar Ali (Mr.)	Director, National CERT

Pakistan

ALI KHAN, Shafqat (Mr.)	Deputy Permanent Representative, Permanent Mission to the United Nations Office and other international organizations in Geneva
AAMIR KHAN, Mohammad (Mr.)	First Secretary, Permanent Mission to the United Nations Office and other international organizations in Geneva
AHMAD, Bilal (Mr.)	First Secretary, Permanent Mission to the United Nations Office and other international organizations in Geneva

Turkey

KETEVANLIOGLU, Salim (Sr.)	ICT Expert, ICT Regulatory Body

United Arab Emirates

AL GHANIM, Mohamed Nasser (Mr.)	Director General, Telecommunications Regulatory Authority

OTHER ORGANIZATIONS AND INSTITUTIONS

AMIN, Mohd Noor (Mr.)	Chairman, International Multistakeholder Partnership Against Cyberthreats (IMPACT)
GERCKE, Marco (Mr.)	Director, Cybercrime Research Institute
HERNANDEZ, Marielos (Mr.)	Executive President of PANI
MONTI, Cristina (Ms.)	Director, European Internet Foundation
MROZ, John (Mr.)	CEO, East West Institute (EWI)
PRÉCSÉNYI, Zoltán (Mr.)	Government Relations Manager, European Government Relations Team, Symantec Corporation
RIGONI, Andrea (Mr.)	Director General, Global Cybersecurity Centre
SANTORELLI, Steve (Mr.)	Director of Global Outreach, Team Cymru

TAYLOR TATE, Deborah (Ms.)	Former U.S. Commissioner, Federal Communications Commission, 2009 WTISD Laureate
WESTBY, Jody (Ms.)	CEO and Founder, Global Cyber Risk

ACADEMIA

GHERNAOUTI-HÉLIE, Solange (Ms.)	Professor, Faculty of Business and Economics, University of Lausanne
UNWIN, Tim (Mr.)	Professor, Royal Holloway, University of London
VON SOLMS, Sebastiaan (Mr.)	Professor, Academy for Information Technology, University of Johannesburg
WAMALA, Frederick (Mr.)	Research Associate/Cybersecurity Advisor, London School of Economics